AD NUMBER

ADB316092

LIMITATION CHANGES

TO:

Approved for public release; distribution is unlimited.

FROM:

Distribution authorized to U.S. Gov't. agencies only; Proprietary Information; MAR 2006. Other requests shall be referred to President, Naval Postgraduate School, Code 261, Monterey, CA 93943-5000.

AUTHORITY

NPS ltr dtd 24 Jul 2009

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

VALIDATING A METHOD FOR ENHANCED COMMUNICATIONS AND SITUATIONAL AWARENESS AT THE INCIDENT COMMAND LEVEL

by

James H. Graham, Jr.

March 2006

Thesis Advisor:	Tom Housel
Second Reader:	Ted Lewis

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, 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 this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Validating a Method for Enhanced Communications and Situational Awareness at the Incident Command Level			**5. FUNDING NUMBERS**
6. AUTHOR(S) James H. Graham, Jr.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Distribution authorized to U.S. Government Agencies only; (Proprietary Information); (March 2006). Other requests for this document must be referred to President, Code 261, Naval Postgraduate School, Monterey, CA, 93943-5000 via the Defense Technical Information Center, 8725 John J. Kingman Road, STE 0944, Ft. Belvoir, VA 22060-6218			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

The availability and interoperability of communications at an incident scene have long been recognized as high-priority problems that need to be addressed to improve our nation's Homeland Security and preparedness. This thesis describes a proposed methodology to address these issues *at the Incident Command level* while enhancing situational awareness and information sharing. The thesis analyzes the results of a research project funded by the Department of Homeland Security at the University of Louisville's IT Research Center for Homeland Security.

The problem being addressed is that the decision-maker with the boots on the ground, the Incident Commander, needs relevant information in the early stages of the emergency at the incident scene and an efficient way to communicate with other resources.

The research project fielded a prototype solution based on readily available commercial off-the-shelf components integrated in a man-portable configuration to provide maximum flexibility, lower costs, and ease of operations. A proposed concept of operations in various prevention and response environments was also recommended in the thesis after analyzing the results of several field exercises and interviews with users.

14. SUBJECT TERMS Communications, interoperability, collaboration, situational awareness, mobile command post, operations center			**15. NUMBER OF PAGES** 141
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

VALIDATING A METHOD FOR ENHANCED COMMUNICATIONS AND SITUATIONAL AWARENESS AT THE INCIDENT COMMAND LEVEL

James H. Graham, Jr.
Director, Information Technology Resource Center – University of Louisville
B.S., Eastern Kentucky University, 1977

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2006**

Author: James H. Graham, Jr.

Approved by: Dr. Tom Housel
Thesis Advisor

Dr. Ted Lewis
Second Reader

Dr. Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The availability and interoperability of communications at an incident scene have long been recognized as high-priority problems that need to be addressed to improve our nation's Homeland Security and preparedness. This thesis describes a proposed methodology to address these issues *at the Incident Command level* while enhancing situational awareness and information sharing. The thesis analyzes the results of a research project funded by the Department of Homeland Security at the University of Louisville's IT Research Center for Homeland Security.

The problem being addressed is that the decision-maker with the boots on the ground, the Incident Commander, needs relevant information in the early stages of the emergency at the incident scene and an efficient way to communicate with other resources.

The research project fielded a prototype solution based on readily available commercial off-the-shelf components integrated in a man-portable configuration to provide maximum flexibility, lower costs, and ease of operations. A proposed concept of operations in various prevention and response environments was also recommended in the thesis after analyzing the results of several field exercises and interviews with users.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

1U – One Unit of rack space
1xRTT – Single Carrier Radio Transmission Technology
AAR – After Action Report
AC – Alternating Current
ALOHA – Area Locations of Hazardous Atmospheres
ANFO – Ammonium Nitrate – Fuel Oil
ARL – Army Research Lab
ATIX – Anti-Terrorism Information eXchange
AT&T – American Telephone and Telegraph
AVL – Automatic Vehicle Location
BATF – Bureau of Alcohol, Tobacco and Firearms
CAMEO – Computer Aided Management of Emergency Operations
CBRNE – Chemical, Biological, Radiological, Nuclear, and Explosive
CCNA – Cisco Certified Network Associate
CDC – Centers for Disease Control
CDMA – Code Division Multiple Access
CIO – Chief Information Officer
COLTS – Cells on Light Trucks
COTS – Commercial Off-the-Shelf
COWS – Cells on Wheels
CPF – Command Post Forward
CST – Civil Support Team
CT – Computerized Tomography
CTU – Command Tactical Unit
CWID – Coalition Warrior Interoperability Demonstration
DC – Direct Current
DEA – Drug Enforcement Agency
DHS – Department of Homeland Security
DMIS – Disaster Management Information System

DSL – Digital Subscriber Line

DSS – Decision Support System

EMAC – Emergency Management Assistance Compact

EOC – Emergency Operations Center

EPA – Environmental Protection Agency

ESU – Emergency Services Unit

FBI – Federal Bureau of Investigation

FDNY – Fire Department New York

FEMA – Federal Emergency Management Agency

FRS – Family Radio Service

FTE – Full Time Equivalent

GHz – Giga-Hertz

GIS – Geospatial Information System

HAZMAT – Hazardous Material

HFN – Hastily Formed Networks

HHS – Health and Human Services

HP – Hewlett-Packard

HSIN – Homeland Security Information Network

IC – Incident Commander

ICE – Immigration and Customs Enforcement

ICP – Incident Command Post

ICS – Incident Command System

ICSS – Incident Command Support Specialist

IDT – Incident Dispatch Team

IED – Improvised Explosive Device

INS – Immigration and Naturalization Service

IP – Internet Protocol

IT – Information Technology

IRT – Incident Response Team

iTRC/HS – Information Technology Research Center for Homeland Security

JOC – Joint Operations Center

Kbps – Kilobits per second

KCTCS – Kentucky Community and Technical College System

Kw – Kilo-watt

LAN – Local Area Network

LCD – Liquid Crystal Display

LEO – Law Enforcement Online

MATT – Medical Assist Tactical Team

Mbps – Megabits per Second

MCSE – Microsoft Certified Systems Engineer

MCTS – Microsoft Certified Technology Specialist

MERS – Mobile Emergency Response Support

MHz – Mega-Hertz

MITOC – Man-portable Interoperable Tactical Operations Center

MSCA – Military Support to Civil Authorities

MSDS – Material Safety Data Sheet

NASCIO – National Association of State Chief Information Officers

NEMA – National Emergency Management Association

NGA – National Geospatial Intelligence Agency

NIC – NIMS Integration Center

NIMS – National Incident Management System

NOAA – National Oceanographic and Atmospheric Administration

NPS – Naval Postgraduate School

NRP – National Response Plan

OSHA – Occupational Health and Safety Administration

PBS – Public Broadcasting System

PC – Personal Computer

PCMCIA – Personal Computer Memory Card International Association

PDA – Personal Digital Device

POD – Point of Dispensing

PPE – Personal Protective Equipment

RDD – Radiological Dispersal Device

RISS– Regional Information Sharing System

RV – Recreational Vehicle

SARS – Severe Acute Respiratory Syndrome

SBU – Sensitive But Unclassified

SCENE – Secure Collaborative Engagement Network for Emergencies

SDR – Software Defined Radio

SINBAD – Southern Indiana Bioterrorism Attack and Defense

SIOC – Strategic Information and Operations Center

SITREP – Situation Report

STEPs – Spatial Templates for Emergency Preparedness system

SUV – Sport Utility Vehicle

S.W.A.T. – Special Weapons and Tactics

TDT – Tactical Dispatch Team

UAV – Unmanned Aerial Vehicle

UHF – Ultra High Frequency

USNORTHCOM – United States Northern Command

VHF – Very High Frequency

VoIP – Voice over Internet Protocol

VPN – Virtual Private Network

WISER – Wireless Information System for Emergency Responders

WLAN – Wireless Local Area Network

WMD – Weapons of Mass Destruction

WTC – World Trade Centers

ACKNOWLEDGMENTS

I would first like to acknowledge the outstanding support of the administration, faculty and staff of the Naval Postgraduate School's Center for Homeland Defense and Security in my pursuit of this Master's Degree. The professionalism, knowledge, and depth of resources they provided were an experience that I will always cherish. I consider it an honor to represent the CHDS program as I move on in my profession.

The friendship, support, and leadership exhibited by my classmates were a constant joy and inspiration. I am truly humbled to be among them as a Cohort and was able to learn a tremendous amount of valuable knowledge by my association with them during this program. I look forward to counting my classmates as life-long friends and collaborators.

I wish to also thank the Department of Homeland Security and the Office of Domestic Preparedness for sponsoring and mentoring this valuable program. Its support of the CHDS program illustrates a commitment to excellence that should serve as an example to all other government agencies. The research funding for the MITOC project at my research lab was also provided by the Department of Homeland Security under a program administered by the National Institute of Hometown Security. I would not have had the opportunity to write this thesis if it were not for them and the visionary leadership of Kentucky Congressman Hal Rogers who championed the concept of a statewide university consortium to address Homeland Security technology problems.

I appreciate the support of my employer, the University of Louisville, and President James Ramsey for allowing me the time to participate this program. I also appreciate President Ramsey's consideration and support of the many Homeland Security-related proposals for research and curricula that I have submitted since becoming a part of the CHDS program as well as the support of my staff during my many absences.

Special thanks go out to Ray Nelson for making me aware of the CHDS opportunity along with Dick Bartlett and FBI Special Agent Steve Stacy for their strong endorsements for my application. I also wish to thank the Metro Louisville WMD Crisis Group, FBI Infragard, Joint ESU, and Area 6 WMD/HAZMAT for their patience and support while I had to reduce some of my duties and commitments with them as I completed this program.

Lastly, I could not have completed this journey without the love and support of my wife, Judy, and daughter, Courtney. Their understanding and support during the many nights and weekends that I was doing class work or thesis writing made it easier for me to put the effort and energy required into the completion of the requirements for the CHDS program over the last eighteen months.

I. INTRODUCTION

A. BACKGROUND

Officer Barry Byers, along with fellow officers from the Greenbelt, Maryland Police Department, were plying the waters in the streets of flooded New Orleans after Hurricane Katrina devastated the area in 2005. They were looking for people to rescue when a military helicopter came in and hovered over them. Someone in the chopper waived a plastic bottle at them and dropped it. Inside was a note warning them of a major gas leak just ahead.[1] It seems incredulous that, in the 21st century, our military had to resort to the proverbial "message in a bottle" to communicate effectively with first responders. Other emergency teams, arriving from out of town to assist in the hurricane response, found that they also could not talk to local command and control, first responders, or dispatchers, because radio, cellular, and landline outages were compounded by a lack of interoperable radios.

Over the past five years, various think tanks and special government committees, such as the Gilmore Commission,[2] the 9/11 Commission,[3] and the U.S. House of Representatives Bipartisan Committee on Hurricane Katrina,[4] have issued reports which stressed that we can improve emergency responses by providing better communications and information sharing solutions to support our first responders. Some suggested key elements contained in these reports address the need for essential communications and Information Technology (IT) infrastructure, to give communities and first responders—more specifically, their Incident Commanders, for the purpose of this thesis—the following capabilities:

- Immediate access to documentation regarding local assets and response guidelines

---

[1] NBC Evening News, 6:30 P.M. broadcast, September 23, 2005.

[2] The Gilmore Commission V, *Forging America's New Normalcy* (Arlington: The RAND Corporation, 2003), 30.

[3] 9/11 Commission, *The 9/11 Commission Report* (New York: W.W. Norton & Company, Inc, 2004), 397.

[4] U.S. House of Representatives, Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative*, February 15, 2006, 163, http://www.gpaccess.gov/congress/index.html, accessed February 2006.

- The ability to refine, update, and manage content from the field
- Real-time collaborative information sharing across jurisdictions and agencies
- Better project and resource management capability
- Mapping and visual graphic support
- Access to intelligence analysis
- Decision support technology
- Interoperability of voice and data communications among local, state, and federal resources.

Today, one would be hard-pressed to find a community in the United States that has achieved more than one or two of these desirable technology-based attributes in actual practice, especially at the Incident Command level. Outside of major metropolitan cities like New York or Los Angeles, there is little evidence of coordinated plans, strategies or capabilities to integrate and deploy such technology tools in support of Homeland Security and Emergency Management. You may see one or more of these critical technology capabilities at an Emergency Operations Center (EOC) in a major metropolitan city. Some jurisdictions may have large complex and expensive “mobile command posts” with some of the desired information technology attributes and trained staff to run them. Deploying such capabilities in small or rural jurisdictions, in the field to support the Incident Commander or in disaster zones with no infrastructure, has proved to be problematic in practice.

This thesis claims that a rapidly-deployable, rugged, highly portable, and easy to use integrated command and control communications system is the most cost-effective and efficient for the Incident Commander to use in many circumstances, especially in the initial hours of a response, rather than the typical "mobile command post" that is based on a large bus or RV chassis. The thesis also supports the argument that the proposed solution potentially solves many of the concerns about the role of failed communications in the response to Hurricane Katrina. This is because the proposed solution is small enough to be carried by two people, costs from one-tenth to one-half the cost of a bus or RV-based mobile command post, is less complicated to operate because of its automated set-up routine, and is easier to get to the incident scene. This claim will be supported by an analysis of size, cost, and ease-of-use features of its integrated Wi-Fi, satellite

telephony, and off-the-shelf commercial software and components. These resources provide situational awareness, collaboration and communications interoperability tools to the Incident Commander that is less expensive and easier to operate than existing systems. The benefits of the proposed solution to enhance situational awareness and information sharing from the field are compelling and will be examined in detail in this thesis.

B. THE COMMUNICATIONS AND INFORMATION TECHNOLOGY PROBLEM

One of the high-priority problems recognized by the Department of Homeland Security (DHS) is providing more robust communications and IT capability at the Incident Command level. Someone at the scene, however, has to act as the man-machine interface to interpret what information is needed, query for the information, analyze the response, and act on the information. Computer, communications and networking technologies are difficult to deploy at the field level and difficult to utilize if the end-user is not proficient in IT, inclined to use the technology, or trained to use it properly.

Communications technology is also costly to widely deploy in what the business sector calls "Enterprise" connectivity. This is an IT term used to describe the ability to rely on ubiquitous and reliable broadband (high speed) data communications across the "enterprise," whether the users are located in the same city or spread across the globe. The military refers to having these capabilities as a higher level of "situational awareness" or a robust "common operating picture." Other military terminology, such as "information dominance" and "joint collaboration" describes needs just as relevant to our hometowns—in the effort to prevent, mitigate, or respond to terrorism and natural disasters—as they are on the battlefield. The private sector and the military seem to have a handle on this problem while federal, state, and local governments have a long way to go in broad–scale application of available communications and IT solutions in a Homeland Security and emergency management environment.

Another problem addressed in this thesis is that many small to mid-sized communities across America do not have the financial resources, expertise, or the ability

to utilize leading edge software and computer hardware. Access to threat matrix intelligence sources, and interoperable communications networks to respond to major natural disaster or a terrorist attack, are almost non-existent. Some rural communities do not have a physical EOC other than a meeting room with some tables and chairs and perhaps a map of their jurisdiction. Many smaller communities do not have full-time staff; especially personnel trained in the latest communications and IT resources. In fact, it is impractical to equip all of America's communities with such expensive hardware, software, and personnel resources or to train their sometimes volunteer Emergency Management and response personnel in the use of rapidly changing, yet critically important, innovations in software and hardware for this growing domain.

The problem to be addressed is that the decision-maker with the boots on the ground, the Incident Commander, needs relevant information *in the early stages of the emergency at the incident scene*. The issues framing the problem are: how to send and receive the relevant information in a field environment; how to present that information so the Incident Commander can make use of it; and who should be trained to use the technology.

C. IMPORTANCE

> The difference between a catastrophe and an incident is what is done with the information in-between.
>
> Richard Russell
> Department of Homeland Security
> 29 June 2004

Catastrophes do occur without passing through the "incident" stage such as a hurricane or other major disaster; however, one can imagine a circumstance where key information, when shared with appropriate parties, could prevent a larger potential catastrophe. For example, a terrorist attack on a building with a Radiological Dispersal Device (RDD) may appear at first to be a normal bombing. If the first responders at the scene had a radiation detector, the larger threat would immediately be recognized and the information passed to the Incident Commander at the scene. If the Incident Commander had access to better situational awareness, such as a Geospatial Information System (GIS)

plot of the area; he or she could determine nearby infrastructure at risk, such as heavily traveled roads, utilities that could be contaminated, or high concentrations of residential tracts that may need to be informed of the need to either shelter in place or evacuate. To make those determinations, access to information will be critical and would include: specifically localized weather and wind direction; software to plot the potential size, track, and dispersion of the radiation plume; and access to knowledge about the potential health risks to the first responders to determine the type of Personal Protective Equipment (PPE) to utilize.

All of the information needed by the Incident Commander in this scenario can be accessed and utilized to mitigate the circumstances, potentially preventing the incident from escalating into a catastrophe, but *only if* the Incident Commander has access to technology. This would include sensors, application software, computers, and most importantly, a network to share this information with others. Therefore, this thesis argues that timely access to information technology is critically important to enable the Incident Commander to make effective decisions in a crisis.

D. RECOMMENDED SOLUTION TO BE VALIDATED

This thesis will chronicle the concept, design, implementation, testing, and validation of a proposed, highly-portable and rapidly-deployable technology delivery platform. It will also address a concept of operations on how to employ this technology as the most cost-effective and rational way to approach the problem of effective technology utilization at the Incident Command level. For example, this thesis will report on how well the proposed solution delivers right information, in the right place, at the right time, without requiring complex technical interaction on the part of the Incident Commander. This proposed approach will address important issues that have been identified in the lack of broad utilization of situational awareness and information-sharing tools at the Incident Command level because:

- It spreads the cost of the solution over a multi-jurisdictional area;
- It provides a standard methodology that would be compatible with local, state, and federal resources while not requiring every first responder and commander to be individually trained in detailed technology use;

- It supports mandated standards for interoperability, especially in radio communications, one of the most visible areas needing improvement in emergency response.

There is a clear need for a low-cost, rapidly-deployable, integrated technology package to connect the Incident Commander and local agencies with the emergency operation support resources of a fully-staffed state or regional EOC and other agency commands. Larger communities may have the subject matter experts and sophisticated software tools to support a local emergency, but getting that information (and avoiding information overload) to the Incident Commander is sometimes problematic.

A back-up support resource that can provide even more than Incident Command support is also needed for communities whose EOC is inadequate, damaged or destroyed, located within a hot-zone, or incapable of scaling up for a big event. For example, the City of New York experienced this on 9/11 when their EOC, along with the FEMA and FBI command centers, was lost when World Trade Center Building 7 collapsed later in the day after the attacks. An FBI special agent who was in their Command Center and evacuated before the collapse, said it took three days before they had computers set up again in a network to enable the widespread sharing of information to work the investigation. The agent also said that a rapidly-deployable phone and data system for all jurisdictions would be a good idea.[5] In fact, Richard Sheirer, Commissioner of the New York City Office of Emergency Management, specifically recommended that, to be more responsive to terrorist attack, cities need to improve all emergency communications capabilities and develop substantial, well-equipped *mobile* Emergency Operations Centers.[6]

---

[5] Personal conversation with FBI agent assigned in New York City on 9/11, FBI Infragard Conference, June 2003.

[6] Testimony of the Former Commissioner of the New York City Office of Emergency Management Richard J. Sheirer, Opening Remarks Before the National Commission on Terrorist Attacks Upon the United States, May 18, 2004 , http://knxup2.hsdl.org/homesec/docs/dhs/nps03-052004-06.pdf, accessed January 2005.

Hurricane Katrina was a prime example of how EOC locations were rendered inoperable due to damage from flooding or loss of communications.[7] A robust, yet portable, communications capability that could be rapidly deployed to alternate EOC sites, as well as to Incident Commanders in the field, would have alleviated some of the critical communications shortfalls that severed command and control from military headquarters and EOC sites to first responders and their incident commanders. These same networks were severed between federal, state and local government, and the EOC locations, further exacerbating the problem. Effective command and control could not be established and sustained in the void of a completely inoperable communications infrastructure. [8]

E. RESEARCH METHODOLOGY AND THESIS STRUCTURE

This thesis reviews the testing process to validate the proposed technology solution and its concept of operations. The question is whether a highly portable mobile command "system of systems" using commercial off-the-shelf components can provide a cost-effective delivery platform for information sharing, communications interoperability, and collaboration at the Incident Command level. The proposed concept addresses some of the most critical IT and communications deficiencies, without the expense of deploying full-time hardware, software, and trained personnel to every Emergency Operations Center or jurisdiction.

The funding for this research project, providing the modality for this thesis, is being provided by the Department of Homeland Security under a $1.2 million, three-year grant to the author's Homeland Security research center at the University of Louisville. The funding authority is the National Institute for Hometown Security, through a cooperative arrangement with the National Institutes of Justice, with the Department of Homeland Security as the granting authority and research recipient. The reported findings required by the funding source provide the empirical research to support this thesis and

---

[7] U.S. House of Representatives, Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative*, February 15, 2006, 191, http://www.gpaccess.gov/congress/index.html, accessed February 2006.

[8] Ibid., 197.

the ultimate validation of the proposed concept of operations. A graduate research assistant administered interviews to subjects suggested by the research team, and advisors from the public safely and emergency management domain. The research project was reviewed by the University of Louisville's Institutional Review Board and was granted an exempt status from their oversight—due to the minimal level of interaction and lack of human subject intervention. Personal experiences and observations during field exercises and deployments, recollections of quotes and comments from observers and users, combined with the results of the interviews and measured performance data, form the basis for the overall findings.

The first chapter of this thesis provides the background information to frame the issue at hand and lists the critical areas that help define the problem statement. It goes on to illustrate the importance of solving the problem and the benefits that will be derived. It concludes with an outline of a potential solution that was validated in a research project.

Chapter II examines the current approaches to addressing the problem. It begins with a review of case studies of successes and failures in the utilization, or lack thereof, of communications and IT in prevention and response to terrorist events and natural disasters. The chapter continues with a review of some of the policies that could potentially address some of the issues listed in this thesis. Chapter II concludes with a recommended course of action for this line of inquiry that combines a technological as well as concept-of-operations approach to address the problem.

Chapter III explores the proposed solution in detail: an integrated communications and situational awareness system called the Man-portable Interoperable Tactical Operations Center, or MITOC for short. This chapter explains the purpose and scope of the research grant to pursue a solution to the problem, the concept of operations to be validated, the design of the MITOC, and a rationale for the selection of the technologies it utilizes. It is also important to note that the research project and this thesis suggest the MITOC as an alternative to the bus or RV-based configuration that is typically utilized as a "Mobile Command Post." The high costs are problematic, as is the need for specialized resources dedicated to running these platforms in every application.

Chapter IV chronicles the performance of the MITOC under different applications and circumstances that may be encountered in various jurisdictions. The research team provided the proposed solution to the Unified Command responsible for providing security to The Kentucky Derby, one of the world's most famous sporting events, drawing over 150,000 patrons to the research team's jurisdiction. This deployment emphasized the MITOC's capacity to be utilized in a "Prevention" mode by providing surveillance and intelligence sharing at the special event scene. The MITOC was later utilized at a Department of Defense technology demonstration for U.S. Northern Command (USNORTHCOM) in an annual event called the *Coalition Warrior Interoperability Demonstration* (CWID 2005). This event illustrated the MITOC's ability to interface with both military and civilian response agencies simultaneously. A rural law enforcement and HAZMAT exercise called *Operation Dukes of Hazard* was conducted to test MITOC's ability to function as a communications and information sharing resource in a rugged environment, beyond the reach of cell phones and radios. A biological terrorism exercise called *Operation SINBAD* put the MITOC to use as an ad-hoc Emergency Operations Center and a communications system for a medical point of dispensing in response to the attack. A final section is devoted to the MITOC's role as a deployable resource with actual emergency response agencies.

Chapter V concludes the thesis with final observations on the technologies, the MITOC's proposed concept of operations, and other applications for the MITOC that are beneficial to national security. It will illustrate how the concept was validated by the empirical research findings and how the utilization of a resource like the MITOC provides value to the Incident Commander. This thesis will offer a recommendation on how to move from concept and prototype to commercialization of the final solution.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CURRENT TECHNOLOGICAL APPROACHES

A. SUCCESSES AND FAILURES IN THE FIELD

It is readily apparent in professional journals, special commission reports, and media articles that there are serious issues to be resolved involving emergency communications capabilities, communications interoperability, and information sharing among agencies within the Homeland Security, Preparedness and Emergency Management domain. Documentation supporting this argument can be found in the National Response Plan (NRP)[9] and the National Incident Management System (NIMS).[10] These plans and guidelines provide a framework that indicates the ultimate responsibility—to address the issues of communications, information sharing, and other technologies supporting the Incident Commander—rests at the state and local level.[11] There is also consensus at all levels that local governments need to make sure they are interoperable and work as a team.[12] State and local governments are almost compelled to develop coordinated plans, since future funding of state and local programs will be dependant upon compliance with NIMS.[13] Because of the potential impact on funding, a concern was noted in discussion among members of the National Emergency Management Association (NEMA) in their annual meeting in 2004. They were concerned

---

[9] Department of Homeland Security, *National Response Plan*, December 2004, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml, accessed June 2005.

[10] Federal Emergency Management Agency, *National Incident Management System*, March 1, 2004, http://www.fema.gov/pdf/nims/nims_doc_full.pdf, accessed June 2005.

[11] Barbara Yagerman, Transcript of Forum Presentation: "The National Response Plan: An Update," Emergency Information Infrastructure Project Virtual Forum, 9/15/2004.

http://www.emforum.org/vforum/lc040915.htm/, accessed July 2005.

[12] Public Entity Risk Institute, "Local Government Preparation for Bioterrorist Acts", November 2001, 4, http://www.riskinstitute.org/ptrdocs/LocalGovernmentPreparationforBioterroristActs.pdf, accessed June 2005.

[13] Gil Jamieson, Transcript of Forum Presentation: "The NIMS Integration Center Implementing the National Incident Management System," Emergency Information Infrastructure Project Virtual Forum, 8/25/2004. http://www.emforum.org/vforum/lc040825.htm, accessed July 2005.

that the NRP and NIMS draft documents do not provide enough information on how to achieve the guidelines for interoperability and better field communications.[14]

Some of the highest priorities listed in the NRP and NIMS documentation deal with information sharing and interoperability, which are both technical disciplines on the surface. Many other facets also need to be addressed in the planning and implementation of solutions.[15] For example, advanced technologies have been demonstrated in reaction to the needs expressed by agencies post-9/11 such as Raytheon's First Responder vehicle.[16] Despite its innovative platform, widespread adoption of this mobile communications vehicle did not materialize due to its high cost and a lack of understanding by the vendor of how such technology should fit into the concept of operations at the state and local agency level.[17]

The primary question most of the sources reviewed have asked is not "should we do it" but "how do we do it." An unanswered question has become apparent: how to fit "it" in a local concept of operations. The issues uncovered in researching the current state of technology in communications and information technology for first responders, for example, address: (1) how agencies address the technology integration issue now and the impact of not utilizing available technology; (2) methodologies to test new approaches to technology implementation; and (3) the policy side of implementing new or advanced technology. For example, an interoperability project in San Diego, California, was able to implement the technical solutions to their interoperability problem in about thirty days. Unfortunately, the agreement to implement the plan took around two years due to the policy implementation problems exacerbated by turf issues and political negotiations,

---

[14] George Mason University School of Law National Center for Technology and Law Critical Infrastructure Protection Project, *CIP Report* (Zeichner Risk Analytics, LLC., October 2003), 4. http://techcenter.gmu.edu/programs/cipp/cip_report/cip_report_2.4.pdf, accessed October 2005.

[15] National Institute of Justice, "Why Can't We Talk," National Task Force on Interoperability, February 2003, http://www.agileprogram.org/ntfi/ntfi_guide.pdf, accessed April 2005.

[16] Steven Brill, *After* (New York: Simon & Schuster, 2004),467-8.

[17] Ramon Abellyro, Design engineer of the Raytheon First Responder vehicle, personal communication with the author, 2004).

according to Dr. David Boyd, Director of Project SAFECOM, which is the interoperability standards program within the Department of Homeland Security.[18]

A Harvard University report explores the issue of why local and state agencies should incorporate integrated strategies rather than "piecemeal solutions."[19] For example, something as simple as an updated directory of agency contacts is outside the grasp of most local governments. Also, there is no standardized protocol as to which entity would maintain such a list on the state or local level.[20] Adding complex technical components and software at the first responder level—such as handheld computers, geospatial imagery manipulation, real-time collaboration, and instant communications—will be exponentially more difficult. The new generation of technologies available to the first responders, based on successful commercial products, provides many useful capabilities in theory; however, there is a concern of information overload and the ability to train the user.[21]

State and Local Governments cannot expect the Department of Homeland Security to provide them with a laundry list of technologies and an instruction manual on how to integrate these tools; all the answers are not there yet. That is why it is crucial for federal programs to sponsor demonstration programs and pilot projects. Such tests in the user domain are referred to as "pathfinder" projects by former Department of Homeland Security Chief Information Officer Steven Cooper.[22] Cooper states that these pilot projects, to be relevant, need to be performed in timeframes of no longer than three to six

---

[18] Randall Larson, "More than Just Connecting Radios," *Homeland Protection Professional* (November/December 2005), 32.

[19] Harvard University, "Beyond the Beltway: Focusing on Hometown Security, Recommendations for State and Local Domestic Preparedness Planning A Year After 9-11", A Report of the Executive Session on Domestic Preparedness, John F. Kennedy School of Government, September 2002. http://bcsia.ksg.harvard.edu/BCSIA_content/documents/beyond_the_beltway.pdf, accessed April 2005.

[20] Robert Martin, Transcript of Forum Presentation: "Emergency Provider Access Directory (EPAD); Empowering Emergency Communications", Emergency Information Infrastructure Project Virtual Forum, 6/2/2004. http://www.emforum.org/vforum/lc040602.htm, accessed April 2004.

[21] John Zykowski, "First Responders Gear Up," *Federal Computer Week* (2003), http://www.fcw.com/supplements/homeland/2003/sup3/hom-edit-08-25-03.asp, accessed March 2004.

[22] Interview with Steven Cooper, *Journal of Homeland Security* (September 2002). http://www.homelandsecurity.org/journal/Interviews/displayInterview.asp?interview=18, accessed April 2004.

months, and budgeted at less than one million dollars. These pilots should be in the field in the hands of the actual practitioners at the state and local agency level.

An unanswered question: What entity is best positioned to conduct and evaluate the results of a pilot project? This entity will vary by jurisdiction and it should be the responsibility of state or local governments to identify and cultivate such a resource. The relevant literature seems to support the contention that academia can serve a very useful role in not only the creation of new technologies, but also in the testing of solutions.[23] In a 2004 speech, former Department of Homeland Security Secretary Tom Ridge referred to universities competing in the Commonwealth of Kentucky for Homeland Security research grants stating, "These organizations will harness the ingenuity and resources of the region's businesses, academic institutions and state and local partners. And thus Kentucky will more effectively develop technologies that will fortify our ability to protect the homeland from terrorists."[24]

This thesis will suggest a methodology to accomplish this integration task at the incident command level, since that is where the critical need is—even more so than at the Emergency Operations Center level.[25] It is important to recognize that technology is not the only element to consider in planning such projects.[26] In fact, technology can be wasted if it does not have a clear mission or does not have an everyday use.[27] To propose a technology solution that is totally integrated into a local or state jurisdiction, one must take into account the "human element" and a "governance structure" by developing standardized usage protocols.[28]

---

[23] Charles McQueary, "Meeting the Challenge of Protecting the Homeland," *TechComm National Journal of Technology Commercialization*, 2004,

http://www.techcommjournal.com/PDFSVol2No1/10-12HOMELAND,10,12.pdf, accessed June 2004

[24] Tom Ridge, Transcript of public speech by Department of Homeland Security Tom Ridge regarding the establishment of the Kentucky Homeland Security University Consortium in Somerset, Kentucky, 11/4/2004. http://www.dhs.gov/dhspublic/display?content=4099, accessed July 2004.

[25] R.A. Bartlett (former Louisville Emergency Management Agency Director), personal communication with the author.

[26] National Institute of Justice, "Why Can't We Talk."

[27] Tobin, "Improving Homeland Security."

[28] National Institute of Justice, "Why Can't We Talk."

Input and, most importantly, leadership by local government must permeate efforts to test and deploy new technologies and policies as an integrated package. Deputy Chief Charles Werner, of the Charlottesville, Virginia, Fire Department states, "Ideally, state and local leaders must define the new standard of interoperability (communications and operations) and accept nothing less."[29] Chief Werner's view is visionary and does capture the essence of the NIMS and NRP guidelines. On the other hand, some command staff in the field may have a negative view of new technology. For example, a member of the research team once overheard a Fire Chief say, "Just give me a radio and a cell phone…that's all I need." This attitude, some would call it technophobia, is ironic because, in a major crisis, radio frequencies may be overloaded with too many people talking over each other on a tactical channel. Or, they may be unable to establish communications with other agencies at the scene of a large incident due to a lack of interoperability. A cell phone can also be easily rendered useless due to network traffic congestion.[30] In the case of widespread weather-related disasters, such as hurricanes or tornadoes, cell phone towers may be blown down.

Solving these types of technology issues is important because today's radio and cell phone availability may be quickly negated by tomorrow's disaster or terrorist attack. The critical importance of communications technology and its impact was acutely realized after the 9/11 attack in New York City due to the destruction of much of Verizon's telecommunications switching infrastructure and how important it was to quickly restore services.[31]

For example, during the testing of some new communications technologies described in the case studies section of this thesis, the MITOC research team experienced cell phone congestion problems at a large open venue in the team's jurisdiction. This event's nearly one-half million attendees quickly overwhelmed the cell networks, even without an emergency. Despite the cell congestion issue, the backbone network of the wireless Internet access that the team was testing worked fine. This was similar to

---

[29] George Mason University School of Law, *CIP Report*.

[30] National Institute of Justice, "Why Can't We Talk."

[31] Brill, *After*, 42.

communications phenomena experienced in New York City after the collapse of the World Trade Center towers that housed many of the region's cell phone towers and radio repeaters. Even though cell phones were not usable for most carriers in the area, either due to physical destruction or congestion, Internet text messaging still worked on cell phones. RIM Blackberries, a relatively new mobile email device at that time, also continued to work for many users. This is due to the architecture of the Blackberries being more Internet-centric rather than circuit-based like the trunks feeding cell phone towers.

Most people in America and the rest of the civilized world can navigate around the Internet effectively. Effective technologies to support communications and information sharing in the realm of the emergency responder and law enforcement professional should be applicable to the job and able to be utilized instinctively—much like a side-arm or other tool of the trade. For example, if one can understand how to shop on eBay or Amazon.com and send an email, one should be able to use a well-designed web-based situation awareness and collaboration software tool. Ellen Gordon of the Naval Postgraduate School pointed out, not long after the attacks of 9/11, that chat rooms and web page announcements are a good way to conduct information sharing briefings during a critical incident.[32] In fact, the Internet has already proven itself to be a reliable means of communications under the terrorist attack conditions on 9/11.[33] Considering that the Internet was originally created as a communications tool with great resiliency in mind, especially under nuclear war conditions envisioned during the Cold War, its basic architectural concept remains sound after nearly forty years.[34] Use of secure wireless Internet that is rapidly becoming ubiquitous is a promising opportunity for enhanced

---

[32] Ellen Gordon, Transcript of Forum Presentation: "Homeland Security in the Heartland," Emergency Information Infrastructure Project Virtual Forum, 11/28, 2001. accessed April 2004.

http://www.emforum.org/vforum/lc011128.htm

[33] Jon Eisenberg and Craig Partridge, "The Internet Under Crisis Conditions: Learning from September 11," Telecommunications Policy Research Conference, 2003. http://tprc.org/papers/2003/195/net911.pdf, accessed February 2006.

[34] Barry Leiner and others, "A Brief History of the Internet", *Internet Society*, Rev. 2003. http://www.isoc.org/internet/history/brief.shtml#Authors, accessed April 2004.

public safety communications and information sharing.[35] The main problem is that most rural areas of our nation do not have wireless access and many areas do not even have wired broadband. This complicates a statewide or regional strategy for the use of Internet-related solutions for the first responder and incident command level. New technologies and policies may boost the effort to bring broadband to all areas of the United States over the next few years, with major positive implications for technology support of Homeland Security.[36]

A largely unexplored question: What is beyond the need for horizontal communications, interoperability, and information sharing among State and Local agencies? The need to provide and receive information vertically, meaning to and from federal agencies and intelligence resources outside of the local jurisdiction, has not been fully explored. Only recently, attempts have been made to provide a two-way information sharing link with the Department of Homeland Security, called the Homeland Security Information Network (HSIN).[37] Unfortunately, it is not seen as useful at the local level since it is limited to only one agency, the Emergency Management Agency, is on only one laptop, and the agency's only designated user cannot add local data to it.[38]

Review of the relevant literature review did not seem to uncover many specific answers, outside of vendor-related sales material and white papers, to the primary question of how to effectively implement new situation awareness and information sharing technologies at the local level in a highly portable and rapidly-deployable modality. At some point, there will be an expectation of first responders, incident commanders, and EOC personnel to have the ability to use basic technological skills to perform their jobs effectively. Until that time, new modalities should be explored to make the best use of the technologies

---

[35] Diane Frank, "Bringing broadband to public safety," *Federal Computer Week*, 2004. http://www.fcw.com/fcw/articles/2004/1018/feat-dcbroad-10-18-04.asp, accessed June 2005.

[36] Mark Rockwell, "Rural Carriers Key To Broadband Vision," *Wireless Week*, 2004. http://www.wirelessweek.com/article/CA440742?spacedesc=Departments&stt=001, accessed June 2005.

[37] Homeland Security Information Network, The Department of Homeland Security, http://www.dhs.gov/dhspublic/display?theme=43&content=3648&print=true, accessed December 2005.

[38] According to Doug Hamilton, Executive Director of Metro Louisville Emergency Management Agency, in personal communication with the author, 2005.

available and affordable today. Therefore, this thesis, which is based on a research project to address this issue, may uncover some unexplored ground in this area.

B. EXISTING METHODS TO ADDRESS THE PROBLEM

There are a number of technological solutions that address the problem of IT utilization in the field in regards to preparedness and response. When examining the various methods of how Information Technology is used to deliver communications, radio interoperability, Internet access, and information sharing tools in the field, there are few "one stop shops" available. They are limited to costly mobile command post vehicles or the concept of transporting several different pieces of hardware, in boxes and crates, to assemble on-site in a command post tent, trailer, or some other form of shelter from the elements.

1. Heavy Truck/Bus/RV Mobile Command Centers

In examining the typical "mobile" command center, the *transport* format for delivering the proposed solution discussed in this thesis, it is apparent that there has been a considerable emphasis on large, well-equipped vehicles that carry all the conveniences of an office. Most that are advertised in the trade journals and at emergency response trade events showcase their vast space, usually with a conference room, and the important necessities of comfort, such as heat and air conditioning, plus a rest-room and a coffee-maker. It is important for agencies to have access to this type of mobile command post for long-duration emergencies requiring days on the scene. While these behemoths of the road are a viable delivery of communications and IT tools to the field, they may be underutilized in their potential utility in favor of the creature comforts emphasized in their manufacturer's advertisements. Even if they are festooned with walls of sexy plasma display screens and sixty-foot hydraulic masts providing 360-degree video surveillance, does the jurisdiction have trained staff to operate the technology? How is it integrated into the agency's operational plans? Does it have connectivity with the outside world via broadband satellite Internet? In one recent demonstration by a leading manufacturer, they proudly emphasized the high-resolution color surveillance cameras

that covered each of the vehicle's flanks—apparently to provide early warning of any terrorists brazen enough to try to attack the command post. This manufacturer also had to provide lodging and travel expenses for a driver with a Commercial Driver's License (CDL). This requirement could impact a jurisdiction's ability to quickly field a unit in a crisis if the designated driver, and even a back-up, were unavailable due to illness or other problems.

In the past five years or so, there has been a trend toward custom-manufactured mobile command centers made by professional coach builders. Previously, most mobile command centers were built from a converted retired school bus or RV by the local agency, many times using their own labor. While more economical than a new custom-designed unit and still a viable practice, the jurisdiction has to weigh the risk of breakdowns with an older unit, a potential lack of safety features required by the Department of Transportation on commercially marketed vehicles, and no warranty on the vehicle or equipment installation. If an accurate set of "as-built" drawings and documentation are not made at the time of conversion, a malfunction may occur sometime in the future when the original builders or designers are retired or assigned outside the jurisdiction and not available to address the problem.

Another issue with a state-of-the art mobile command center—,with all the jurisdiction's information technology, communications and radio interoperability built into it as permanent fixtures—is that the vehicle could experience a mechanical breakdown or accident en route to the scene that would effectively render the technology useless when needed the most.

The average cost of today's mobile command centers is up to one-half million dollars.[39] This cost is well outside the range of affordability of many jurisdictions, especially small cities and rural agencies. Even with sharing such a resource under mutual aid, it is becoming more difficult to find the funding for the larger units coveted as a status symbol by many departments.

[39] Randall Larson, "Roomier, tougher, better: If there were an Olympics for mobile comm. centers, the latest models would be real contenders," *Homeland Protection Professional* (October 2004), 38.

2. Trailer-Based Command Centers

Another method to provide transportation of on-scene Information Technology that is less expensive than the bus or RV-based mobile command center is to outfit a trailer with the necessary electronics and set up a work area. Depending upon size, a trailer could be equipped with many of the same attributes of the large mobile command center. Some are equipped with slide-out sections that add floor space once on-scene or a large side opening with built-in awnings for fair-weather use. The advantage in pursuing this avenue is the relatively lower cost and complexity. The trailer can then be paired with any "Prime Mover," which is a truck appropriately sized and powered to tow the trailer. If the Prime Mover has a malfunction or is involved in an accident that does not damage the trailer, a substitute Prime Mover can be dispatched to pick up the trailer to go on the scene. Once on-site, the trailer can be dismounted allowing the Prime Mover to be available for other duties. This option is especially attractive as an alternative to the heavy truck, bus, or RV platform due to the cost savings, and existing vehicle assets can usually serve as the Prime Mover.

The primary disadvantage to utilizing a trailer is its difficulty in maneuvering in tight quarters and traversing rugged terrain or streets filled with debris from a disaster or terrorist attack. Special skills are also required in driving with a trailer around corners and other vehicles to prevent damage to the unit or causing an accident by turning too sharply.

3. Van-Based Mobile Command Centers

A van-based solution makes sense for some jurisdictions since they can have the equipment capacity of some of the larger units but with limited interior space for only one or two operators. The advantage is lower cost—about one-half the average heavy truck, bus, or RV solution. These units range in size from the Ford F-350 truck chassis to a larger unit becoming more popular that is based on the Dodge Sprinter chassis. The primary disadvantage is maneuverability and handling. Even though the broadcast industry relies heavily on this vehicle configuration, they do not seem to have garnered much popularity in public safety circles.

4. SUV-Based Mobile Command Centers

This solution also provides a cost-effective alternative to the heavy truck, bus, or RV solution. The Raytheon "First Responder" was the first widely-known and marketed SUV-based mobile command center, developed in the spring of 2002 as a response to the radio interoperability issues experienced between police and fire departments at the World Trade Centers after the terror attacks of 9/11. Raytheon had acquired a small company called JPS, which builds a radio interoperability switch that could be built into an electronics rack inside a vehicle. They outfitted a Chevrolet Suburban with the JPS unit, some console radios, a laptop and a satellite dish for mobile Internet, and started showing it around Washington D.C. and various law enforcement and emergency services trade shows. It was widely hailed as an innovative solution, but its more than $1/4 million price tag was still somewhat steep for the market Raytheon was trying to reach.

Raytheon appeared to use the "First Responder" as a marketing vehicle in the literal and figurative sense. It provided a delivery modality for their interoperability product, the JPS ACU-1000, and garnered much desired Homeland Security-related visibility for this huge firm best known for its military contracting. By the end of 2003, approximately $20 million dollars worth of "First Responder" vehicles were sold.[40] Even with those early sales being viewed as somewhat of a successful launch, the price prevented sales to many jurisdictions that had an interest and the need for the solution. For example, for the research team's jurisdiction, a Suburban platform equipped with the Raytheon/JPS interoperability suite and wireless Internet access similar to the solution offered in this thesis, was quoted at $300,000. To provide a lower cost alternative, Raytheon started marketing the electronics package as a stand-alone product called the MCK-1000 and would then refer the purchasing agency to an approved integrator closest to the jurisdiction to install and service the unit in a vehicle they may already own or in a less expensive used SUV they would buy locally and bring to the installer. The price after "unbundling" the electronics from the vehicle was still an astounding $146,300. Other SUV-based solutions, by specialty vehicle integrators such as AK Specialty Vehicles

[40] Brill, "After," 599.

"Command 17" and L3's "MCV," are the usual configurations with totally built-in electronics racks. They have the same disadvantage as the larger command centers, including the high cost and, if the truck is in an accident or won't start, your response is jeopardized.

5. Portable Command Centers

This configuration seems to be the least prevalent in the marketplace but potentially offers the most cost-effective solution with the flexibility to enable movement of the unit from vehicle to vehicle or even indoors, freeing the vehicle for other duties. Such a unit could also be placed in strategic locations not accessible by vehicle. Several references can be found for "portable command centers" by doing an Internet search, but the listings do not uncover more than a few systems that integrate wireless Internet access, data storage, or command relevant computer applications. For example,

- Telex-Vega offers a product that is portable and provides radio interoperability with on-scene dispatch capabilities, but does not offer other command center functions such as computer servers, wireless local area networking with Internet access.
- General Dynamics released a product in 2002 called ReadySET™ that offers a portable modular system. It can mix and match component modules to fit the needs of the agency. It does not seem to be marketed outside of the military, perhaps due to its extremely high price tag of $180,000 or more for a system providing only VoIP telephony, wireless networking, and an Ethernet switch. That pricing does not include radio interoperability or a satellite terminal.
- Cisco Systems and CACI International teamed up to place a Cisco 2700 series router and a wireless access point in a rugged travel case with a panel on the outside to plug in power and network connections. Once connected to a satellite or landline broadband connection, it can function as a Wi-Fi hotspot and VoIP phone system. This system was quickly engineered in response to the Asian Tsunami of December 2004. There is a Cisco brochure that refers to it as the MCK for "Mobile Communications Kit" but no reference to it could

be found with CACI or a distribution channel to price or acquire a unit so it is assumed that it was an engineering proof-of-concept only.

C. THE KATRINA EFFECT

The effect that Hurricane Katrina of 2005 had on stimulating national debate about communications resiliency, utilization, and redundancy in the domains of preparedness and emergency response is an excellent thesis topic unto itself. For purposes of this thesis, however, it is important to summarize the impact of Hurricane Katrina on emergency communications, and relate the data to further validate the proposed solution and concept of operations described in this thesis. For future catastrophes, the information provides a tool and method to potentially fill some of those identified communications gaps. The key finding of the House of Representative's Katrina Report, *A Failure of Initiative,* regarding communications issues, was that the lack of communications and situational awareness paralyzed command and control.[41] This is the domain that the proposed solution in this thesis is engineered to address.

The devastation Hurricane Katrina wreaked upon the communications infrastructure along a vast segment of the Gulf Coast of the United States was unprecedented. An area nearly the size of the United Kingdom was rendered without power and communications for weeks. This impacted all elements of emergency response and recovery since both landline and cellular telephone networks were either destroyed or overloaded. Central offices were flooded or main trunk lines severed. Cell and radio towers were blown down or without power or their base stations flooded. Even when a unit remained operational under back-up power after the storm passed, it later ceased operations when their batteries ran down or their generators ran out of fuel. There was no refueling capacity due to impassible roads, no power to pump fuel into supply trucks, or the base stations were in cordoned off areas where local law enforcement agencies would not allow repair technicians or supply trucks to enter, especially in the New Orleans area.

[41] U.S. House of Representatives, *A Failure of Initiative,* 191.

According to the U.S. House of Representatives Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, some sobering statistics on the impact of the hurricane on the region's communications infrastructure were revealed:[42]

- More than a million telephone subscriber access lines were put out of service in the states of Louisiana, Mississippi, and Alabama;
- Thirty-eight 911 call centers were rendered inoperable;
- Two-thousand cell sites were knocked out of service;
- Seventeen BellSouth central offices were completely down and thirty-two others had no connection to the telecommunications backbone network.

Prior to Hurricane Katrina, it was unheard of to completely lose a central office to a natural disaster due to the redundancies built into these systems, much less this number of them. BellSouth's central offices had endured the wrath of other historic hurricanes—like Hugo in South Carolina in 1989 and Andrew in Florida in 1992—without losing a single central office.[43] Since 911 call centers rely on dial-tone to the public supplied by these central offices to take their emergency calls, in addition to providing their own dial-tone, they had two points of failure to be concerned about. In the case of Katrina, many 911 call centers and, therefore, local emergency dispatchers, did not have any incoming information to dispatch emergency crews because the telephone network was down. This caused a failure in basic situational awareness and emergency response.

What can be done to mitigate the possibility of totally losing a region's telecommunications infrastructure? The weakness in the Katrina disaster was the fact that hurricanes do happen in this region and can cause flooding, but Federal, state, and local government did not adequately plan for resiliency from such a disaster. The flooding

[42] U.S. House of Representatives, *A Failure of Initiative*, 163-164.

[43] The author, as an employee, produced a corporate promotional video in 1994 for BellSouth that touted this fact as an example the resiliency of the company's telephone network.

from the failure of the levees around New Orleans actually caused more damage to the ability to communicate than the actual hurricane winds did. This too, however, was predicted as a distinct possibility.

Satellite communications proved to be the primary modality to achieve back-up communications. This communications technology not only included Internet access for sending and receiving email, but also provided access for voice telephony and radio communications. These fixed, mobile and handheld systems provided a lifeline for situational awareness and critical communications with dispatched emergency workers when the radio and cell networks were inoperable.

Aside from the obvious need for emergency workers to be able to communicate, Katrina also impacted the nation's critical energy infrastructure along the Gulf Coast. It was imperative for these damaged oil and gas companies to get the oil terminals, pumping facilities, and refineries back online to restore the flow of energy to the nation. The workers also had to be able to communicate to their corporate offices to provide situational awareness and receive instructions on priorities to address and expectations on replacement crews and equipment. One example is Valero Energy, an energy company that relied heavily on satellite communications with both hand-held satellite telephones and Voice-over-IP telephony over satellite links.[44] This enabled them to locate critical staff, communicate with the field, assess conditions, and rapidly recover from the disaster.

Voice-over-IP or VoIP, as it is commonly referred to, is a communications technology that turns analog voice transmissions into data packets that can then be sent over the Internet along with other data and re-constituted at a device such as a computer equipped with VoIP software or a phone specifically designed for VoIP operations. Consumers have been using VoIP since the early days of the Web, primarily to make out-of-the-country calls since there are no long distance charges for VoIP calls. Businesses caught on later and have been increasingly adopting VoIP switching systems that

[44] Thomas Hoffman, "After Katrina Valero Energy Turns to Satellite Communications," *Computerworld* (September 8, 2005). http://www.computerworld.com/mobiletopics/mobile/story/0,10801,104477,00.html, accessed November 2005.

leverage their investments in sophisticated data networks and broadband connections. A VoIP telephone, or even a "system" of VoIP phones, can use a satellite connection for its broadband access to the Internet, hence its value in an emergency communications strategy.

A vivid example of the value of VoIP telephone capability in a disaster was experienced during Hurricane Katrina. In a story worthy of a Hollywood script—featuring overlapping disasters of the hurricane, a tornado ripping the side off a building, rising flood waters, a crippling power and telephone outage, and hundreds of encroaching gangsters bent on pillaging their fortress—a small group of local government officials, including Mayor Ray Nagin and some of his city IT staff, used VoIP to stay connected to the outside world.[45] The Mayor and his staff of about fifteen, including some IT professionals, abandoned their city hall operations center during the hurricane for the relative safety of the nearby Hyatt hotel's fourth floor. A tornado, spun off of the hurricane, ripped one side of the building off, and the subsequent damage from winds and flooding to cell towers, generators, and phone networks left them without telephone service and in the dark for two days. When temporary power was restored to the hotel, one of the IT staff recalled that he had recently subscribed to Vonage, a commercial VoIP provider. He was able to locate a working Ethernet jack that provided Internet service in a hotel conference room (it is not clear how the Internet service to the hotel was still operational) and he was able to establish a working VoIP phone with his laptop, which served as their only link to the outside world until they performed a daring upgrade. In an "official" looting of a nearby Office Depot; the IT staff was guarded by Police Chief Eddie Compass as they appropriated several IP phones, printers, and the store's email server to return to the hotel. There they set up an eight-phone command center using the single Vonage account. The infamous phone call from President Bush to Mayor Nagin as Air Force One flew over the city was reportedly made over this tenuous, but working, connection.

---

[45] Christopher Rhoads, "Cut off: At center of crisis, city officials faced struggle to keep in touch," *Wall Street Journal*, 9/9/2005, http://www.von.org/usr_files/Katrina%20-%20WSJ%20--%20Cut%20off%20Mayors%20office%20uses%20VoIP%209-9-05.pdf , accessed November 2005.

Satellite communications, VoIP, and wireless communications were combined in an integrated fashion, referred to as "Hastily Formed Networks" or HFN, to provide emergency communications after Hurricane Katrina at multiple sites in Hancock County, Mississippi, by a group of faculty and students from the Naval Postgraduate School (NPS) of Monterey, California.[46] This opportunity to provide emergency communications and humanitarian relief, by reconstituting destroyed telecommunications infrastructure, came after Professor Brian Steckler and an NPS team had previously applied HFN in a rapid response to the tsunami disaster that occurred in Thailand in December 2004. Lessons learned from that deployment were valuable in planning their response to the devastation of Hurricane Katrina. Professor Steckler and his team of faculty and students brought in mobile satellite dishes for broadband backbone connectivity and connected that to wide-area wireless transmitters referred to as "WiMax" that fed service to localized Wi-Fi hotspots for the hospital and emergency services that had set up command posts in a parking lot. Access to the Internet, email and basic VoIP telephony was accomplished in only five hours after their arrival. As the deployment lengthened, the NPS team added antennas and access points to extend the network farther out into the disaster zone. This type of emergency communications deployment is a potential solution to the impact of major consequence events on the communications infrastructure, and further validates the concept of operations proposed in this thesis as well as how the solution can support the Incident Commander responding to such an event.

Mobile command centers using satellite access have been touted as a potential solution to emergency communications by various Katrina-related reports, and interviews with politicians and pundits. An example from the House of Representatives report, "A Failure of Initiative," illustrates the disadvantages of the typical mobile command center

[46] The author was introduced to Naval Postgraduate School Professor Brian Steckler in September of 2005 which led to discussions of mutual interests in rapidly-deployable communications and hastily-formed wireless networks. Professor Steckler and his team had recently returned from their mission in support of the Katrina disaster. This personal communication regarding his observations and an examination of his team's detailed situation reports has greatly increased the author's understanding of how to more effectively utilize these communications tools in a disaster scenario. More information and the SITREPS from the NPS HVN deployment can be accessed on the NPS website at http://www.nps.navy.mil/disasterrelief/Katrina/Journal.htm.

configuration—a brute force oversized vehicle packed with tons of the latest technology. FEMA's flagship mobile command center, a tractor-trailer called "Red October," was part of the original plan to provide emergency communications in New Orleans after the hurricane passed. Its sheer size, however, and lack of maneuverability in the debris-strewn and water-filled streets, prevented it from reaching the Superdome as ordered.[47] As a potential solution to this situation, an idea suggested for the re-vamped National Response Plan, due out after the writing of this thesis, includes a recommendation for using helicopters to deliver small mobile communications vehicles into a disaster zone or driving them in from nearby staging areas.[48] When asked by a Public Broadcasting System (PBS) narrator about the inability of people to communicate with each other after the hurricane, Louisiana Governor Kathleen Blanco stated that it was frustrating not to have a portable network in place to take care of that.[49] In addition, very strong statements were made regarding the criticality of addressing the communications and interoperability issues brought to the nation's attention—once again in Senate testimony by both Governor Blanco and Governor Barber of Mississippi.

> We saw in Katrina what the nation learned with the collapse of communications systems after 9-11. If you can't communicate, you can't coordinate. In Louisiana, we are working to acquire mobile command units and develop a statewide interoperable solution that incorporates the entire emergency community. I ask Congress to design uniform interoperable standards with dedicated funding.50
>
> Governor Kathleen Blanco
> Senate Committee on Homeland Security & Governmental Affairs
> February 2, 2006

---

47 U.S. House of Representatives, "A Failure of Initiative,"168. http://www.gpaccess.gov/congress/index.html, accessed February 2006.

48 Larry Margasak, "Government Prepares for Next Big Disaster," *Associated Press*, December 31, 2005. http://www.comcast.net/news/index.jsp?cat=GENERAL&fn=/2005/12/31/294424.html, accessed February 2005.

49 Martin Smith, "The Storm," *Frontline*, PBS Broadcast Special, http://www.pbs.org/wgbh/pages/frontline/storm/etc/script.html, accessed December, 2005.

50 Senate Committee on Homeland Security and Governmental Affairs, Testimony of Governor Kathleen Blanco, February 2, 2006, 2. http://www.senate.gov/~gov_affairs/index.cfm?Fuseaction=Hearings.Detail&HearingID=314, accessed February 2006.

Governor Blanco's specific comments and suggestions regarding communications interoperability and emergency surge capacity were echoed at the same Senate hearings on the aftermath of Hurricane Katrina by Governor Haley Barbour of neighboring Mississippi.

> Our last recommendation that I hope is obvious to everyone: The need for sustainable, interoperable communications is paramount. Areas like South Mississippi need such a communications system for its first responders, local officials and state officials, whether elected officials or state law enforcement, National Guard, etc. Inability to communicate blinds even the strongest leaders and most dedicated first responders. It hamstrings everyone from FEMA to the local constable. Congress should make establishment of a sustainable, interoperable communication system its first priority in providing resources for futures calamities.[51]
>
> Governor Haley Barbour
> Senate Committee on Homeland Security & Governmental Affairs
> February 2, 2006

D. CONCLUSIONS

The proposed solution and concept of operations defined in this thesis are uniquely designed to operate precisely in the fashion that the preceding interviews, testimony, and reports recommend—especially in relation to the communications issues faced after Hurricane Katrina. The literature validates the claim put forth in this thesis that there is a gap in the solutions offered in the marketplace for a flexible and relatively low-cost mobile communications and operations center to support the Incident Commander in the field; especially in the first critical hours of a crisis. The literature underscores the need and the opportunity for the proposed solution detailed in this thesis.

The Whitehouse Report on Hurricane Katrina, released in February 2006, made 125 recommendations for FEMA to address before the next hurricane season beginning in June of 2006. Recommendation number 37 details the recommendation of a portable

[51]Senate Committee on Homeland Security and Governmental Affairs, Testimony of Governor Barber, February 2, 2006, 11-12. http://www.senate.gov/~gov_affairs/index.cfm?Fuseaction=Hearings.Detail&HearingID=314, accessed February 2006

command and communications system that is modular, easy to use, and operational as an integrated end-to-end solution to provide enhanced situational awareness—literally the subject of this thesis.[52]

[52] U. S. Government, The White House, "The Federal Response to Hurricane Katrina: Lessons Learned," 23 February, 2006, Appendix A, http://www.whitehouse.gov/reports/katrina-lessons-learned/appendix-a.html, accessed February 2006.

III. PROPOSED SOLUTION

A. DEPARTMENT OF HOMELAND SECURITY GRANT OPPORTUNITY

On 4 November 2004, Tom Ridge, Secretary of the Department of Homeland Security at the time, announced the *Kentucky University Homeland Security Consortium* in a press conference in Somerset, Kentucky.[53] This concept of a "virtual" Homeland Security-focused National Laboratory was comprised of the combined resources of the public and private universities, colleges, and community college system of the Commonwealth of Kentucky in collaboration with the private sector. The virtual lab idea was the brainchild of Kentucky's 5th District Congressman Harold (Hal) Rogers. As Chairman of the Homeland Security Appropriations sub-committee, Chairman Rogers was keenly aware of the national need to tap the intellectual capacity of academia and the ingenuity of high-tech businesses in the fight against terrorism. His vision and persistence led to the initial proof-of-concept funding of $4.5 million, which grew to a $9 million research funding pool in the following year.

This innovative program, managed by the National Institute for Hometown Security, publishes a list of prioritized technology needs or projects that the DHS is willing to fund to the various post-secondary institutions in the state. The focus is on funding applied research which consists of concepts or technologies that can be developed in a prototype operational model in less than a year, and rapidly commercialized by private industry very soon after the proof-of-concept is demonstrated to work. The requested solutions or desired capabilities, provided by DHS for this program, target applications that can be quickly fielded and commercialized to support the protection and resiliency of our nation's critical infrastructure.

The incentive for these educational institutions to collaborate on these grant opportunities is, of course, research funding. Many researchers have also expressed a sense of value in becoming engaged in an important contribution to our nation's security.

---

[53] Transcript of public speech by former Department of Homeland Security Secretary Tom Ridge regarding the establishment of the Kentucky Homeland Security University Consortium, http://www.dhs.gov/dhspublic/display?content=4099 , accessed March 2005.

In fact, this program has done more, in the past two years of its existence, to foster collaboration than any other academic edict from the state higher education regulatory bodies. Even though there are only two formally-recognized research institutions within the Commonwealth of Kentucky—the University of Kentucky and the University of Louisville—there are many subject-matter experts and centers of excellence in the state's regional universities and private colleges that have made this program a success. Aside from the actual applied research, the Kentucky Community and Technical College System (KCTCS) can contribute to the training of the knowledge-workers who would operate the commercialized technologies created by scientists and engineers in the higher-degree granting institutions. This network already trains first and second responders sanctioned by the National Fire Commission.

The involvement of the private sector is critical to achieving the end-result desired by DHS—the rapid manufacturing, marketing, distribution, and servicing of the needed technologies. This emphasis also benefits the Commonwealth's initiatives to create and foster a knowledge-worker economy. If the research funded by the program results in new job creation, either by licensing the technologies to new start-up ventures or existing industry, it will greatly benefit the economic development goals of the state. This is particularly true in Chairman Rogers' district, where a desperate attempt is under way to transition from a coal mining and farming economy to a high-tech economy by workforce training and new opportunities.

The author, as Director of The University of Louisville's Information Technology Research Center for Homeland Security (iTRC/HS), submitted a proposal to create a rapidly-deployable and interoperable communications system, and its concept of operations strategy, in response to the first proposal solicitation. The submission was in response to DHS's stated need for radio interoperability and communications technologies. The iTRC/HS and the author, as Principal Investigator, were subsequently awarded a research grant in the amount of $380,200. The approved grant budget allocated approximately $150,000 for equipment acquisition, including the vehicle to transport the electronics suite and a mobile satellite dish. Approximately $60,000 went toward outside consulting and engineering design of the electronics suite, and the remainder toward

iTRC/HS staff salaries for effort expended on the research and the university-required Facilities and Administration overhead fees.

This first phase of the research grant was to establish a baseline test-bed capability utilizing Commercial Off-The-Shelf (COTS) components and software that, the team concluded, provides the best cost/performance ratio. The research team based its findings from on-scene and laboratory tests utilizing loaned and demonstration equipment from interested vendors in a series of real-world exercises and deployments.

One of the requirements of this grant was to provide DHS with a written progress report on the research findings and milestones achieved every three months, plus a mid-project progress report presentation to the DHS Science and Technology Directorate. This program was clearly designed with an expectation of tangible performance in an application suited for the real world, as opposed to a "Bunsen-burner" science project that would only see the lab—and never the light of day.

Based upon the successful prototype created in its initial research grant, the iTRC/HS was awarded a $730,800 follow-up grant in January of 2006. Provided by the DHS through the Kentucky University Homeland Security initiative, the grant would continue the project by fine-tuning the electronics package and adding additional capabilities, such as remote sensor and a low-cost Unmanned Aerial Vehicle (UAV), over the subsequent two years.

B. THE MAN-PORTABLE INTEROPERABLE TACTICAL OPERATIONS CENTER (MITOC)

The proposed technology solution that was accepted for funding and ultimately became the focus of this thesis is called the MITOC, which stands for *Man-portable Interoperable Tactical Operations Center*. Like most other security-related technology devices or programs, the research team proposed a name that implies performance under field conditions and specifically identifies its most important attributes requested by the DHS, for example:

1. Man-Portable

The attribute of being light enough for a two-man lift of the primary MITOC component is one of the key advantages in the entire project. Typical mobile command posts are custom-fitted with their communications and other electronic equipment. The systems are usually integrated into the vehicle as semi-permanently installed items and are not meant for removal except for repair or replacement. The Man-portable aspect of the MITOC allows ultimate flexibility in transportation options and, more importantly, easy reallocation to a back-up vehicle if the primary carrier is disabled for some reason.

2. Interoperable

This attribute refers the communications, computers, and software on board being able to connect and share information within other communications and IT applications within a local jurisdiction as well as with other agencies expected to be involved in the prevention or response activities of the MITOC. The issue of radio interoperability, addressed in some detail later, has been a highly contentious subject over the past ten years, after the inability of police and fire assets to communicate over incompatible radio frequencies during the aftermath of the terrorist attacks at the Oklahoma City Murrah Federal Building bombing in 1995, and the World Trade Centers on 9/11. Software applications such as Geospatial mapping, document and image sharing, or live instant messaging to provide real-time information sharing, are all attributes of an "interoperable" system. The computer and software platforms have to be chosen with compatibility in mind for both hardware and software. The MITOC design philosophy takes all these elements into consideration.

3. Tactical Operations Center

This is a military-sounding term, but it was chosen for its crystal clear connotation: that the MITOC is intended to be utilized as a "tactical" tool in the field during a crisis or under adverse environmental conditions—as opposed to a climate-controlled data center. The "Operations Center" descriptor is intended to illustrate that the MITOC is more than a set of radios, even if they are interfaced with an

interoperability system. It suggests the ability to be self-sufficient in the field with the IT and communications tools to provide visual, verbal, and transmittable data information both at the scene and externally.

The idea of the MITOC's design approach and innovative features stems from ongoing discussions that began in mid-2003 with MSgt John "Al" Staples, a communications specialist with the 41st WMD Civil Support Team (CST). His CST utilized a heavy truck platform for its mobile command post. MSgt Staples suggested that the UofL Homeland Security research center should work on delivering best-of-breed interoperable communications and wireless Internet capability that could be carried in an affordable SUV platform, as opposed to the large bus and RV chassis mobile command centers that are the dominant platform. Being an expert in mobile communications and an enthusiastic seeker of the latest technology advances in the field, MSgt Staples has been an invaluable contributor to the MITOC research program since its inception. He also introduced the research team to Ramon Abelleyro, a nationally-recognized expert in radio interoperability and mobile communications systems designer who was ultimately chosen as the lead design engineer and external consultant for the project.

Mr. Abelleyro was the outside consulting project engineer on the first known robust mobile command post based on an SUV platform that was developed by Raytheon. The "First Responder" vehicle was developed to address some of the communications deficiencies experienced during the aftermath of the 9/11 attacks at the World Trade Centers in New York City.[54] Mr. Abelleyro's experience with this ground-breaking platform and his own mobile communications systems laboratory provided the research team with time- and money-saving concepts as well as improvements on previous designs that were incorporated into the MITOC design.

[54] Brill, "After," 467-468.

Figure 1. MITOC Capabilities Diagram

4. Design and Features

a. Portability

The notion to have the electronics suite portable enough to be transported in a variety of common ground vehicles, such an SUV or pick-up truck, as well as rescue-type boats or helicopters, came from similar attributes of rapidly-deployable military field equipment. Years of battlefield-tested design has proven that the flexibility and portability of gear housed in rugged cases and designed to be lifted by one or two soldiers made logistics a lot easier. Heavy equipment loaders such as forklifts are a luxury not typically found outside of airfields and supply bases. Therefore, the housing and systems configuration of the MITOC electronics suite was chosen to allow a safe two-person lift to tailgate height without special mechanical assistance. Subsequent designs are exploring further minimizing the size to a one-man lift by using a modular approach with two cabinets instead of one larger one. Related components would be linked wirelessly.

b. Rugged Construction

The MITOC case housing, from SKB Industrial Cases, was chosen after evaluating the cost and features of several transit case manufacturers.[55] The current design was less expensive than competing models and very adequate in regards to external load bearing. It featured easily removable covers, both fore and aft, and molded-in handles that made lifting more manageable in tight spaces. The chosen design was a 14U rack capacity configuration that slides directly into the rear cargo bay of most full-size SUVs, such as the Chevrolet Tahoe and Suburban, as well as the Ford Expedition and Excursion. These models are the most common SUVs utilized by emergency response and law enforcement agencies. The SKB case is constructed of nearly indestructible roto-molded plastic and has a rugged "electrometric" shock mount system for the internal rack that protects the electronic components from shock during transport. The research team's engineer, however, found that the rack design lacked adequate rear support for longer components. Therefore, he fabricated a custom-designed aluminum bracing cage that integrated into the rack to reinforce the internal structure.

c. Energy Management and Power Module Design

Supplying electrical power to portable electronic systems is one of the most difficult tasks to balance in a project like this. Every added component either shortens the battery life during a mission or increases the capacity needs of the power generation module requiring larger, more expensive power generating equipment and inverters.

The original energy plan called for a 600-watt inverter/charger mated with three Optima "Bluetop" deep discharge gel-cell batteries to power the electronics suite. At least one 12v DC battery is necessary to run the radios, and the other components are 120v AC. The battery pack serves a dual purpose in that the entire unit can run off the battery pack because the inverter passes the proper voltage to the radios and other components. This allows the batteries to serve as a buffer from "dirty" AC power off a

[55] SKB website, http://www.skbcases.com/industrial/product/racks/rk1-us.html accessed January 2006.

basic generator or surging power due to instability in the grid. It also allows for an hour or so of full battery back-up power if the power grid fails while the unit is being used indoors, or if you have to re-fuel the generator while being used in the field. The inverter was initially installed inside of the SKB transport case and the batteries were outboard next to the case. A small Honda generator, rated at 900 watts, also ran outboard of the unit to keep the batteries charged, using very little fuel in the process.[56]

This configuration has proven to be unworkable for several reasons:

- The inverter/charger combo unit made the SKB case too heavy.
- The tight fit in the case resulted in overheating of the inverter and a subsequent automatic shutdown during a mid-summer test mission.
- A later test mission that added the outboard command post elements—six Cisco VoIP telephones, six HP laptops, and one HP printer/scanner/fax machine,—overtaxed the inverter/charger and batteries, requiring a separate power cable from the generator directly to the phones and computers.
- The batteries are bulky and heavy, requiring them to be transported one or two at a time. The other issue the research team is currently addressing is the safety issue of loose batteries inside the support vehicle. Some sort of sealed housing vented to the outside will have to be fabricated, one that also allows for easy change-out of the batteries or removal from the vehicle.

d. Solving the Problem

A basic miscalculation regarding the energy draw of the laptops threw off the energy balance. Further investigation found that manufacturer's listed rating assumed that the laptops were already fully charged while, in actual field conditions under load, they were drawing far more. This required a rethinking of the energy management plan and the power module. Being on a tight budget, the project did not have much money to work with and set about looking for a more powerful inverter/charger combination and a safe housing for the batteries. The most attractive solution for a rugged inverter/charger combination unit was from a defense supplier called Tactical Power Systems. Their unit that met our specifications was well over $3,000. The grant would not cover that, so, for

[56] Honda Generator website, http://www.hondapowerequipment.com/ModelDetail.asp?ModelName=eu1000i, accessed January, 2006.

only $700, a much larger 5.5Kw generator was acquired that can power all the equipment with a wide margin—in case there is a need to provide power to some other emergency gear during a deployment.[57]

The massive infrastructure collapse that occurred over such a wide area after Hurricane Katrina in 2005 set the bar for a fresh look at how energy should be addressed for the MITOC. In the first week or so of the Katrina disaster, response agencies could not assume gasoline and diesel fuel were available anywhere in the affected area, either for vehicles or generators. The mutual aid and EMAC (Emergency Management Assistance Compact) response crews from outside the area were advised to bring their own fuel. This illustrated that the MITOC concept of operations had to factor in fuel availability in every contingency: whether it is to be deployed in a future wide-ranging catastrophe scenario like another series of devastating hurricanes, a massive earthquake, or other protracted emergency affecting the fuel supply chain like a pandemic outbreak or fuel shortages due to terrorist attacks on our energy infrastructure.

Our current power module also tested the incorporation of a loaned 2.5Kw inverter/charger equipped with two 90-watt solar panels. Even though its configuration and housing is too bulky for the final recommended design, it has proven to be a reliable power supply; the solar system can keep the batteries charged, but it does not quite provide enough power on its own for the entire system under full load. Two additional 90-watt solar panels would serve that purpose, or even the supplemental power from the economical Honda genset would allow for extended deployments without the need for much gasoline. This aspect of the research project will receive much more attention in the subsequent phases.

The recommendation for the final design of the energy management system is still under study. A potential solution would be to use a special on-board generator that runs off the SUV engine. This system could also incorporate interior and exterior 120v outlets, for maximum flexibility at an on-scene Command Post. The installation of a second battery that is always charged by the system could serve as the

[57] Briggs & Stratton Generator website, http://www.hondapowerequipment.com/ModelDetail.asp?ModelName=eu1000i, accessed January 2006.

radio power supply. There are two major manufacturers of this type of generator. The research team was considering a unit from Auragen since there is a local distributor/installer.[58] An issue worth further consideration is that the company is currently petitioning for bankruptcy, and this solution does not come cheap at around $6,000, plus installation. The project is also considering a competitive system from Atlantic Power Solutions.[59] The small Honda genset could still be carried as a back-up, and the solar panels could be integrated into the roof-top module to fold out on deployment to also provide a back-up power source in the event the support vehicle ran low on fuel. The issue of on-board energy generation is also being intensely researched by the military, since generators are heavy and noisy, while batteries are also heavy and have to be continuously charged by a gasoline or diesel power source.

5. The Basic MITOC Electronics Suite

The MITOC electronics suite has been continuously evolving since the beginning of the research project. The goal is to have an integrated package of complementary systems that provide a public-safety oriented set of capabilities to support the Incident Commander, and a small Incident Command Post with the following Commercial Off-The-Shelf (COTS) capabilities housed within the SKB transport case:

- Radio base stations compatible with the user's jurisdiction
- Radio Interoperability to support the radio frequencies utilized in the user's jurisdiction and surrounding mutual aid agencies
- An Internet router with an integrated VoIP telephone switch
- An Internet server
- A wireless local area network
- A keyboard/controller with a daylight viewable monitor screen
- Panels for phone jacks, antennas, and power
- Cooling fans
- Speakers

---

[58] Auragen vehicle generator website, http://www.aurasystems.com/, accessed January 2006.

[59] Atlantic Power Solutions website, http://www.vehiclepower.com/index.html, accessed January 2006.

a. Radios

The design concept of the MITOC is to keep all of the components modular and interchangeable for maximum flexibility. The radios utilized in the commercial versions of the MITOC should be customized for each client since they may use different radio models than the jurisdiction the prototype supports in Kentucky. The research engineers chose four Kenwood radios that represent the primary public safety frequencies used in the United States. The unit is equipped with both a base station and a handheld for 50 MHz, 150 MHz, 450 MHz, and 800 MHz. Space in the transit case rack representing one unit (1U) could be saved if only two radio base stations were needed.
Another radio technology, used for data transmission, has been successfully trialed in the MITOC project. The research team used 900 MHz transceivers for relaying the Internet backbone from the satellite dish to the MITOC unit at a remote location. Another application for such a radio is to transmit Local Area Network (LAN) connectivity to remote users away from the primary MITOC wireless "bubble."

b. Radio Interoperability

This is perhaps one of the most important capabilities of the MITOC because radio interoperability is arguably the most recognized and targeted problem area in public safety communications. There are a number of solutions in the market that can take the analog audio output of a radio, basically the sound coming over the wires to the speaker, and input that signal into some sort of switch or matrix to allow different radio channel signal outputs to be heard by all parties using either channel.

Current state-of-the art interoperability systems convert the analog audio output of the radio desired to be interconnected into a digital signal allowing more flexible manipulation of the transmit/receive audio. In the case of the system chosen for the MITOC prototype, the digital signals are further processed into Internet Protocol (IP), which consist of packets of information. These packets, essentially disassembled snippets of the original information (the Incident Commander's voice, for example), are then routed to the desired destination within the switching matrix just like email over the Internet. By distilling all audio signals coming and going throughout the system, the IP-

based interoperability also allows the flexibility of mixing non-radio audio signals such as cellular or satellite telephone calls. In theory, the Governor of Kentucky could be on a telephone at his desk and speak directly to someone at the scene over a handheld radio through this system. There are several well-known and equally serviceable interoperability systems the project team considered for the MITOC. Each system has certain feature or price benefits that may better fit a local jurisdiction's needs. The project team elected one of the more expensive systems, the Telex-Vega IP-223, due to its flexibility and capability to serve as an on-scene tactical dispatch systems.[60] Depending upon local jurisdiction needs, a small tactical interoperability system called the ACU-T from Raytheon/JPS Communications may be the best solution.[61] The ICRI from C-AT is a similar system that could work within the MITOC configuration.[62]

One of the most important facts we discovered in the research was that vendor marketing department promises of rapid and easy connections between dissimilar radios are somewhat overstated for the current technologies being fielded. Radio Interoperability is not yet "plug-and-play," at least not in an ad-hoc fashion under duress in the field, without some careful pre-planning. Ideally, to better ensure interoperability at the scene, an agency should pre-program the frequencies, PL tones, side-tones, and sometimes other esoteric nuances that are native to the radio systems in the other local agencies they expect to work with, or neighboring jurisdictions that would respond under mutual aid. The worst-case scenario would be a situation where no agency radios at the scene have been programmed into the interoperability system. Some radios require custom-made "pig-tails" to connect them into the programming capability of the system. The various "pig-tail" connectors for the many different hand-held radios manufactured on the open market are difficult to obtain—or build from scratch in the middle of the night when it is raining and the chemical plant is about the blow up. Someone also has to tell the radio technician the exact frequencies, codes, and other nuances of the alien radios to program into the system, or radio interoperability is not going to happen.

---

[60] Telex-Vega website, http://www.vega-signaling.com/RadioDispatch/products.nsf/pages/VIPER_Custom_Configurations, accessed January 2006.

[61] JPS website, http://www.jps.com/downloads/PDFS/ACUT.pdf, accessed January 2006.

[62] C-AT ICRI website, http://www.c-at.com/icripages/icri.html, accessed January 2006.

More importantly, radio interoperability is only effective if you also set protocols that all connected agencies would follow regarding good radio channel allocation and rules for proper use. For example, you need a mutually agreed upon plan as to tactical channel assignments to keep from overloading a bridged channel and the determination of whether or not you will be using standard English as opposed to 10-codes or other proprietary verbal shorthand that may not be used in other agencies on the scene. In addition, incorrect configuration of an interoperability system could lead to too many users being interconnected, thereby cluttering the bridged channel or potentially causing feedback over radio repeaters if the systems are not balanced correctly.

The MITOC project is currently seeking additional funding to explore a new type of technology that could get closer to "plug-and-play" for radio interoperability. Software-Defined Radio (SDR) has been demonstrated by the alien radio being keyed near the console, thereby allowing the system to then read that into a software program that essentially "clones" that frequency. The voice traffic can then be manipulated and combined within the interoperability switch. The military is trialing this technology now and it may become commercially available within the 2006 to 2007 time frame.

Another radio technology of interest for future MITOC research is called "cognitive radio." This type of radio technology constantly scans for available frequencies and appropriate bandwidth and then transmits traffic in a burst of signals over whatever clear frequency it finds. Software inside the unit decrypts the transmissions on the various frequencies for delivery to the user. This is somewhat farther out on the horizon than the previously described Software-Defined Radio, but incorporates some of its architecture. If this type of radio were to replace the legacy units now in service, there would be no need for an interoperability solution since dedicated frequencies would no longer be needed.

c. Internet Router

A router is needed in any Information Technology application where you have one connection to the Internet shared by more than one user. It takes the local area

network traffic signals and routes those outgoing requests to the Internet, and routes incoming responses, such as downloaded web pages, email, or other data, to the users. After evaluating several other configurations, the MITOC utilizes the Cisco 2811 series router,[63] chosen for the following reasons:

- Its small form factor only takes up 1U of rack space
- It incorporates built-in network security, including Virtual Private Networks (VPN), that provide high security and encryption of network traffic as well as anti-virus and firewall applications
- It incorporates Cisco Call Manager Express VoIP telephony that can support up to 36 VOIP telephones without an additional telephone switch in the rack.[64]

Cisco was chosen for the core of the network application because of the market dominance of the Cisco product line. This drives a high number of "Cisco-certified" technicians to draw from. This is especially true in Kentucky because of an aggressive placement and subsequent success of Cisco Network Academies across the Commonwealth in the Kentucky Community and Technical College System (KCTCS) educational network. The ubiquity of the Cisco product line also may ensure that service and maintenance parts will be available on a faster turnaround than an off-brand network solution.

d. Internet Server

A server is needed in the MITOC network to serve as a host device for applications accessed by the users. For example, when a user requests map imagery that contains large files, the server buffers the request and stores the material on-site for faster refreshing of the user screens upon subsequent requests. It also acts as the interface controller, resident storage, and computing device for the technician to control the satellite dish and router, and to perform modeling and computing functions. The design team chose the Supermicro server for its price and performance.[65]

---

[63] Cisco 2811 router website, http://www.cisco.com/en/US/products/ps5881/, accessed January 2006.

[64] Cisco Call Manager Express website, http://www.cisco.com/en/US/products/sw/voicesw/ps4625/index.html, accessed January 2006.

[65] Supermicro, Inc. server website, http://www.supermicro.com/products/system/1U/?typ=P4, accessed January 2006.

e. Wireless Local Area Network (Wi-Fi)

One of the most important features of the MITOC is the ability to provide a "bubble" of secure wireless Internet access around the support vehicle or MITOC (if placed inside a building.) This wireless network also can provide access to authorized users to the on-board applications of the MITOC. Aside from the six wireless-equipped laptop computers carried on-board the support vehicle, an Incident Command Post supported by the MITOC can allow other authorized wireless-equipped laptops and/or PDA devices to log onto the MITOC's network. This is the core capability of *data interoperability.* This utility allows on-scene collaboration with instant messaging among disparate agencies, reducing some of the radio traffic, especially for longer discourses that all users may not need to hear.

The MITOC once again uses Commercial-off-the-shelf Cisco 2.4GHz access point equipment for the wireless network due to its low cost, reliable performance, and ease of set-up. The research team also tested proprietary "mesh" networking systems that have some interesting features and a higher "survivability" rating than the Cisco commercial systems. The tens of thousands saved by using the more basic system, however, can be put to better use elsewhere in the configuration. The project will continue to investigate "mesh" wireless systems, including Cisco's new Aironet 1500 series Mesh product.[66] Rajant's redesigned Breadcrumbs units will also be trialed in the future.[67] As configured, the research team has measured an effective outdoor transmission range of around 1,500 feet in flat terrain, which is acceptable for most deployments. Higher external antenna placements could increase the range and will be a subject of future performance testing.

f. The Voice-Over-IP (VoIP) Telephone Switch

As stated in the description of the Router, it contains an optionally integrated VoIP telephone switch, called the Call Manager Express, which saves 1U or

---

[66] Cisco Aironet website, http://www.cisco.com/en/US/products/ps6548/index.html, accessed January 2006.

[67] Rajant Breadcrumbs website, http://www.rajant.com/index.html, accessed January 2006.

more of rack space and provides a flexible telephone system that can support up to 36 stations, either desk models or handheld units. Having a robust telephone system for your Incident Command Post is a benefit not found in most mobile command posts, even the large RV or bus-based units. It allows the IC team to work together simultaneously to reach the outside world for resources, and to provide situational awareness to dispatch the EOC or other entities. It allows for private conversations between ICP members and first responders in the field equipped with handheld units. The VoIP capability also provides needed phone services in the event of a major incident that affects cell phone service, such as a hurricane or other major disaster. Even large special events, like the Kentucky Derby, saturate commercial cell phone service to the degree that even Nextel cell phones, the most prevalent brand in public safety, are useless.

The VoIP telephone system reaches out via the broadband satellite dish and actually pulls its dial tone from a land-line telephone company central office switch in another location. The MITOC pulls its dial tone from the University of Louisville telephone switch. To account for all contingencies; it would be prudent to engineer the dial tone to come from a stable land mass distant from the local jurisdiction. Using that configuration, a regional event, like a hurricane or earthquake would not affect the dial tone from a central office across the country, thereby ensuring telephone service for the deployed MITOC. The distance makes no difference to the satellite connectivity but, since the signal has to go 22,500 miles into space and back, there is a short delay, called propagation delay, experienced at the beginning of the call.

The MITOC's VoIP connectivity is designed to be a somewhat robust connection that can provide service for a minimum of four simultaneous conversations via its twelve-phone field communications system, while simultaneously supporting Internet and fax access.

g. Controller Terminal

The MITOC is equipped with a 1U rack-mounted screen and keyboard terminal that stores in a closed mode within the rack for transport, and slides out for keyboard and screen viewing during deployment. The technician or user can use this

terminal to control all aspects of the MITOC including configuration or trouble-shooting of the satellite deployment, wireless LAN, server, router, VoIP sub-system, application software and network security. This unit is also equipped with a daylight viewable screen, which is critical for outdoor viewing in even moderate sunlight that makes viewing of the screens of ordinary laptops or PCs virtually impossible.

h. Ancillary Support Equipment External to the MITOC's SKB Case

The following items are carried separately in rugged transport cases or other appropriate transport for tactical use:

- (6) HP laptop computers configured with 512k of memory and built-in security featuring auto-encryption of the hard drive, to protect data if stolen, and built-in Wi-Fi capability.
- (6) Cisco VoIP desk model 7960 series telephones that can serve as the Incident Command Post's communications system or even an ad-hoc EOC environment.[68] These phones can be used in the field under a folding canopy (summer) or with additional side curtains (winter) on a folding table. All this can be transported with the MITOC on the support vehicle. One or two desk units can even be used inside the MITOC's support vehicle in the mid-cabin Incident Commander's pod.
- (6) Cisco VoIP handset model 7920 series portable phones that can be used in tandem with the desk models in the ICP or an EOC-like environment.[69] Their range can extend approximately 1,200 feet from the MITOC, allowing the ICP team personnel to roam near the ICP and still remain in contact without having to tie up a radio channel. This connectivity also provides privacy since the IP phone traffic is encrypted and cannot be monitored by scanners, unlike public safety radios.
- A Columbia Weather Systems portable weather station that can be quickly set up near the incident scene to wirelessly transmit on-scene weather data, such as wind direction, speed, and barometric pressure, to the MITOC for automatic integration into its on-board plume dispersion modeling software.[70] This allows quicker and more accurate assessment of the "hot-zone" for the Incident Commander to better plan response agency staging locations,

---

[68] Cisco 7960 desk VoIP phone website, http://www.cisco.com/en/US/products/hw/phones/ps379/ps1855/index.html, accessed January 2006.

[69] Cisco 7920 wireless VoIP handset phone website, http://www.cisco.com/en/US/products/hw/phones/ps379/ps5056/index.html, access January 2006.

[70] Columbia Weather Systems website, http://www.columbiaweather.com/, accessed January 2006.

evacuation routes, and response strategies. Utilizing weather data for plume modeling and prediction from sources such as weather radio, airport weather, NOAA weather, or other remote providers, could result in a disastrous miscalculation of which way the wind is blowing near the site. This is because the wind speed and direction could be drastically different at other collection locations away form the incident scene, making this a critical response tool in hazmat responses or terrorism attacks involving WMD or HAZMAT-related releases that could spread aerially.

- A Globalstar FAU-200 satellite telephone antenna that allows for up to three standard single-line telephones to be plugged into the antenna unit for phone calls or a data connection providing 9.6 Kbps data rate for email or fax use was tested during several deployments.[71] This antenna can be mounted on the support vehicle for in-route use or at the scene for back-up to the main satellite dish during initial set-up or if a malfunction occurs in the MITOC satellite sub-systems. Redundancy, even at the relatively low speed of this system, is critical since breakdowns will occur at the most inopportune times.

- A Verizon Broadband Access PC Card is utilized for Internet access while en route to the incident scene, or as another redundant back-up connectivity path aside from the main satellite dish in the event of system failure or conditions unsuitable for the satellite dish deployment.[72] Inserted into a PCMCIA slot in a laptop PC, this card can allow Internet access at speeds of 700-800 Kbps nominally with higher bursts of speed under optimum conditions. This service is available in most major markets and is slated for nationwide coverage, according to Verizon's marketing literature. Even in non-broadband mode, it can receive Internet access at speeds comparable to residential dial-up service (around 40 Kbps), which allows for email access, instant messaging, and limited web access. The service is affordable at around $150 for the card itself, and $80 per month for the service plan. Other cellular carriers have similar service offerings and are discussed later in this thesis.

- An all-in-one printer-fax-copier-scanner is currently transported with the MITOC and can be accessed by any PC on the wireless network. Many times, a paper document, list, or map is preferable to the Incident Commander than a digital image—as described later in this thesis. The unit is attached in the mid-cabin of the support vehicle for field use and can be easily removed to accompany the MITOC if utilized in an indoor EOC-type deployment.

---

[71] Globalstar satellite telephone website, http://www.globalstarusa.com/en/products/prod_display.php?id=3, accessed January 2006.

[72] Verizon Broadband Access Card website, http://www.verizonwireless.com/b2c/promotion/controller?promotionType=miniPac&action=miniStart, accessed February 2006.

i. Software Tools Utilized and/or Tested by MITOC

GIS (Geospatial Information Systems) mapping software was provided for several MITOC demonstrations by Plangraphics STEPs on a custom-built basis.[73] LOJIC was used as a free local resource available in the research team's jurisdiction.[74] Google Earth can be accessed by virtually any late model PC with broadband Internet access.[75] All these tools provide varying capabilities to include:

- Identification of potential problem areas near an incident scene, such as schools, residential areas, hospitals, and nursing homes;
- Identification of transportation routes for evacuation, equipment staging, and road blocking;
- Locations of Critical Infrastructure sites that could be affected, such as power generation/transmission, telecommunications, water, or government;
- Location of watersheds that could be adversely affected by toxic run-offs from a hazmat incident;
- Location of industrial sites near the incident scene that could contain volatile compounds or other hazardous substances;
- Automatic Vehicle Location (AVL) to track and pinpoint locations of other vehicles utilized in the deployment.

Incident Management Software called "Watch Command," provided by L3 Communications, was tested in two major MITOC demonstrations. The research project will evaluate other similar software at a later date including WebEOC, DMIS, and EM2000. The "Watch Command" application provided:

- Incident logging and tracking
- Situation Reports (SITREP) documentation and sharing
- Central database and shared resource for NIMS documentation

Collaboration Software called "STEPs" was a prototype application provided by the Plangraphics STEPs software. The project will evaluate similar

[73] Plangraphics STEPs website, http://www.plangraphics.com/smartmart/smartmartapplicationpage_steps.htm, accessed February 2006.

[74] LOJIC website, http://www.lojic.org/apps/index.htm, accessed January 2006.

[75] Google Earth website, http://earth.google.com/, accessed January 2006.

applications called Groove and Homeland Security Information Network (HSIN). In this application, STEPs provided:

- Real-time collaboration among responding agencies, both on-scene and remote
- Sharing of documents, images, maps, and video
- Real-time "chat" or "Instant Messaging"

Imagery Software to enable visualization of the physical area around the incident scene was tested. "Pictometry," provided by Pictometry International,[76] provided:

- High-resolution imagery from recent aircraft flyovers
- 45-degree oblique views in addition to orthographic (overhead) views
- Ability to mark-up and share images,

Integrated emergency operations software was provided by the Environmental Protection Agency (EPA) called "CAMEO".[77] It provides the following capabilities:

- Computer-Aided Management of Emergency Operations
- Marplot – Mapping applications
- ALOHA – Plume dispersion modeling
- Chemical Reactivity Worksheet (volatility and effects of combined chemicals)

HAZMAT database software called "WISER" was provided by National Library of Medicine; it can be loaded into a laptop or desktop computer as well as a PDA.[78] WISER provides:

[76] Pictometry website, http://www.pictometry.com/, accessed January 2006.

[77] EPA CAMEO website, http://www.epa.gov/ceppo/cameo/what.htm, January 2006.

[78] WISER website, http://wiser.nlm.nih.gov/about.html, accessed January 2006.

- Chemical database by name
- Medical advice on exposures
- Effective response guidance

Intelligence resources for sensitive but unclassified (SBU) information can be provided to the MITOC via sources such as FBI Infragard, RISS/ATIX, Northeast Intelligence Network, CyberCop, LEO, and the Critical Infrastructure Report and Daily Brief from the Department of Homeland Security. These are all subscription-based services with differing measures of security and access. Some services such as LEO and FBI Infragard utilize VPN (Virtual Private Networking) for security, which is currently problematic for use over the satellite network due to the propagation delay. When utilized, these non-classified services can provide the Incident Commander with:

- Regional and National Alerts
- Listservs on specific subject areas
- Encrypted email capability
- Database resources
- Open-source news compilations

An Emergency Medical and Public Health software package was provided by EMSystem.[79] This system is able to provide MITOC users with:

- Emergency Room patient diversion status
- Hospital bed status
- Medical alerts
- Public Health alerts

Video surveillance for the local MITOC project's jurisdiction was provided by Northrop-Grumman TRIMARC, which is the local traffic camera network.

[79] EMSystem website, https://www1.emsystem.com/, accessed January 2006.

MITOC's on-board streaming web cameras, both fixed and wearable, have been utilized in a surveillance mode. These cameras have been utilized to:

- Monitor traffic flow, which would be beneficial during evacuations or other incidents;
- Conduct covert mobile surveillance;
- Share situational awareness with other agencies and the EOC/JOC.

Videoconferencing has been tested with standard streaming webcam video in initial trials; specific videoconferencing systems will be evaluated at a later date to provide:

- Real-time interactive collaboration
- Telemedicine
- Input local video feed for remote situational awareness

National Power grid monitoring is provided by Genscape; however, this is a specific license for use by the iTRC/HS in research and may not be cost-effective for individual agency use.[80] The Genscape product provides:

- Real-time status of energy grid interconnections
- Real-time status of individual power plants
- Identification of power supply of individual plants
- Regional real-time weather

6. Applications

The MITOC is designed from the ground up to be extremely flexible and modular in both its software and hardware elements. This allows for a variety of "modules" to be pre-configured for different applications, different vehicle support platforms, or even different types of Incident Commanders or a similar role, whether in the public or private sector. Software applications are generally limited only by the ability of the user to afford or obtain support in their jurisdictions. The prototype MITOC relies on a suite of

[80] Genscape website, http://www.genscape.com/na/index.shtml, accessed January 2006.

software applications and an equipment configuration that is unique to its jurisdiction. The current configuration runs under the Windows Operating System and incorporates the software and hardware elements that represent a broad user appeal for typical public safety applications. This inherent flexibility in the MITOC's architecture allows a jurisdiction to utilize the software applications that makes sense for them, rather than being tied to a specific vendor's solution for GIS, Incident Management, or Collaboration tools.

a. Vehicle Support Platforms

Also, it is important to reiterate that the MITOC is not intended to be just another mobile command post. As previously mentioned, most of those are fixed configurations in specific public-safety focused vehicles;—mostly large heavy truck, bus, or RV chassis costing hundreds of thousands of dollars more than the typical MITOC configuration, even when the MITOC is paired with its support SUV. The main take-away from this thesis should be that the MITOC can go in almost *any* vehicle—from Compact SUV or Pick-up truck, on up to include the most common full-sized SUVs favored by public safety agencies. The primary advantage to the MITOC is its *man-portable* capability to enable its easy movement form one vehicle to another, or to an ad-hoc indoors command center or temporary EOC. This is opposed to most other mobile communications applications in vehicles that are fixed permanent installations that limit flexibility of use and would be put out of service if the vehicle were disabled for any reason.

The MITOC's ability to be shipped in its own transport case via normal airline or cargo carrier also adds to its application flexibility. This capability supports rapid disaster recovery applications to ship multiple units to operational bases nearest the disaster zone, for ultimate transport, via available local vehicles, to the scene or where needed the most. The following applications include those that the research team tested primarily relating to Homeland Security, including preparedness and emergency services. In addition, there are many more applications that can leverage the architecture, flexibility, and ease of use our research team has built into the MITOC concept; they are

included to illustrate the broad applications of rapidly-deployable communications and collaboration systems. Some software applications may have to be localized, depending upon the location, vendor support, or needs of the local jurisdiction. Any Internet accessible or web-based application software, or other on-site licensed software, can be integrated by a MITOC client to meet their specific needs. The following are examples of current and planned MITOC applications. Other capabilities will be pointed out as possible enhancements or additions that are technically possible.

7. Public Safety Applications

a. Fire/HAZMAT

Most firefighting scenarios would not need to access the broadband satellite capabilities of the full MITOC configuration due to the single-agency response used at most fires and limited on-scene deployments. Larger events, wildfires or large fires involving volatile sites with longer expected deployment durations, could benefit from the MITOC applications and/or modules, radio interoperability, and software tools to collaborate with other mutual aid departments that may be on-scene.

HAZMAT events are typically longer in duration than structure fires and involve more cooperation with other outside agencies during an event including local government, transportation, state offices, and federal agencies like the EPA and OSHA. A MITOC could be of benefit to a HAZMAT Incident Commander. Typical MITOC hardware and software capabilities to be utilized in fire/HAZMAT long duration or mutual aid scenarios would include Geospatial Information Systems (GIS), Imagery databases, and electronic facility blueprints to assess the situational environment. Incident Management / EOC and collaboration software would be used to establish and share on-scene situational awareness with remote resources or command locations. Emergency response software within CAMEO and WISER (described earlier) could provide assistance and decision support on how to manage the situation at hand in concert with MITOC's on-scene weather and wireless Internet capability.

Radio Interoperability would be utilized in very large multi-agency responses, major wildfires involving multiple jurisdictions, or HAZMAT situations such

as a terrorist attack with WMD, a major chemical plant explosion, or a train derailment involving a mutual aid response. In a terrorism scenario involving WMD, the ability to have radio interoperability with a variety of other local, state, and federal agencies would be critical. In these types of cases, the Incident Command structure would quickly escalate to a Unified Command structure involving collaboration across agency commands.

8. Law Enforcement

a. S.W.A.T. – Bomb Squad – Surveillance

The typical Special Weapons and Tactics (S.W.A.T.) and/or Bomb Squad deployment would utilize MITOC in a concept of operations where the MITOC/CTU would provide support for the IC wherein information about the mission could be downloaded via a cellular network connection on the way to the scene, thus saving time. Since many S.W.A.T. deployments are for stand-offs with individual(s) in a building or responding to actionable intelligence concerning a bomb threat, Internet access to various law enforcement databases by the MITOC could provide value-added capabilities in these cases. Internet availability to access criminal databases and property data, both residential and commercial, could reveal details about the target building, such as who owns it and phone numbers associated with the building's residents, workers, and neighbors, to call them to conduct an evacuation.

The proven ability of the MITOC to support covert remote surveillance with a variety of video resources would be invaluable in a barricaded subject, hostage, school or workplace shooting, or potential bomb scenario. The MITOC has already shown its ability to process video from covert resources such as a robot, hidden streaming web cameras, and wearable covert cameras. New technologies—such as the video ball that can be tossed in windows, and low-cost Unmanned Aerial Vehicle (UAV) systems such as the one MITOC is slated to trial in 2006—will add significant value to the Law Enforcement tool suite.

b. Riot and Crowd Control

The ability of the MITOC to give an Incident Commander situational awareness in a stand-off mode would be beneficial in a riot or crowd-control situation such as massive protests or other major civil disobedience disturbances. Real-time video feeds from covert, fixed street surveillance or traffic cameras can provide intelligence to the IC to plan road blocks or force deployments. Instant-messaging and sharing of imagery using marked-up street maps with field commanders allow instructions to be passed without being monitored on radio scanners.

c. Counter-Narcotics Operations

Counter-narcotics operations and interdiction activities could benefit from a MITOC operating covertly in a van or other vehicle utilizing video surveillance, radio interoperability with state and federal assets, and GIS databases. This asset would be especially beneficial in a rural environment to provide the Internet access for streaming video surveillance and collaboration with multiple agencies on a surveillance and/or interdiction mission.

d. Special Event Security

This application is extensively addressed in the Case Studies section of this thesis. Most all of the MITOC's feature set has already been proven to be beneficial to law enforcement in a Special Event security scenario such as a large sporting event, political rally, or other mass gathering. MITOC's Internet access would provide access to intelligence databases and warnings, collaboration with other agencies on scene, and access to real-time video surveillance, using covertly placed and wearable cameras, could also be shared with remote support resources such as a Joint Operations Center. MITOC's communications interoperability and VoIP telephony provide excellent field command post capability.

e. Federal Joint Operations Center (JOC)

In the event of a terrorist attack, the FBI would lead an effort by multiple federal agencies in concert with state and local assets to conduct the criminal

investigation and establish a secure link with the FBI's Strategic Information and Operations Center (SIOC). The JOC is envisioned to be near the WMD event to facilitate the investigation activities. The MITOC's secure Internet access, Wireless Secure Internet, and VOIP telephony could provide the JOC with needed infrastructure in any appropriate facility to provide total information security.

9. Emergency Services

a. Ad-Hoc Emergency Operations Center (EOC) or EOC Surge Capacity

Many smaller communities do not even have a physical EOC. Even if they have a designated EOC room or facility, which is usually some tables and chairs in a meeting room, they usually do not have full-time staff. It is especially rare to find that they have personnel trained in the latest Information Technology tools and resources. In fact, it is impractical to equip all of America's communities with such expensive resources or to train all of the volunteer Emergency Management personnel in the use of rapidly changing, yet critically important, emergency management software and hardware coming onto the market for use in an EOC environment.

The MITOC can be a valuable resource, especially when shared in a rural region by communities whose EOC is inadequate and even for urban areas whose EOC could be damaged or destroyed in a hot-zone, or incapable of scaling up for a big event. The ability to rapidly deploy a small collaborative and interoperable solution that provides EOC functionality will make our communities safer at a lower cost than constructing numerous EOC hard facilities.

b. On-Scene Situational Awareness (State and Federal Level)

The MITOC's satellite Internet access and portable generator power allows it to serve as a rapidly-mobile unit to provide real-time on-scene situational awareness to larger remote agencies, such as the Department of Homeland Security and/or FEMA, for on-the-ground conditions after a major terror attack or natural disaster. Geographically dispersed units, or even units airlifted into the affected zone, could

provide long-term monitoring to the local situation via real-time SITREPS, video surveillance and sensor monitoring—even in areas without operating infrastructure.

c. Disaster Communications and Humanitarian Relief

The MITOC's integrated communications suite can provide emergency response or relief agencies with long-term Internet and telephony services for up to thirty-six users with additional phones and laptops. The dial tone for the telephone system is over the satellite Internet connection and is "pulled" from a central office outside of the affected infrastructure.

A MITOC can also be utilized to provide victims of a disaster with a public location to send email or make a phone call to friends or relatives to inform them of their status or to reach their insurance carrier for claims. FEMA can also use it for a relief site for the public to access their web-based FEMA claim services.

10. Medical Applications

a. Medication/Vaccine Point of Dispensing (POD)

In the event of a mass casualty incident, bioterrorism attack, or pandemic outbreak requiring the emergency dispensing of medications or vaccines to the public, the MITOC could provide robust infrastructure to the medical or public health agency staffing the POD. The staff could utilize the wireless Internet access and VoIP telephony in this clinic for internal communications, database access, and external communications to provide SITREPS and information sharing with state or federal agencies such as the Centers for Disease Control (CDC) or Health and Human Services (HHS). Immediate online access to CDC databases for procedures on handling a dynamic health situation in an environment hastily set up, such as a gymnasium or town hall, would be a tremendous asset.

The Strategic National Stockpile, a secret national multi-location stockpile of medical supplies and medications, would ship a "Push-Pack" to an affected area for use by local medical response teams in a POD situation. The MITOC could serve as a communications and data resource to accompany the medical "Push-Pack."

b. Mass Casualty Triage and Field Hospitals

In the event of a mass casualty incident, a field operation to triage the victims or provide surge capacity to hospitals would require information access and sharing among the staff and to external support agencies or hospital assets. The mobile and man-portable aspect of the MITOC could provide rapidly-deployable communications under this scenario.

c. Telemedicine

In any of the above scenarios, the MITOC can provides "telemedicine" capability for remote medical assets to conduct patient assessment, provide advice on treatment, x-ray or other scan evaluation, or other advanced services and telemetry of patient vitals and scans.

d. Hospital Disaster Recovery

As observed in the aftermath of Hurricane Katrina in 2005, major hospitals were either significantly affected or even shut down by flooding and a continued power outage, rendering communications inoperable for days with patients and staff trapped inside. A MITOC and small generator deployed to the marooned staff by boat or helicopter could establish communications to assess situational awareness and to provide the ability to coordinate a plan of action.

11. Critical Infrastructure Protection and Resiliency Applications

a. Resiliency to Attack and Disaster with Back-Up and Recovery

The MITOC can provide the capability for an airport, chemical plant, energy provider, maritime shipping port, or other critical facility to have a back-up capability for telephone and email functions, even after a major disaster or terrorist attack. The MITOC can either be stored nearby in a protected and stable location, or flown in from a central site to provide on-scene recovery, or as an alternate site support to serve as a management command center at an alternate location.

The MITOC can also provide on-scene situational awareness for utilities affected by a widespread disaster to enable more accurate assessment of on-the-ground conditions. If utility crews are needed in a disaster area, it would be assumed the communications and power infrastructure are somewhat disrupted, which also affects their ability to communicate field assessments, job progress, and job assignments from their headquarters. Utility crews can use MITOC to keep in touch with their supervisors, assignment desks, and even their families, while on extended deployment in a disaster zone.

b. Business Continuity

Business and commerce are drastically affected by large natural disasters. History has shown that many businesses, even medium-sized ones, do not open again if a large segment of their infrastructure and ability to conduct business is disrupted for any length of time due to a disaster, either man-made or natural. For example, many businesses in the World Trade Center zone, affected by the collapse of the towers after the terrorist attacks of 9/11, never reopened. Conversely, those businesses with back-up locations and a solid business continuity plan were able to inform their customers of their status and stand-up operations within a reasonable time after the attacks. MITOC would be a valuable tool for a business that relied heavily on phones and computers, which describes most businesses in today's Information Age, to accomplish this task.

Business Continuity is a Homeland Security issue since the economic stability of our nation depends on a strong and resilient base of commerce. Any long-term disruption to the confidence in the economy can make us vulnerable and severely impact our nation's ability to rebound from a disaster or terrorist attack. The ability of well-prepared businesses to bounce back will keep costs in check and increase public confidence, therefore aiding in the recovery.

12. Expeditionary Activity Applications

The following potential applications of the MITOC are not directly related to Homeland Security per se; however, one can argue that the exploration for the subsequent

acquisition of energy resources and advancement of our scientific knowledge are important to our National Security and the preservation of our way of life.

a. Oil and Gas Exploration

The MITOC could be deployed with discovery expeditions to remote areas where geology field teams spend weeks in search of oil and gas deposits. Even though they currently use handset satellite phones, the additional broadband Internet capabilities of the MITOC at their base camp could be useful for more robust capabilities to send and receive geologic and geospatial data, maps, and imagery.

b. Mining Operations and Safety

Mining operations are usually in remote areas that may not be served by landlines for telephone service or Internet connectivity. A MITOC could be utilized in lieu of running expensive phone lines to a mine. Underground mining is one of the most dangerous undertakings due to the constant potential for collapse or explosion. The MITOC's wireless capability, coupled with the mesh wireless system from Rajant using small, rugged wireless access points that could be placed underground, would provide a digital lifeline to miners and rescuers.

c. Scientific Research

Archeological digs, environmental monitoring, and geological studies in remote areas, even in the extremes of polar and desert regions, could benefit from MITOC's portable communications capabilities. The ability to support a large base camp with a telephone system, computer network, and a weather station integrated with radios and geospatial software applications that are rugged and portable, would be welcomed by field researchers.

13. Commercialization Strategy

The commercialization of applied research is one of the primary goals of many academic research projects. This emphasis can be positive for both the researcher and the institution since there is usually some monetary incentive for both if the technology that

is transferred becomes successful in the marketplace. This process also benefits our nation—and sometimes even humankind in general—if the technology being transferred from research to the market provides for our security or provides a more efficient method or a product to serve a basic human need.

There is an expectation from the Department of Homeland Security that the MITOC will be commercialized to put the technology into place to protect our critical national infrastructure as soon as possible. The funding was also focused more on applied research than basic research, which allows for more rapid commercialization. There is also an expectation from the funding sponsor that, if at all possible, the new venture that will be created to integrate, market, and maintain the MITOC be located in the most economically distressed area of our Commonwealth of Kentucky, the eastern portion of the state, to assist in technology-led economic development. The types of skilled manufacturing, electronics integration, software integration, logistics and distribution, and programming jobs created by new ventures in the technology domain are nearly double the standard average wage in Kentucky.

The commercialization process begins at the Principal Investigator's university with a disclosure of any intellectual property anticipated in the research that should be protected by a patent or copyright. If there is a legal opinion that the research is able to be protected by a patent, the university handles that process and pays for the patent search and filings. The researcher and the Office of Technology Transfer then negotiate a split of any revenues that may result from licensing of the intellectual property to a private sector entity that takes the product to market.

The research validates the MITOC architecture and concept of operations, proving it to be a useful and needed tool in commercially viable markets. The portable design and modularity of the MITOC also provides a very cost-effective modality to provide the necessary communications, situational awareness, and collaboration tools needed for the Incident Commander. For example, the prototype MITOC system's off-the-shelf components retail for around $80,000 as described. The transport vehicle would add another $35,000. Therefore, it would be feasible to offer a commercial version of the MITOC for around $160,000, including the vehicle, while still assuming a reasonable

profit for the integrator. This is significantly less expensive than the typical bus or RV-based mobile command posts that run from $300,000 to over $1 million. This validation should provide the justification for a commercial enterprise to manufacture, market, and service the systems. This technology transfer process will have a positive impact on our nation's security as well as the economic vitality of our state.

C. CONCEPT OF OPERATIONS

1. At the Incident Command Level

One of the most important elements of the concept of operations for the MITOC is to minimize and/or simplify any interaction between the Incident Commander and the technology presented by the MITOC. The rest of the Incident Command System (ICS) team such as Logistics, Planning, Operations, and Finance/Administration should have an expectation to directly utilize IT in their roles *if such resources are available at the scene*. The MITOC configuration will provide that IT capability at the scene.

The research team's interviews and research indicate that the Incident Commander should not be distracted by having to manipulate the Information Technology or spend an inordinate amount of time inside a "mobile command post," especially in the early phases of a response. The IC has an instinctive predisposition to be surveying the scene with an eye on the situation and on his/her troops. Once a plan of attack has been formulated and the response is underway, having a place out of the weather or an environment somewhat insulated from the noise and confusion of an active emergency scene may be beneficial to some ICs. This may be especially important when assimilating critical information for a major tactical decision and some freedom from distraction would be important.

Ergonomics providing a more supportive environment for the IC are designed into the MITOC concept of operations with the visual interface (the primary display screen) to the technology suite able to be accessed either inside or outside of the support vehicle. For example, a 32-inch LCD display screen that is easier to view than a PC screen can be presented to the IC at the window of the support vehicle on an articulated arm or viewed inside the vehicle at a preferred angle and distance from the IC. The SUV's mid-cabin

design, with the factory-mounted rear seats removed, allows easier entry to the third-row rear seat for the IC outfitted in a bulky turn-out coat and helmet, or a Police/S.W.A.T. commander with weapons and duty-belt.

One of the major challenges to the MITOC project is in providing advanced technologies to support the Incident Commander without the expectation of direct interaction between the IC and the technology. The recommended solution should not expect the IC to be a skilled technology user. This skill-set expectation may change in the future because many people growing up in today's Information Age accept portable technology gadgets as natural extensions of themselves. At some point in the near future, the technology-savvy generation will start filling Incident Command and First-Responder roles.

It is encouraging to see that there are examples of forward-thinking jurisdictions attempting to affect a sea-change in technology utilization at the Incident Command level. Usually this is observed in large metropolitan jurisdictions most at risk from terrorist attack, such as New York City or Washington, D.C. These jurisdictions also have a large professional workforce pool, as opposed to volunteers as seen in most rural and small communities. Large metro jurisdictions also have the available budget to try new approaches and the availability of Information Technology departments to assist in the selection, deployment, and servicing of advanced IT tools.

For example, the 2004 FDNY Strategic Plan laid out several goals to "Advance the technological capabilities of the Department."[81] In this set of recommendations, an overview of the latest improvements in communications were listed. They included new UHF radios that are better capable of penetrating buildings, mobile repeaters that extend radio signals, and an interoperability solution to link dissimilar frequencies of other mutual aid departments from outside New York City. These improvements are a direct result of the criticisms levied on the emergency response to the 9/11 terror attack where

[81] FDNY Strategic Plan, 2004, Goal 6.0, Advance Technology, 33-37. http://www.nyc.gov/html/fdny/pdf/pr/2004/strategic_plan/goal_6.pdf , accessed December 2005.

police and fire units could not communicate during the response because of incompatible radio systems, directly contributing to the loss of lives when the buildings collapsed.[82] Additional improvements listed in the Strategic Plan included upgrading the mobile command center with GIS and videoconferencing capabilities. The most unique and unexpected advancement, however, was the call to develop electronic wireless command post boards. These incident status boards are the staple of an Incident Commander's repertoire of on-scene tools—a physical board with either grease pencils or magnetic markers to track who is where. These are especially prevalent in the Fire Service.

It is important to note that the FDNY planning for this technology is also taking into account the limitations of this electronic Command Post technology. The Strategic Plan specifically mentions the system will have the requirement of an off-site duplicate back-up copy of all the electronic postings. This serves two important purposes, one being that the electronics can fail or malfunction, usually at the most inopportune moment. Who has not suffered the fall-out from a computer on the fritz or, worse yet, one affected by a virus or run-down battery? The other reason for the back-up copy is to have a documented trail of the Incident Commander's decisions and the deployment of troops in the event of another catastrophe like the collapse of the World Trade Center Towers. In that incident, the command status boards in the Command Post locations were all lost in the collapse, taking with them the timeline and an accurate depiction of what units were deployed and where they were last known to be in the buildings. Replacing this tried-and-true method of incident management, and replacing it with technology, is a powerful testament to the FDNY's acceptance of new technology to help prevent future tragic losses of both firefighters and civilians.

Will Public Safety agencies in smaller communities, and especially rural areas, accept new electronic substitutes for their commonly-used resources, many of which are paper-based? For example, there was discussion at a meeting of one of the research team's (a major metro area) response agencies on the various guides and booklets

---

[82] National Institute of Justice, "When They Can't Talk, Lives Are Lost," *National Task Force on Interoperability*, February 2003, 3, http://www.safecomprogram.gov/SAFECOM/library/interoperabilitybasics/1160_nationaltask.htm, accessed August 2005.

recommended for a more complete assessment of a chemical or radiological incident. The recommendation was made that more than one booklet or guide should be consulted since there may be differences among the guides in the recommended actions to take. a The individual who was making the recommendation for the training session always carries a tub full of these books, guides, and other "tree-based" resources in his response vehicle. As one of the most respected experts in our jurisdiction on Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) response, his recommendations carry a lot of weight in our jurisdiction. In support of his argument, a member of the training audience stated, "When you're wrestling with the dragon, a paper resource you can tear out of the book and pass up the line is invaluable."[83]

The concept of operations for the MITOC must take this mindset and its prudent notion of on-scene redundancy into consideration. Since the support vehicle that transports the MITOC is seriously space-challenged, it is not reasonable to stock a library of response guides on-board. As a back-up contingency, having a paper (laminated for durability) contact and resource list that indicates who carries those guides in their vehicle would be critical in the event of a total systems failure. Other redundancy measures are also designed into the MITOC's concept of operations. As previously stated, much of the MITOC's resource data is obtained over an Internet connection through multiple means of connectivity. Electronic CBRNE guides, digital versions of the paper guides advocated in the training class, are resident on all the MITOC's six laptops and our research team's Personal Digital Assistant (PDA) devices. To give the ability to have a paper version to "pass up the line" as advocated, the MITOC is equipped with an on-board printer to allow printing of just the document page(s) needed, which is analogous to "tearing out the page." The MITOC's solution has two very important advantages over the paper guides. One is that the MITOC's resource guides, or sections thereof, can be easily updated by downloading the latest version or other pertinent new information whenever we are connected to the Internet, whereas the paper guides are updated usually only once every year or so. The other primary advantage is the ability to

[83] Richard Wellinghurst, Joint Emergency Services Unit member, in personal communication with the author, November 2005.

print multiple copies of the desired document so all appropriate members of the ICS team or First-Responders can have their own copy of the relevant data. This would include a Material Safety Data Sheet (MSDS) resource that is often used in HAZMAT responses, or a print-out of a map or building blueprint at the scene.

Most jurisdictions, especially smaller communities and rural departments, must contend with few resources, such as trained personnel or IT staff, to try new technologies. The MITOC solution was designed to address this limitation and does not assume that the Incident Commander, or the ICS staff in a larger deployment for that matter, has the requisite skills to deploy and utilize the same type of assets described earlier in the FDNY Strategic Plan.

In practice, wielding technology at the incident scene involves more than having skills in the use of a personal computer. The various application software suites used in the MITOC are the heart of the solution and represent the actual man-machine interface. Application software requires training and experience in its use, its nuances, and its limitations. It is not practical to expect today's typical IC, their ICS team, or their First-Responders for that matter, to be skilled IT users or even accepting of the technology. That being said, alternative methods to *acquire and interpret* the technology assets and the information needed by the Incident Commander must be engineered into the recommended solution set. Personnel costs have to be taken into consideration in any recommended design and concept of operations. In many cases of technology deployment, the personnel costs far outweigh the actual costs of the hardware and software solutions if the Information Technology utilized is not designed for the non-technical end-user.

The concept of operations for the MITOC and its support team embraces the operational role of a small but growing discipline called Incident Dispatch Team (IDT) or Tactical Dispatch Team (TDT). The concept of Incident Dispatch Teams has been around since the mid-1990s, having started in California.[84] Even though it has strong supporters and enthusiastic feedback from jurisdictions utilizing IDTs, this operational tactic has yet

[84] Website on Incident Dispatch Teams, www.springhillfire.com/class_of_1999.htm, accessed December 2005.

to be utilized across the board as a standard operating procedure. Incident Dispatch has been utilized for at least ten years and got its start in fire operations to combat the wildfires of California, the same venue as the Incident Command System (ICS). Therefore, it is curious that the tactic is not even mentioned in the National Incident Management System (NIMS).

The role of the IDT is to provide support functions to the Incident Commander, such as NIMS-required documentation and operations of communications at the incident scene, just as the MITOC concept of operations advocates. This allows the Incident Commander to focus on the tactical decisions that are time-sensitive. Having a trained dispatcher or a team of them at an incident scene will also lighten the load at the primary dispatch point, especially during a major incident or even at a special event. The unique attributes of a trained dispatcher, such as being detail-oriented, having the ability to accurately take-in and repeat information while simultaneously juggling multiple tasks, makes a dispatcher the ideal candidate for this position.[85]

Certification and training are critical elements to ensure that personnel assigned to this task are fully engaged in the utilization of ICS and are issued appropriate electronic as well as personal safety equipment.[86] Several private sector firms are engaged in providing training that is recognized for certification of IDTs. The California Fire Chiefs Association also provides training to certify IDTs for mutual aid deployment. FEMA does not list any training relevant to IDT, or specific training for Incident Command support in the areas of communications or Information Technology systems.

A similar concept of operations is being utilized by the Westmoreland County, Pennsylvania Department of Public Safety. They staff their mobile command post, an RV-sized unit, with an Incident Response Team (IRT).[87] Their assertion is that their "Command Post Forward" (CPF) strategy provides the Incident Commander with better

---

[85] Website for Incident Dispatch.Net, http://www.incidentdispatch.net/intro.htm, accessed December 2005.

[86] Larsen, "Incident Dispatchers Can Lighten an IC's Load.

[87] Robert Mateson, "Supporting the Incident Commander: The Command Post Forward/Incident Response Team Approach," *International Association of Emergency Management Bulletin*, November 2004.

support because the IRT can assess the incident first-hand and make appropriate recommendations on the staffing of ICS positions as well as fill some or all of those positions quickly for the IC. Rather than these support personnel being only dispatchers, their concept seems to emphasis experience in Emergency Management and staffing the CPF from EOC-type personnel.

The concept of operations for the MITOC distills the IDT/IRT down to its essence—a technical support person assigned to the Incident Commander. Being an SUV-based rapid-deployment resource, as opposed to a fully-staffed bus or RV type mobile command post, the MITOC and its SUV are structured to go in lean-and-mean. Being conceived as a first-on-scene resource, it is not practical to utilize an actual Incident Dispatch "Team" due to the limited space in the SUV and a usually shorter duration deployment than a full-sized mobile command post. The concept of having an on-board skilled technical person to serve as the resource to the Incident Commander is one of the MITOC's *key components* to ensure effective utilization of the hardware and software that is recommended in this concept of operations.

While the MITOC's support vehicle is en-route to the scene, a technician or specialist familiar with radio communications and Incident Management technology resources could be accessing relevant information to prepare for the Incident Commander's anticipated requirements based on the type of emergency or deployment. The MITOC uses a cellular-based technology to access the Internet for this part of the deployment. Therefore, a minimum of a two-person team should be assigned to fill the role of a MITOC support unit. Once on-scene, the driver could support the Incident Commander as part of the ICS command structure, provide force protection if they are a sworn law enforcement officer, as two of the research team members are, or provide additional technical resources such as radio operations or information access to knowledge-management resources.

An enlightening discussion with a Deputy United States Marshal and a retired Fire Chief uncovered some ideas that ultimately resulted in the recommended method to

staff the technology resource position for the MITOC.[88] They indicated, justifiably so, that Full Time Equivalent (FTE) costs to staff a new position is problematic, even for a larger jurisdiction like Metro Louisville. It is more than just the money issue, even though that is the biggest hurdle. In a professional organization such as police or fire departments, you often have a long history of tradition within the organizational structure and hierarchy, tenure, and chains of command. Inserting a new position into such a culture takes a lot of time and energy, which was not the mandate for this project. Therefore, it was suggested that some agencies may be open to a volunteer position similar to the concept of a volunteer firefighter. The analogy is credible, since even our Metro area has a large suburban corps of volunteer fire departments whose members, like volunteer firefighters everywhere, have to attain rigorous qualifications to serve. Just as the brave men and women who answer the call to serve their communities—who maintain peak physical conditioning to meet the requirements of the job and haul out day or night to enter a burning building—a new cadre of certified tech-savvy volunteers could be mustered to serve the Incident Commander in an emergency environment. This would open up a whole new avenue for those with technology or communications skills who want to serve their community like a firefighter, but have other skills to offer. An appropriate title or designation for this position could be "Incident Command Support Specialist" (ICSS) that ultimately carries a certification requiring a specific level of Information Technology, radio and other communications knowledge, or field ability. This would be similar to a firefighter having to pass physical and skills testing, or a HAZMAT trained volunteer having to take training and pass the "Technician" or "Operator" level certification. Such a requirement would separate the "wannabes" from the truly committed, while serving to act as a precursor to professional status in departments that could support full-time positions for an ICSS.

There would be an expectation of sub-certifications and experience in the specific applications utilized in the MITOC technology architecture. For example; our strategy for the ICSS role would recommend a minimum level of a Microsoft Certified Technology

[88] Richard Knighten, Deputy United States Marshal and A. J. "Bud" Fekete, (ret.) Louisville Fire Chief, in personal communication with the author, 2004.

Specialist (MCTS) or Microsoft Certified Systems Engineer (MCSE) for the operating system, and Cisco Certified Network Associate (CCNA) for the networking side. Radio familiarity on the communications side should also be emphasized. However, other than certification for Amateur, sometimes known as Ham, radio, there does not seem to be a public safety radio operator certification, or even a standardized training program, for the field level user. This is where on-the-job experience and observation of good radio protocol will be necessary. In fact, the problem of the lack of radio training for in the field users extends even into the ranks of first responders.[89]

In addition to user skills in the technology, it will be critical for the ICSS to be well-versed in the domain and special needs of whatever type of department the MITOC is a part of; whether that be emergency management, Homeland Security, law enforcement, or HAZMAT. The ICSS will be required to anticipate the needs of the Incident Commander. Therefore, base level certification will need to start at the NIMS certification in ICS. The minimum level should be the IS-300, 400, 700, and 800 level courses in NIMS-compliant ICS understanding, which are offered in a web-based learning environment on FEMA's training website. Other domain specific training or familiarity should rest with the department responsible for the MITOC's operations to ensure maximum benefit from the technology being utilized and from the ICSS as the primary operator.

This volunteer staffing concept may well serve certain types of deployments and jurisdictions such as a suburban area, small town, or rural fire departments. Applications with HAZMAT responsibilities would significantly benefit from a MITOC deployment due to the frequent need at a HAZMAT scene for longer deployments and access to data relevant to chemical or radiological exposures, reactions, and attributes. GIS utilization and consultation with multiple agencies requiring radio interoperability are also seen more at HAZMAT incidents, making the MITOC deployment more appropriate than a typical structure fire, unless it was of a huge magnitude or in a critical area.

---

[89] Steven Proctor, "First Responders Lack Radio Training," *Primedia Business Magazines and Media*, 2004, http://www.findarticles.com/p/articles/mi_m0HEP/is_6_22/ai_n6067591#continue accessed 13 December 2005.

Staffing of a MITOC with an ICSS in a law enforcement role would more than likely require a professional status, either part-time or full-time, since volunteerism is not a tenet of law enforcement agencies. This is due to the public risk, sensitivity, or even danger of some operations well-suited to the MITOC, including undercover and S.W.A.T team deployments. Special events requiring security operations, such as major sporting events, political conventions, and any major crowd gathering, are excellent opportunities for the MITOC to support law enforcement operations. Unless the MITOC is a regional public safety resource shared among agencies, similar to our research project, it is again more probable that those deployments should be staffed by law enforcement communications professionals.

The MITOC's technology suite is specifically designed to encompass the necessary technology tools for the initial on-scene needs of the IC, while also having the ability to support the initial deployment until larger assets such as the RV or bus-based mobile command posts roll onto the scene hours later. If larger assets do become involved at some point in the response, the MITOC's data network can easily integrate into a multi-resource configuration at the Incident Command Post (ICP) or move to another area needing support. This redeployment can occur while serving as an umbilical to the larger mobile assets, thereby extending the wireless "cloud" and subsequent reach of the Incident Command team to serve First-Responders or tactical troops in the field some distance away from the ICP itself.

The concept of operations so far has focused on the short-term deployment of the MITOC, primarily as an asset to the Incident Commander. In this configuration, the MITOC electronics package is located in the rear compartment of the SUV and the IC would work from either inside the mid-cabin or just outside the vehicle to enable interaction with the ICSS.

For longer on-scene deployments, where the ICP is staffed with a growing cadre of the ICS team to include Planning, Logistics, Operations, and the ICSS; the concept of operations calls for the erection of an on-board 12' x 14' canopy behind the SUV to shade the team in hot weather or, with the addition of snap-on sides, provide some measure of protection from the elements in inclement weather. The deployment package

also includes a 3’ x 6’ folding table and six folding canvas chairs, providing some modicum of comfort at the scene, and a sturdy dry location to place the six desk IP telephones and laptop computers, also carried on-board. With the generator that is also part of the “extended-deployment” package, the MITOC could operate an ICP autonomously for up to 36 hours with the fuel and supplies it can carry.

At some point in this type of extended on-scene deployment, larger mobile command post assets will be expected to join in the response. This mobilization could consist of state emergency management mobile assets, mutual aid from larger jurisdictions, National Guard assets such as a Civil Support Team, or FEMA’s Mobile Emergency Response Support (MERS) vehicles.[90] The FEMA MERS are generally not expected to roll onto the scene until 72 hours or more after a major incident. The MITOC has been designed to serve as extensions to these larger mobile assets by merging wireless networks and other technologies such as sensors and surveillance capabilities. Examples of several successful MITOC test deployments, where the unit was integrated with larger mobile command posts, is described in detail in the case study chapter of this thesis.

The next higher level of deployment would be for an extended emergency such as a natural disaster or major terrorist attack. The concept of operations calls for the portable MITOC to be removed from the support vehicle and stationed in an appropriate facility that could serve as an EOC, such as a community college or hotel meeting room. The “man-portable” design that allows this level of flexibility in the MITOC concept of operations is one of its key attributes that differentiates it from other mobile command centers.

In the MITOC research project, the ubiquity and convenient locations of the nation’s community colleges are being considered as a potential location for not only MITOC deployments as an alternate site for an ad-hoc EOC, but for other emergency sites to serve the community, such as medical POD for antibiotics or vaccines. Another potential humanitarian aspect would use the community colleges as centralized public

[90] FEMA Mobile Operations Capability Guide for Emergency Managers and Planners, http://www.fema.gov/rrr/mers01.shtm, accessed December 2005.

information locations for people in an affected area to get printed material and instructions, and utilize the MITOC telephones or computers to contact their insurance companies, FEMA, or loved ones after a destructive event, even if the area's public telecommunications utilities are out of service.

The benefit to establishing community colleges as a natural site for an ad-hoc EOC with MITOC technology is due to their physical space availability and usually robust IT infrastructure. Another important consideration is that the public generally knows where the local community college is located if instructed to go there for medical prophylaxis or food and water distribution. The Kentucky Community and Technical College System (KCTCS) is a partner in the MITOC research project and will test this segment of the concept of operations in exercises scheduled for 2006. The research results will be shared with "Prepare America," a national Homeland Security initiative comprised of community colleges in anticipation of a formalized plan to incorporate MITOC systems into a national strategic plan. This plan will integrate the MITOC's capability to provide EOC capability in rural and small-town America to respond to emergencies where the community is either too small for an EOC or perhaps the resources they did have were rendered unusable or hazardous in a natural disaster or attack. The MITOC's inherent design allows for up to thirty-six VoIP telephones and thirty or more wireless laptops to its base system. Perhaps more importantly, the IP-based radio interoperability system in the MITOC also allows 911 dispatching from the system over either VHF or UHF radio frequencies. This level of communications capability rivals many Emergency Operations Centers in some cities.

2. Concept of Operations with the Local/State Emergency Operations Center

The MITOC, supported by its SUV or in a stand-alone configuration in an ad-hoc facility, is relatively self-sufficient with its mobile Internet and power generation capability. The MITOC concept of operations calls for connectivity and interaction with one or more EOC assets, even simultaneously, during extended deployments. This capability is important to provide information sharing, more specifically on-scene situational awareness, to emergency management and/or command level personnel at the

appropriate level above the responding agency. For example, the MITOC could initially link upstream with a local EOC in the nearest jurisdiction to the incident. As the need arose, it could also link with the state EOC or even a National Guard JOC (Joint Operations Center).

This capability is achieved with information-gathering and collaboration tools contained in the support vehicle and those inherent to the MITOC's electronics suite. One example of such an information-gathering tool would be sensor inputs, like on-scene weather data provided by MITOC's portable wireless weather station, or even chemical/radiological sensors, scheduled to be added by mid-2006. The MITOC's software contains plume-dispersion modeling software to allow prediction of the spread of a toxic or radioactive cloud by linking MITOC's sensors to various specialists at the EOC that could interpret the data for the IC. While that analysis is underway, the on-scene ICSS could be doing other time-sensitive activities, thereby increasing the efficiency of the response.

Other information gathering tools include MITOC's wireless surveillance capability, accomplished by streaming video cameras that can be set up at the incident scene. These stationary or portable cameras not only provide the ability to feed visual data back to the IC from points around the scene, but to also provide an EOC with a more accurate common operating picture of the incident. The videoconferencing aspect of this technology allows real-time visual interaction between the IC and an EOC.

The most dramatically beneficial use of this on-board videoconferencing technology may be in a medical application. A MITOC on-scene could provide emergency room doctors in a remote hospital with video, high-resolution still imagery and other patient telemetry for remote triage advice, or even recommendations on decontamination and/or isolation of patients exhibiting symptoms of biological or chemical exposure. The MITOC prototype is tasked with supporting the containment of a human biologic vector (a contaminated person) by Metro Louisville's Joint Emergency Services Unit (Joint ESU). The operational scenario calls for the MITOC to be on-scene supporting the IC of this combined S.W.A.T / Hazmat / Public Health team, which has to respond to any reports of passengers on an aircraft exhibiting troubling symptoms that

may indicate they are contagious and a threat to our community. Members of the Joint ESU tactical team would don Personal Protective Equipment (PPE) and attempt to isolate the suspected human vector somewhere on the plane, and take blood and temperature samples as well as high-resolution imagery. This data would be wirelessly transmitted from the tactical team to the MITOC on the airport tarmac, which, in turn, processes it into an email or even a live videoconference with the state EOC or department of Public Health as well as the Centers for Disease Control (CDC) for recommended action.

Collaboration tools such as WebEOC or HSIN consist of web-based software that allows multiple individuals to collaborate online to share documents and other data. This technology is invaluable to provide the controlling EOC with situational awareness from the scene, or additional research and recommendations from the EOC to the Incident Commander. These capabilities require broadband Internet access delivered by the MITOC that otherwise may not be available to the IC.

3. Concept of Operations at the National Level

Some anticipated MITOC deployments could require interaction between the on-scene IC and national level operation centers such as Northern Command's Joint Operations Center (JOC), the Department of Homeland Security's Homeland Security Operations Center (HSOC), the FEMA NIMS Integration Center (NIC), or the FBI's Strategic Information and Operations Center (SIOC). The flexibility of providing upstream situational awareness for the MITOC is theoretically limited only by the deployment application and agency affiliation of the on-scene Incident Commander. For example, a real-life scenario would probably not see a Fire Battalion Chief directly interfacing with FBI SIOC or a S.W.A.T. team commander talking directly to Northern Command. The pre-planned ability of these remote resources, to either access the Internet traffic or situational awareness from the MITOC over secure but compatible protocols, is an extremely powerful tool to allow federal assets to assess the situation accurately in the area affected by a disaster or attack.

The lack of on-scene situational awareness capability severely impacted the credibility of FEMA's former Secretary, Michael Brown, when his comments on a

national live interview illustrated that he was not fully aware of some of the extreme conditions on the ground in New Orleans during the 2005 Hurricane Katrina disaster. The reporter pointed out that, if he had been watching their news feeds, he would have been aware of the crisis at the New Orleans Convention Center. Regardless of that fact, even network news may not be able to be everywhere, all the time, during a rapidly-unfolding terrorist attack with WMD, or a wide-ranging catastrophe like a Category Five hurricane or massive earthquake. A rapid-deployment fleet of relatively low-cost support vehicles equipped with MITOCs could be driven and air-lifted into the disaster zone with trained teams to do on-the-ground damage assessment, hot zone mapping, and infrastructure checks, while feeding the real-time data back to FEMA's NIMS Integration Center (NIC) or the DHS HSOC.

Regardless of the scenario or type of deployment, the concept of operations for the MITOC is to serve as the on-scene support to the Incident Commander and to also serve as the eyes and ears upstream to more in-depth resources and command personnel. If this concept of operations and strategy on how the MITOC is deployed and staffed is adopted, exercised, and written into standard operating guideline of a jurisdiction, the entire chain of command in the emergency response or prevention/security initiative shares a common operating picture, thereby enhancing the ability to save lives and/or property.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TESTING AND EVALUATION OF THE PROPOSED SOLUTION

A. SPECIAL EVENT APPLICATION: THE KENTUCKY DERBY – MAY 2005

The Kentucky Derby, on the first Saturday in May at Louisville, Kentucky's Churchill Downs, is one of the most recognizable sporting events in the world. . This special event attracts over 150,000 patrons from all over the world, including celebrities and leaders of politics and industry. It is broadcast live around the world, making it a prime terrorist target since any incident would be seen by millions, in real time, and the large crowd could potentially panic under any type of overt attack causing even more casualties.

"The Derby" is in the research team's jurisdiction; the University of Louisville IT Research Center for Homeland Security (iTRC/HS) already provides technology consulting and command center support for the agencies providing security for the event. Therefore, it was logical to test the MITOC's Incident Command capabilities on-scene at the venue.

The iTRC/HS was hosting all the federal agencies providing WMD monitoring, intelligence-gathering, information fusion, and support from its 50-seat command center, called the Collaborative Engagement Theater, thirteen miles away. Agencies including the FBI, BATF, U.S. Marshals, DEA, ICE, INS and Secret Service brought in encrypted satellite communications to link to their headquarters and monitors receiving video feeds from covert high-resolution remote control surveillance cameras. This command post, referred to in federal terms as the Joint Operations Center (JOC), was also in communication with the police command post located in the downtown Metro Louisville EOC. This is where the overall Incident Commander, a Louisville Metro Police Major over Special Operations, was located. He also had two on-scene Incident Commanders at the venue.

The iTRC/HS provided the MITOC to the security detail as a remote command post situated in the police compound to support one of the on-scene commanders within

the infield area of the track. There, the two-man crew established a wireless link providing data interoperability with a larger mobile command center truck called the Sentinel provided by Cisco Systems and L3. This Special Event application deployment test of the MITOC accomplished the following:

1. Shared Satellite Internet

The wireless data interoperability link was established with the larger command post truck on the scene by sharing a common wireless local area network (WLAN) provided by the L3 Sentinel truck's satellite dish. The MITOC had not yet been equipped with its satellite Internet dish, so this connection provided the broadband backbone for transmitting data from the MITOC to the federal JOC and the police command post at the EOC. The speed was approximately 256Kbps downstream from the satellite, and 64Kbps upstream to the satellite.

Findings: This activity provided a proof-of-concept for the mission the MITOC was designed for; first on scene to provide Incident Command Support in the first critical hours of an incident. When larger and mobile command posts roll onto the scene hours later, the MITOC can provide an effective technology hand-off and continue operations at the scene, or move on to another affected area while staying wirelessly connected to a larger "Mothership" resource like a Heavy Truck, bus, or RV-type mobile command center.

The other finding was that the broadband speed of the L3 Sentinel's satellite service was not optimal for receiving and transmitting dense geospatial information or live streaming video. It performed flawlessly, however, on high resolution photographs and situation reports (SITREPS). Therefore, this test prompted our research team to order the MITOC's satellite service at a minimum of 1mbps downstream and 256Kbps upstream. A downstream Internet speed of 512Kbps would still be acceptable with 128Kbps being the minimum acceptable speed on the upstream link. Obviously, the cost of the service is a real issue when specifying recommendations, and a cost/benefit trade-off that is specific to the application the service will be primarily used for must be taken into account.

2. Uploaded Surveillance Imagery

The MITOC relayed several different type of surveillance imagery to the JOC and EOC including live streaming digital video from web cams at low resolution, stored and forwarded video files at high resolution, and auto-refreshed high-resolution photographs every minute.

Findings: The surveillance aspect of the MITOC to provide on-scene situational awareness to a remote command center was successful and opened the door for more ambitious use of this technology for the 2006 Kentucky Derby by integrating newer technologies, covert cameras, and better live streaming performance with the MITOC's current broadband capability, which is twice as fast as the L3 Sentinel's dish used in 2005. The test also showed that a MITOC can also be able to support covert streaming video to provide better situational awareness to the on-scene Incident Commander. This technology was utilized at the Kentucky Derby to transmit live streaming video from miniature cameras hidden on federal agents and police officers carrying Wi-Fi-equipped tablet computers. The video was transmitted to the JOC, which was located on-scene that year. The MITOC will facilitate that valuable intelligence and situational awareness tool in 2006 and transmit the imagery simultaneously to the on-scene commander, the overall Incident Commander, and the federal JOC. The auto-refreshed high-resolution photographs provided surprisingly good results and could be utilized in a variety of situations, from the fixed camera on a mast to images taken by security forces of suspects for review by the command staff, or compared to criminal databases.

Another application of this proven capability would be to provide close-up high-resolution photographs, of people presenting symptoms of disease or radiation, which would be intercepted by a special team at the entrance of the venue. This special team, the Joint Emergency Services Unit, scans for chemical, radiological, and biological threats at our jurisdiction's special events. If a person tries to enter with a suspicious looking lesion, pustules, swollen glands, or otherwise looks unhealthy; the team would separate the individual to an area to take vitals and a high-resolution photograph for

evidence and, if warranted, transmit that image to the CDC for review. The MITOC would provide the intermediate data archiving and transmit the image to the JOC, EOC, or CDC.

3. Wireless Remote Weather Station

The MITOC carries a portable wireless weather station that can be set up on-scene to provide temperature, wind chill, humidity, barometric pressure, dew point, wind direction, and wind velocity. It uses a battery-powered wireless access point to transmit this live data back to the MITOC where it is automatically entered into a software application to perform plume modeling and prediction overlaid onto a geospatial map of the area; in this case the Churchill Downs venue for the Kentucky Derby and surrounding residential and business areas.

This capability is critical in the event of any release of a toxic substance into the air. This could occur from a terrorist attack involving chemical weapons or radioactivity carried in the smoke and dust cloud from a radiological dispersal device or "dirty bomb." The plume modeling supported by this weather station would also be crucial in the event of a train derailment at the active tracks next to the venue, or an accidental release from one of the nearby industrial sites that deal with hazardous materials.

Findings: The wireless weather station is an important asset for any security detail since it provides instant data that would be able to provide the Incident Commander with an indication of wind direction as soon as something unusual happened. If there was a suspected release due to an explosion or an obvious cloud of any sort, the IC could use the wind direction in relation to the source event to determine if the Incident Command Post is in the direction of the plume and, if so, move quickly. If not, it is then ready to compute where the plume will head and allow that information to be shared with other appropriate agencies.

4. Satellite Phones

One of the lessons learned and detailed in the After-Action Report (AAR) for the 2005 Kentucky Derby was the fact that communications at the scene deteriorated as the

day went on. This was due to overwhelming use of cellular phones by patrons while police were vying for those same voice channels over their cellular phones to keep radio traffic to a minimum. Even with the cellular carriers boosting their network coverage by bringing in Cells-on-Wheels (CoWs) and Cells-on-Light Trucks (CoLTs), the service was spotty at best. Even the trusty Nextel cellular phones favored by law enforcement had difficulty making calls on the phone network. The MITOC provided a central location for police commanders with Globalstar satellite phone service that was unaffected by the saturation of the cellular airwaves. If a real emergency had occurred, cellular phone service would have been totally useless. The MITOC's satellite phones would have been the only way to reach the outside world.

Findings: The After-Action Report for the Kentucky Derby 2005 indicated this issue is important enough that several stand-alone satellite phones will be rented for the 2006 event for use by Incident Commanders in the field. This capability will also be greatly enhanced at the 2006 Kentucky Derby with the addition of the MITOC's broadband satellite service, which supports VoIP telephone service. This will allow the MITOC to access telephone company landline dial-tone from the University of Louisville telephone switch and feed it to the IC's phone system: six desk-top sets and six wireless handsets with a range of ¼ mile, set up at the MITOC. This configuration will serve up to four simultaneous users, allowing those with wireless handsets to roam about the venue and make external calls while not being affected by saturated cellular service.

5. Tested Data Radio to Remote Team

The Joint Emergency Services Unit (Joint ESU) mentioned above was stationed at the entrance of the Churchill Downs venue, but had no wireless Internet access at that location. The MITOC's on-scene wireless local area network did not have the power to reach the team nearly two-thousand feet away on the other side of the Grandstand, which is a huge structure full of concrete, steel, and heavy wrought-iron that blocked the standard Wi-Fi network signal.

The MITOC carries a high-powered 900 MHz data radio that allows a transceiver to be set up at the broadband source; in this case it was the MITOC, and another at the receiving end—in this case the Joint ESU.

Findings: The Data Radio flawlessly allowed the Joint ESU to access the MITOC's broadband Internet access over an encrypted 512Kbps link providing enough bandwidth to support their laptops' access to the Internet. This gave them the bandwidth they needed to perform their mission. It worked so well that the research project may acquire a permanent unit under the next round of grant funding.

6. Access to MetroSCENE.net

The MITOC provided the on-scene commander with the same software tools provided to the JOC and EOC. These software resources included an Information Sharing web-based Internet portal designed by the iTRC/HS called MetroSCENE.net (SCENE is an acronym for Secure Collaborative Engagement Network for Emergencies). This portal provided the on-scene commander, users in the field served by the MITOC, and the command staff at the JOC and EOC with detailed geospatial information system (GIS) called LOJIC. This GIS tool is used by our jurisdiction's utilities and public safety agencies, providing mapping, locations of utilities and roads, distance calculations, and even the outlines of structures. An orthographic satellite image was overlaid on the map, giving the on-scene commander a detailed view of the Churchill Downs venue. Other tools accessed through MetroSCENE and the MITOC at the Kentucky Derby included: Pictometry, a high-resolution aerial imagery tool with interactive capabilities; Watch Command, a collaboration and Incident Management and documentation tool; and STEPs (Spatial Templates for Emergency Preparedness) for traffic camera access, GIS databases, and access to reference guides and local contact databases.

Findings: Having a common portal to use across agencies will be a necessity to ensure adequate information sharing and collaboration. The prototype MetroSCENE.net provided one controlled and secure place to access all the web-based tools. The project was not funded to develop a robust permanent tool. Its purpose was to prove, in concept, that a web portal would be acceptable to the anticipated users as the preferred delivery

modality for collaboration and information sharing. The research team will investigate various collaboration and information sharing portals over the next grant funding period. The goal will be to seek a product that will provide maximum user-friendliness and ubiquity across jurisdictions to recommend to the commercialization licensee. The reality is, however, that each jurisdiction will probably have a preferred collaboration tool. Therefore, the recommended product will probably be offered to those jurisdictions that do not have an electronic incident management, collaboration, and information-sharing tool.

7. Summary of Findings

The MITOC provides robust on-scene situational awareness to the Incident Commander while allowing that information to be shared with other command entities, in this case the JOC and EOC. This provides a shared common operating picture for all command staff, which enables better decision making in an emergency or terrorist attack. The MITOC's performance illustrated its ability to serve as a secure site for reception of intelligence information from the JOC and EOC and as a situational awareness feed from the Special Event venue back to those entities. In this application, the implications for using the MITOC in a "preparedness and prevention" role are apparent, and were considered a success by the research team, which was supported by interviews with some users of the MITOC from various agencies at the scene.

B. URBAN JOINT MILITARY/CIVILIAN APPLICATION: COALITION WARRIOR INTEROPERABILITY DEMONSTRATION (CWID) – JUNE 2005

CWID is an annual demonstration of interoperability and collaboration technologies for joint forces.[91] For 2004 and 2005, it was sponsored by United States Northern Command to specifically focus on military support to civil authorities. The MITOC was engaged in CWID 2005 as a test of its ability to serve as an on-scene interface to military assets responding to a WMD terrorist attack that also required joint

[91] Coalition Warrior Interoperability Demonstration (CWID), http://www.cwid.js.mil/c/extranet/home accessed January 2006.

collaboration and interoperability across jurisdictions involving military, local, state, and federal agencies. This event also included the private sector and military supported critical infrastructure. In this case it was a major privately-owned chemical production plant, and a lock and dam on the Ohio River under the jurisdiction of the Army Corps of Engineers. The McAlpine Lock and Dam is a key choke point in one of the highest-capacity shipping channels in the Eastern Hemisphere, being second only to the Panama Canal in regards to commercial tonnage passing through.

CWID participation resulted from the Kentucky National Guard's 41st WMD Civil Support Team (WMD-CST) whose communications team chief, MSgt Al Staples, initiated a joint proposal that created a concept for Joint operations called Kentucky SCENE (Secure Collaborative Engagement Network for Emergencies). The Kentucky SCENE team involved L3/MPRI, a defense contractor; Plangraphics, a geospatial information firm; Pictometry, a high-resolution imagery firm; the National Geospatial Intelligence Agency (NGA), a government intelligence agency; and the University of Louisville's Information Technology Research Center for Homeland Security (iTRC/HS).

The opening of the exercise scenario featured a group of terrorists that gained entry to the chemical plant by overtaking a worker as he arrived, stealing his clothes and ID badge to gain entrance, and then opening a gate for others to enter. They then took over a barge at the loading dock to block river traffic, and the scenario called for a later release of its toxic cargo into the air and river so the plant's on-scene HAZMAT and fire department could practice mutual aid collaboration with the Rubbertown Mutual Aid Association, the nation's oldest mutual aid compact.

The support truck with the MITOC arrived on scene with the initial HAZMAT and law enforcement units, and was directed to the administrative building where the on-scene security provided a quick situation brief. After that location's situation was stabilized, the MITOC moved to the U.S. Army Corps of Engineers headquarters site at the McAlpine Lock and Dam on the Ohio River. Here, the scenario called for a second group of terrorists to attack a chlorine barge in the entrance of the lock to close off this critical waterway. The following technologies were successfully demonstrated for CWID:

1. On-Scene Surveillance and Situational Awareness Sharing

The MITOC team and plant security established an Ethernet connection, from the chemical plant's video surveillance camera network to the MITOC parked outside, by simply running a cable out the window to save time. That direct connection was utilized to upload live on-scene imagery from their digital surveillance system of the plant's grounds to the MITOC's server. The team then routed that live imagery in real time to the local JOC, State EOC, and USNORTHCOM.

Another innovative surveillance application that was accomplished was to feed live streaming video from a Coast Guard vessel underway conducting surveillance of the second mock attack location at the McAlpine Lock and Dam. They were tasked to survey damage to the lock from the water. The National Geospatial Intelligence Agency (NGA), one of the Kentucky SCENE CWID partners, wanted to test the performance of their wireless network with secure encryption capability on live streaming video while underway on a vessel. The MITOC's Wireless Local Area Network (WLAN) was accessed by the NGA team on the Coast Guard vessel and used to successfully transmit their streaming digital video while underway. The imagery was simultaneously accessed and re-transmitted by a National Guard communications vehicle from the 41st WMD Civil Support Team co-located with the MITOC at the scene. The encrypted streaming video signal was then accessed by the local JOC over the standard encrypted Internet feed from the MITOC, while the video was also transmitted over the NIPRNET military Internet feed from the 41st WMD CST vehicle's KU-band satellite connection.

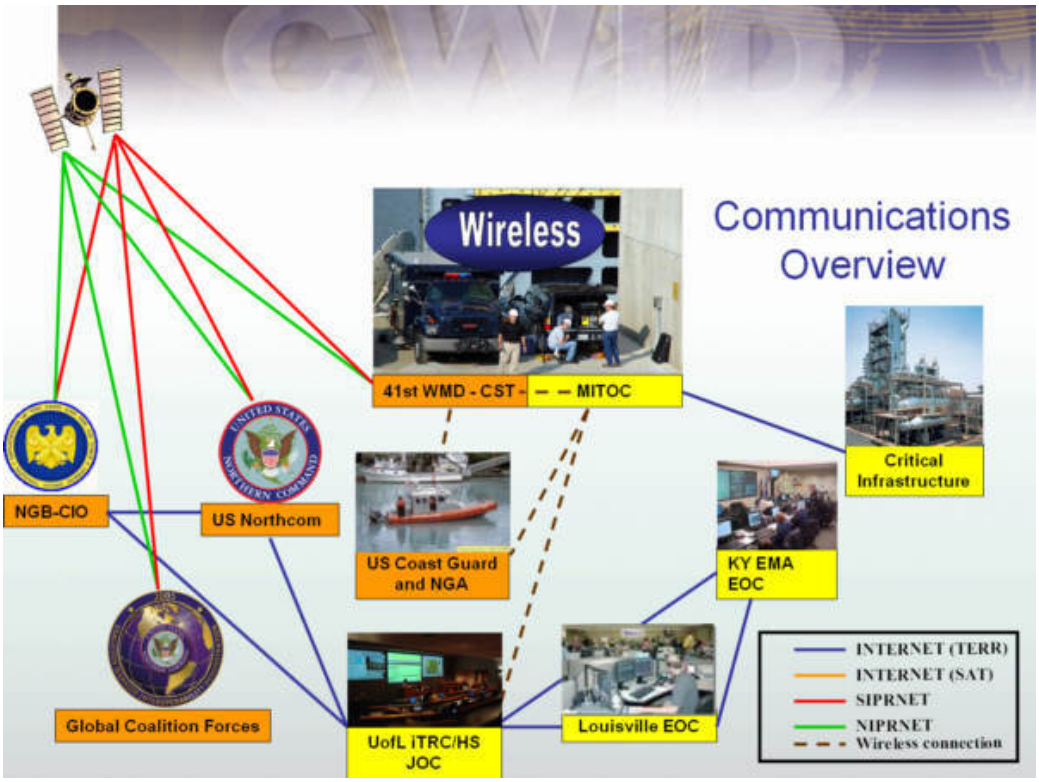

Figure 2. MITOC Communications Overview for CWID 2005

Findings: Creativity and innovation are excellent tools when technical experts are available to look for ways to overcome obstacles to sharing information. Even though the MITOC research team was able to quickly access an on-scene surveillance network at the chemical plant, it does not mean that a typical emergency response team would have someone technically capable of performing the same feat, especially under duress in the heat of a crisis. The experience of the MITOC research demonstrations and exercises illustrated that the most creative ad-hoc solutions occurred when two or more technically proficient operators worked together as a team. Unfortunately, this would probably not be the case in a real deployment unless the previously recommended Incident Command Support Specialist position, staffed by more than one person, was utilized. Therefore, the inclusion of communications and information technology drills in Homeland Security and emergency response preparedness would enhance the ability to address regional or jurisdictional challenges before they are experienced in the field during the emergency.

2. Incident Command Support

The MITOC utilized Plangraphics Spatial Templates for Emergency Preparedness (STEPs) collaboration, and the Geospatial Information Systems portal to access and upload situational awareness data from both incident scenes.

The MITOC's portable weather station was utilized to create a plume dispersion model for both incident scenes and upload the data into STEPs. This provided on-scene situational awareness to the Incident Command Post, since both sites involved chemical leaks that went airborne.

The MITOC also had access to and relayed on-scene input to L3/MPRI's Watch Command Incident Management software. This prototype product had recently been chosen as a statewide emergency management tool that will be located in all EOCs to provide Incident Management reports to the Kentucky EOC. It had not been deployed outside of the State EOC at that time and the CWID demonstration offered an opportunity to test it in a live situation that tied collaborating field units, in this case the MITOC and an Incident Commander, with the state and local EOCs. Watch Command was accessed over a secure web connection and allowed the Incident Commander and field responders to enter Situation Reports (SITREPS) as the event unfolded. Imagery, documents and even live video could be placed in folders, which could be shared with other authorized users at the local JOC, state EOC, and the USNORTHCOM JOC.

Another technology partner, Pictometry International, provided their imagery tool with recent high-resolution photographs of the chemical plant and McAlpine Lock and Dam areas affected by the mock terrorist attack. The forty-five degree high resolution oblique views offered by this resource allowed law enforcement operations commanders to plan their counter-terrorism operations in greater detail. This shared Common Operating Picture included their mark-ups of the imagery that was subsequently shared with other agencies to evaluate potential road blockages, fields of surveillance, and fields of fire before committing to a counter-attack. The high bandwidth provided in the MITOC technical configuration allowed for the easy transfer of the large file sizes of the high-resolution imagery.

Findings: There are many software tools available to first responders and incident commanders for collaboration, decision support, and information sharing. Practitioner use in the field with feedback is the only way to determine their efficacy, since the typical sales collateral always makes it look easy and, in many cases, it is. The primary issue is not the technology. Just as we found in the interoperability of radios, it is the standards of use, protocols, and familiarity with the capabilities that determines how effective the tool becomes to the Incident Commander and his or her responders in the field.

For example, the research project team and the Kentucky SCENE coordinator for our CWID participation set up a training day with plenty of advance notice so our local participating agencies could become familiar with all the new software collaboration and incident management tools to be demonstrated in the CWID trial. There was a low turnout for the training, which ultimately hampered the initial ability for agency representatives, primarily in the JOC, to input data and make their analysis of the situation in a timely fashion to the State EOC and US NORTHCOM's JOC. As the first day of the CWID demonstration progressed, and especially into the second day, the proficiency of the users increased to the point that they could process meaningful information and manipulate the software tools much more effectively. The lesson learned here was that the software resources were not fully effective in delivering on-scene situational awareness and supporting effective joint decision-making because of the initial learning and experiential curve of the users at the remote sites located at the JOC, State EOC, and USNORTHCOM.

3. Summary of Findings

The ability of the MITOC to provide a technology bridge to conduct counter-terrorism operations performed well in a joint operational environment. Its technical configuration and concept of operations supported the goal of CWID 2005 in

demonstrating the ability to conduct joint operations between military and local response agencies—one of USNORTHCOM's core tenets of Military Support to Civil Authorities (MSCA).[92]

The most important issue discovered in the MITOC deployment in support of CWID 2005 did not involve technology. It was clear that the MITOC possessed the technological capability to tightly integrate with the on-scene National Guard WMD-CST communications unit, and provide rich multimedia from the scene to provide robust situational awareness and a common operating picture to others regardless of their location. All these capabilities were blunted somewhat due to incompatible administrative protocols, a lack of prior training, and a lack of experience with the tools at the remote command level, which initially diminished the efficacy of the MITOC's capabilities.

For example, even after months of planning for the event, an administrative edict by the National Guard's Information Technology security department, in the last days before the demonstration, prevented the full integration of the WMD-CST's systems with the local wireless technology component, provided via the MITOC and the NGA's secure WLAN network. Even though the hardware was on-board the WMD-CST vehicle, which would allow full interoperability across the IT domains between the two vehicles and access to the MITOC's wireless network, the National Guard IT Security department declined to allow the communications chief to access the network and conduct this part of the planned tests.

A similar issue arose with the National Geospatial Intelligence Agency's request to allow their encrypted wireless access points to ride the National Guard's network. They were also denied permission to place one of their encrypted wireless access devices on-board a National Guard UH-60 Blackhawk helicopter for testing of the ability to access the local wireless network from the air over the incident scene. The last-minute refusal to grant the helicopter access had more to do with safety issues, however, than IT security. The effort to perform radio interference testing on the ground, to ensure that the

[92] United States Northern Command, "First Responders – Role of NORTHCOM," http://www.northcom.mil/index.cfm?fuseaction=s.first_role accessed January 2006.

wireless signals would not affect the flight safety of the helicopter, was not successful due to a variety of scheduling conflicts and, ultimately, the NGA ran out of time and abandoned that part of the interoperability test.

It is ironic that the goal of CWID was to test interoperability between military and civilian technologies, and an administrative order was what prevented full interoperability to occur—not a lack of technological solutions. From an IT security standpoint, one can somewhat understand the reluctance of the National Guard IT administrators to allow connectivity to a non-military university research project, but it was surprising to see them decline access to a national intelligence agency that deals in the highest levels of security. An all-out effort should have been made to certify the MITOC and NGA's networks used in CWID as temporary low-risk connections in the demonstration. There should be a follow-up with the National Guard to see if there are protocols or guidelines for allowing interconnection with such agencies in the heat of an emergency, as opposed to a demonstration or exercise. This important issue should be addressed in advance, and a protocol put in place between USNORTHCOM and the Department of Homeland Security on behalf of federal, state, and local response agencies if full interoperability of voice *and* data is to be achieved at the moment that it is needed the most, which is in the heat of a crisis.

An unplanned-for event provided some valuable research data for the research project's Summary Findings. The issue of reliability and redundancy in the MITOC's architecture was addressed by accident during CWID 2005. The satellite dish currently utilized by the MITOC for broadband Internet access had not yet been installed when CWID occurred. The research team arranged for trial use of a broadband wireless backbone Internet feed from US Wireless Online, a local business network provider. The network provided by US Wireless Online utilized a long-haul line-of-sight connection from an industry-standard 802.11a transmitter atop one of downtown Louisville's office towers. The McAlpine Lock and Dam site for the CWID demonstration was approximately 6,250 feet from the transmitter. The MITOC team set up alongside a 10-story structure used to mount the replacement lock door and placed an antenna on top of this tower, aimed toward the access point. The NGA also placed their access point nearby

to ensure maximum coverage in the waterway for their part of the demonstration. In a real-world emergency, these actions would have taken an hour or so to accomplish. That also assumes that the response agencies had the right contacts at the site to gain access to the tower. In the case of the CWID demonstration, the MITOC research team had access, the day before, to conduct tests for optimum performance. Since the site was a secure location under jurisdiction of the U.S. Army Corps of Engineers, the research team left the antenna array on top of the tower to save some set-up time for the next day's demonstration. During the night, a major thunderstorm came through and the antenna was apparently hit by lightning and disabled. When the MITOC arrived to begin operations at the McAlpine Lock and Dam site, the wireless broadband backbone feed was dead.

The MITOC research team contacted the vendor for a replacement antenna array. In the meantime, the demonstration went on as planned. Fortunately, the engineer who had designed the MITOC's interoperability equipment had also incorporated a cellular data modem using the CDMA 1xRTT transmission protocol, a fairly ubiquitous cellular data service, as a back-up to obtain Internet access. The cellular modem was quickly routed through the MITOC's router, which enabled sharing and access over the WLAN. Even though it was a relatively slow connection at about 40Kbps, it enabled the research team to upload SITREPs to the CWID JOC, and was perfectly adequate for accessing and sending email messages without large file attachments. After the replacement data radio antenna arrived about an hour later, the network was re-routed to the broadband connection, allowing for multimedia uploads at speeds up to 4Mbps.

This redundancy capability has now been integrated into the MITOC with a more robust service offering from Verizon cellular using their broadband access card. This PCMCIA card is inserted into a laptop card-slot and enables consistent broadband download speeds of 400-700Kbps, around the speed of consumer-grade DSL service, with bursts of up to 2Mbps. This service is available in about 171 major markets at the time of this writing. Outside of those markets, it still works on the CDMA network providing speeds comparable to dial-up access. The card is around $150 and the monthly access fee is $60-80 per month depending upon the plan you have. According to the Verizon service agreement, users are not supposed to use this service in a shared

environment, even though it is technically possible and easily done. To comply with the service agreement, the MITOC utilizes the Verizon card in the Incident Commander's laptop and will not integrate it into the WLAN for exercises and demonstrations. In the event of a real emergency where shared access to the card would provide optimum network access and utilization, a decision will be made to violate the service agreement in the interest of public safety.

Since other major cellular providers such as Cingular and Sprint also offer similar broadband services, the Department of Homeland Security should consider the negotiation of a separate service agreement with these vendors to authorize federal, state, and local response agencies to utilize the unique capabilities of these broadband cellular networks in a shared network fashion. While it is understood that the utility of cellular services could be diminished or rendered inoperable in a large regional disaster such as a major hurricane or a terrorist attack using a nuclear weapon, the ubiquity of these cellular broadband services would greatly benefit routine responses. This fact is far too important to discount as a potential solution to a national broadband capability for first responders at a relatively low cost.

As observed in Hurricane Katrina, cell towers may be damaged or inoperable due to power outages for extended periods, draining back-up battery banks and generator fuel, while congestion from civilian use could clog circuits. There are potential technical counter-measures, even for those extreme cases, as well as the rapid deployment of cells-on-wheels (COWS) and cells-on-light-trucks (COLTS) to the site of a major disaster to quickly restore service, *primarily for emergency responders*.

MITOCs deployed under FEMA with both portable cellular broadband repeaters *and* satellite broadband could be effective in the early hours of a large regional event to provide emergency communications to response agencies. A public-private partnership with national cellular providers to develop a hardened version of cellular service with rapid-deployment of back-up capability should be explored. This approach could provide a less costly solution to improve first-responder communications than waiting until new radios and expanded frequencies eventually replace legacy systems across the country.

In summary, CWID 2005 provided a broad landscape to test various elements of the MITOC's technical architecture, as well as expose some critical operational issues that should be addressed for effective military support to civil authorities. These issues include training and familiarity with the technology solutions by all agencies that will be expected to provide input or collaborate using the tools. The technologies will only be useful if they are utilized in the daily operational routines of the agencies. A doctrine of utilizing these technologies only in emergencies guarantees that their full effectiveness will be significantly diminished.

Protocols for voice and data interoperability and pre-agreed Memorandums of Understanding on interconnections and sharing of information should be worked out and drilled among the military, federal, state, and local organizations that would be expected to work together in a region during a major crisis. Depending upon stressed Incident Commanders to work out the bugs during an event will be counter-productive and possibly detrimental to public safely, security, and property.

C. RURAL LAW ENFORCEMENT APPLICATION: OPERATION DUKES OF HAZARD – SEPTEMBER 2005

This event was a Domestic Terrorism exercise in rural Eastern Kentucky to test the MITOC's ability to provide communications capabilities to local law enforcement and emergency responders in mountainous terrain with no cell phone coverage and limited radio capability. The scenario involved a local law enforcement investigation of what they thought was a typical methamphetamine lab set up in a trailer in a remote area of an abandoned coal mine. Upon entering the area to serve a search warrant, the drug task force officers came under fire from a sniper in an abandoned building. The MITOC was called in to support the law enforcement stand-off with the sniper, as well as to provide intelligence resources to the Incident Commander. As the scenario progressed, intelligence came in to link the suspects to a white supremacist group plotting to build an Ammonium Nitrate – Fuel Oil Solution (ANFO) bomb and use the meth lab as a funding source. This required intelligence gathering, communications with outside agencies,

deployment of a fire department and hazmat team, and assistance from a specialized team with a robot. The MITOC's command post hosted the six separate agencies and provided the IT resources to coordinate a response.

1. The Incident Command Post

Once on-scene, the MITOC's support vehicle and research team located in an area that was secure, yet provided an un-obscured view of the portion of the sky where the satellite is located. A fully operational Incident Command Post was then set up in less than thirty minutes from arrival. This command post's creature comforts and technology, delivered as cargo in the MITOC's SUV, included:

- A folding table and chairs for six operators
- A folding canopy that provided protection from the sun to enhance viewing of laptop screens. It also featured removable sides that can be used in inclement weather.
- Six desk versions of the Cisco VoIP telephones and six wireless handset versions
- A combination printer/scanner/copier/fax
- A 32" LCD display screen
- A remote weather station
- A generator for on-scene power
- 12v batteries for radio operations
- External high-gain antennas to extend the WLAN

2. Radio Interoperability

The MITOC's radio interoperability suite had the capability to link the radios of the Drug Task Force officers and the responding Fire/HAZMAT team. The MITOC team had determined in advance what frequencies were being used by the agencies; once on-scene, it only took a few minutes to program the system to allow for the interoperability to be achieved.

3. Army Research Lab's "Packbot"

One of the co-principal investigators on the MITOC grant is Dr. James Gantt, a retired U.S. Army Colonel, who was the Chief Information Officer for the Army Research Laboratory in Maryland. He now serves as the Director of Murray State University's Telecommunications Systems Management Program, a partner in the MITOC grant. Dr. Gantt arranged for a "Packbot" from the Army Research Lab (ARL) to join the MITOC research team on this exercise to test the ability to integrate the systems. The Packbot is a small lawnmower-sized tracked robot with a retractable "head" that contains high-resolution video cameras, lighting, and infrared sensors. It is designed to be remote controlled over standard Wi-Fi networks and can go into small confined spaces. It has been used successfully in Afghanistan and Iraq in clearing caves and in conducting surveillance of dangerous zones and Improvised Explosive Devices (IEDs). The use of the Packbot with this MITOC exercise was to illustrate the ability for proven military technology to cross over to first responder agencies. For example, Packbot is much smaller, faster, and more agile than the typical robots frequently used by Police S.W.A.T. and bomb-disposal units—at about one-half the cost.

ARL sent two operators who joined the MITOC shortly after arrival on-scene. They were able to establish their own wireless network, but it soon became apparent that the frequencies used by the MITOC interfered with the Packbot's control system. After some adjustment, Packbot was off and running, but there was not enough time to fully integrate its video feed into the MITOC's systems. However, it still provided excellent situational awareness via its own monitor at the scene for the Unified Command Structure established at the MITOC Incident Command Post. The Packbot was sent off after the sniper in the building and was soon sending back a video signal that allowed the on-scene law enforcement incident commander to determine a plan of attack.

4. Geospatial Information System and Plume Dispersion Monitoring

The exercise scenario then progressed to having the Drug Task Force officers corner the sniper, who then used his cell phone to send a signal to detonate the ANFO bomb in the trailer suspected of housing the meth lab. A real ANFO bomb, made from

ten pounds of ammonium nitrate and a few gallons of diesel fuel, totally obliterated the trailer. A HAZMAT team then went downrange to inspect the site while staying in radio communication with the MITOC Incident Command Post.

The Plangraphics STEPs GIS portal was utilized to provide detailed orthographic mapping of the mountainous area of the incident and displayed a clear spatial rendering of where the ICP, the sniper, and suspected meth lab were located in relation to each other. The system's views were able to be shared with all the agencies on the scene and with external locations such as a state EOC or State Police Post, which were simulated in this exercise.

The important issue addressed in the exercise scenario was that there was an elementary school within a short distance, which could have been affected if any dangerous chemicals utilized in meth production were released in a cloud or plume from the trailer explosion. The remote wireless weather system sent back wind speed, wind direction, temperature, and barometric pressure readings that were fed into the CAMEO ALOHA plume dispersion modeling system. It rendered a plume model on a map from the STEPs portal, which was then shared electronically with the responding agencies, as well as printed out in hard copy on the ICP printer. From there, the map could have been faxed from the MITOC or emailed to other agencies off site. The plume model indicated that the school was not in danger from the hypothetical chemical cloud and did not need to be evacuated.

5. Broadband Internet Access

Access to broadband Internet via the satellite system allowed the Incident Commander, the local Emergency Management Agency Director under a Unified Command Structure, to pull up Material Safety Data Sheet (MSDS) information from the web, which provided critical information on the potential chemicals that are typically seen in methamphetamine production. The MSDS data gives volatility, specific gravity, and interaction information to HAZMAT responders. Even though a lot of the same information is contained in voluminous hard copy binders carried in the hazmat trucks, a simple search on the Internet allowed the MSDS sheet to be accessed and printed for

more than one responder to view. The MITOC also had a software package on-board that provides for modeling different chemical mixtures and their combined effects if mixed in a situation similar to the exercise's explosion.

6. Summary of Findings

This was the first exercise deployment for the MITOC that had all of the technology elements (proposed in the original grant proposal to the Department of Homeland Security) installed and working in an integrated fashion. It was an important test of the overall systems integrity and efficacy in the rugged rural environment.

Even though all the Incident Command Post components were initially operational within thirty minutes, such as the weather station, laptops, WLAN and phone-to-phone communications, the satellite dish initially failed to lock onto the satellite. This delayed the use of Internet access for the MITOC for over an hour. Even though cellular service was not accessible in the mountainous terrain, the MITOC's back-up Globalstar satellite telephone unit allowed the MITOC team to transmit and receive email or fax. The team was also able to place a call to the satellite system provider to assist the MITOC technician in trouble-shooting the dish. The technical support determined that the power-up sequence the technician used was incorrect and, once the system was correctly re-initiated, the satellite dish was quickly locked on providing broadband access to the WLAN. This situation again illustrated the importance of having a back-up plan with redundant communications capabilities and was a valuable lesson learned from our experienced engineer.

The radio interoperability was easily achieved in this case because of careful advance planning. By determining the frequencies that were already being used by the responding agencies, the MITOC technician was prepared with the right cables to make the required radio connections. This is the type of activity that needs to take place, in advance, in all agencies that expect to require any type of radio interoperability among mutual aid responses or cross-agency deployments.

The ARL Packbot could have easily been integrated with the MITOC's sub-systems if there was additional time available to make and test the connections. It did

perform its counter-terrorism tasks as expected—with the exception of some down-time due to splashing into a puddle of water that temporarily shorted out its electronics. The unit had to be partially disassembled to be dried out. The exercise did illustrate the advantage of having proven military technology available to be acquired by state and local agencies since the Packbot can be now commercially acquired from its manufacturer, iRobot; the same firm that makes the "Roomba" robotic vacuum cleaner. With time and mass distribution, the Packbot's $80,000 price tag may come down enough to see use by response agencies on a shared resource basis, similar to what the MITOC research team advocates for the MITOC system. Future testing to achieve full integration with MITOC will determine if it should be an "optional accessory" as the MITOC is commercialized.

The GIS and plume modeling tools were essential to this type of scenario and, from talking to the responders; they would not have had these types of resources at the scene with their existing agencies. The MITOC's ability to deliver telephone communications and Internet access to the remote scene at a reasonable cost was also deemed advantageous by the response agencies and the head of the local emergency management agency.[93] This appears to indicate that MITOC deployments on a shared regional basis would be a valuable tool in the preparedness and response capabilities of rural jurisdictions.

D. MEDICAL OPERATIONS/EXERCISE SUPPORT APPLICATION: OPERATION SINBAD – DECEMBER 2005

Operation SINBAD (**S**outhern **In**diana **B**ioterrorism **A**ttack and **D**efense) was a regional full-scale exercise over two days, encompassing over twenty response agencies and nearly five-hundred participants. It took place at the Indiana National Guard's Muscatatuck Urban Training Center in south-central Indiana and was sponsored by the Indiana Department of Homeland Security.

[93] Per statements made by Charles Caldwell, Perry County Director of Emergency Management, and Officer Dan Smoots, Kentucky Operation Unite Anti-drug Task Force captured on news report video from Heartland News provided to the MITOC research team by the station.

The MITOC research team was contracted to design and implement the exercise as well as serve as the Exercise Control Team. This type of operation required radio coordination and commands to field Controllers and Evaluators.

1. MITOC as a Portable EOC

The MITOC's ability to be removed from the support vehicle and utilized as a stand-alone portable "EOC-in-a-box" with telephones, radios, and laptops proved to be a valuable asset to the Exercise Control Team. It also provided a Case Study on its effectiveness as a support infrastructure to serve as an ad-hoc EOC where none currently exists.

Upon arrival at the exercise venue, the MITOC was unloaded from the SUV by a two-man crew who lifted it out and set it on its form-fitted roller pallet. It was then easily rolled into the building assigned as our Exercise Control Center. Since power, telephone lines, and Ethernet access to the Internet were available in that building, the satellite dish did not need to be deployed. The MITOC was able to integrate the dial-tone from the National Guard base's phone system and share several lines among the system's VoIP telephones, both desk and wireless handset models. The MITOC also took the Ethernet line into its server and used that to provide the Wi-Fi network for the handset phones and laptop computers.

2. Radio Interoperability for Exercise Control

The various response agencies that generally participate in these types of exercises should mirror real world operating conditions, including challenges faced in mutual aid deployments. In real life, they also usually operate on different radio frequencies with the requisite interoperability issues. Even though the MITOC's interoperability capability could have been used to address any interoperability issues with the participating agencies, a decision was made that they should drill with the assets they would normally bring to the scene. The MITOC's capabilities, however, still provided a valuable function using the system's radio interoperability suite to support the Exercise Control Team.

The capability for the MITOC to monitor the various response agencies' frequencies was a unique attribute that added significant value to the Exercise Control Team. For example, a controller would make a call to the 911 Dispatch Center for a simulated incident. Unlike most other exercises, however, the controller could then monitor how long it took the dispatcher to radio the dispatch and even evaluate how accurate the dispatch was in relation to the call into 911. The controller could then monitor the radio message traffic of all agencies responding to the incident, and any miscommunications during the relaying of information between them, since they, themselves, did not have interoperability between the federal, state, and local response commands.

The MITOC was also used to extend the range of the controller radio network by bridging several cheap Cobra FRS (Family Radio Service) radios with the MITOC's larger base station and professional handheld radios.

3. MITOC as a Medical and Public Health Support Resource

The MITOC also served as a resource to the medical and Public Health agencies responding to the simulated bioterrorism mass casualty attack involving pneumonic plague in the second day of Operation SINBAD. In this exercise, as in real life, such a mass casualty bioterrorism or pandemic outbreak event would require the establishment of a medical point-of-dispensing (POD) of medications to the affected or exposed public. In this simulated event, up to ten thousand area citizens were potentially exposed, and the various public health agencies coordinated a POD at a school for the orderly dispensing of antibiotics. To accommodate the projected patient load of 300-400 patients per hour, approximately eighty public health, medical, and security personnel were involved in the exercise. They had requested telephones from the National Guard for the school building used as the site of the POD. They did not, however, request Internet access for any computers to access external resources. Even though it was not necessary in the exercise, a real life deployment such as this would have required Internet access to share information with area hospitals as well as State Public Health, CDC, and federal Health and Human Services Headquarters.

The MITOC was moved to the POD site and connected to a SUV outside the building for its satellite Internet access. This capability illustrated the efficacy of utilizing the MITOC in a public health POD, or even a medical field hospital or emergency triage site set up in an area with no infrastructure.

4. Summary of Findings

The MITOC system was set up in less than an hour illustrating that a larger multi-station EOC version could have been easily set up during an emergency, accommodating up to thirty-six telephones and computers using the MITOC infrastructure.
The ability of the MITOC to serve as an exercise control system was a surprising new capability that only came about by accident. It will be addressed in future exercises and developed into one of its marketable applications.

The medical and public health applications are obviously critical capabilities since a mass casualty attack or major natural disaster would require rapid deployment of medical resources to an area that may be devoid of infrastructure due to damage. MITOC could support robust communications to and from the site, including videoconferencing and telemetry of patient data such as x-rays, lab tests, and CT scans. This capability, known as telemedicine, has been field-proven in military field hospitals. The exercise illustrated that MITOC can rapidly bring remote telemedicine capability to the site of a terrorist attack or natural disaster, and at a reasonable investment.

E. MITOC'S OPERATIONAL MISSION: THE JOINT ESU

The Joint Emergency Services Unit (Joint ESU) is a new concept first fielded in Metro Louisville that is a joint tactical response team comprised of law enforcement S.W.A.T. team members, HAZMAT specialists, and public health specialists. The original idea came about during an exercise held by our Metro Louisville Crisis Group where the scenario featured a group of terrorists releasing a nerve gas inside a school. When the first fire/hazmat team arrived, they could not enter the building to assist any victims because the heavily armed terrorists were still in the building. Even when the local FBI's tactical team arrived, they could not enter the building to neutralize the

terrorist since none of them, or the police S.W.A.T. team, had been trained in Personal Protective Equipment (PPE) rated for nerve gas, which is referred to as Level A protection.

To remedy this situation, an initial cadre of local FBI agents was trained at the HAZMAT Technician level that would allow them to enter the most hazardous environments. However, this only addressed part of the problem. In 2004, the emergence of SARS, a deadly airborne pathogenic virus, presented some difficult challenges for the public health community. In the event of a potential pandemic outbreak due to a disease like SARS or a bioterrorism attack, public health officials may need to enforce a quarantine and/or isolation of passengers exposed to someone who is a suspected carrier of disease coming in on an airline flight. Allowing the passengers to disembark risks the potential spread of the disease in the community where they landed. A crowd control issue may arise if they all wanted to quickly get off the plane out of fear of being contaminated or further exposed.

As a response to that dilemma, some initial funding and support from the United States Marshals, plus strong leadership from advocates from the Federal Protective Service and the Police S.W.A.T. Team Surgeon, established the Medical Assist Tactical Team (MATT) in late 2004. This concept called for all the MATT's tactical law enforcement team members to be trained and range certified with their weapons in various PPE. The concept of operation for the MATT also called for HAZMAT team members to be trained in tactical entry techniques. They are to follow the law enforcement tactical team in to test a suspected hazardous environment for WMD or a suspected human biologic vector while the tactical team secures the surrounding environment.

The MATT's name was changed to the Joint ESU in 2005, with strong support and funding from the Kentucky Office of Homeland Security. The operational mission expanded to potential deployments anywhere in the Commonwealth of Kentucky. In

addition, the U.S. Marshals Service is now in the process of deputizing all the sworn law enforcement personnel to allow the Joint ESU to conduct operations anywhere in the United States.

Since this fifty-plus member joint team is assembled from various agencies, their individual radios do not have the same frequencies. Any one of the team members could serve as the Incident Commander. They also do not have any common information-sharing protocols or collaboration software tools. Their funding allows for some

equipment acquisition for command and control, which will need to be carefully considered to allow for maximum flexibility among the various agencies, as well as interoperability.

The MITOC research team was invited to join the Joint ESU in late 2005, to bring advanced Information Technology tools, communications and computer consulting, and on-scene support to the Joint ESU Incident Commander with the MITOC. This unique opportunity will allow the Joint ESU to serve as a "living laboratory," enabling the MITOC research team to assess the MITOC's current and future technology solutions, *as well as* the proposed operational protocols within this thesis in an actual operational environment.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

The research conducted during the MITOC project for the Science and Technology Directorate of the Department of Homeland Security—consisting of performance evaluations, demonstrations, and user reactions, plus the relevant literature discovered—confirm the initial problem statement for this thesis. The field research illustrated an acute need for a resource like the MITOC at the Incident Command level—the focus of this thesis. The after-action reviews of the MITOC's capabilities during multiple preparedness and response exercises in various environments, user and observer reactions, and the performance of the MITOC's integrated technology suite over the nine months of the research project's first phase, indicate that the efficacy of the overall concept is sound.

The research also uncovered and/or validated additional viable applications for the MITOC, outside of the typical Homeland Security-related Incident Command support mission that the initial research focused on. These additional applications seem outside the scope of this thesis on the surface; however; business continuity, medical triage or point of dispensing, and exercise command and control situations all have Incident Commanders. An Incident Commander, in practice, could just as easily be a doctor in charge of a field triage tent or a corporate CIO in charge of keeping a company's voice and data flowing after a natural disaster. The Incident Command Structure, endorsed and amplified by the adoption of NIMS and the National Response Plan, is a viable crisis management tool for businesses to adopt to improve crisis response and disaster recovery, and is endorsed by the business continuity industry.

A. VALIDATING THE METHODOLOGY

The objective of this thesis is to *validate a method to enhance collaboration and situational awareness at the Incident Command level.* The utilization of the MITOC as the tool, and its proposed concept of operation, is the method this thesis seeks to validate.

To ensure that all of the initial critical elements referenced in the Introduction section of this thesis are addressed by the MITOC and its concept of operation, each one is reviewed in the following paragraphs.

1. Immediate Access to Documentation Regarding Local Assets and Response Guidelines

The Broadband Internet capability of the MITOC, either by satellite or broadband cellular, gives the Incident Commander the ability to obtain this information if it is held by their jurisdiction at an Internet-accessible resource at another location like the EOC, for example. The MITOC technology suite also has that information resident in its on-board laptops and server, in the event that an Internet connection cannot be established. Response guidelines are also available in PDA format that can be carried by first responders and Incident Commanders at the scene.

The currently available technology is not expensive or difficult to use to perform this task. In fact, a fully-equipped MITOC is not necessary to achieve this goal, if the Incident Commander's jurisdiction would adopt the practice of having this information collected, consistently updated, and available on a laptop or PDA assigned to the response agencies. Therefore, we have a policy and information infrastructure, such as data collection, for the local assets and administration of the database as an issue that needs to be addressed before the technology can effectively deliver it to the Incident Commander.

The final assessment of whether the MITOC and its concept of operations achieves this goal is "Yes," but is dependent upon local jurisdiction policies for some of the relevant data.

2. The Ability to Refine, Update, and Manage Content from the Field

The MITOC's technology suite allows for this function, which is the core ability to provide situational awareness *from* the incident scene to share that information with other agencies either at the scene, en route, or at a command center located elsewhere, such as an EOC or JFO.

For example, the CWID 2005 demonstration illustrated this capability when live video of the incident scene was successfully transmitted to USNORTHCOM, thereby enabling simultaneous viewing by coalition partners in twenty-five countries around the planet. In addition, the ability of the MITOC's technology suite demonstrated the ability to mark-up and share high-resolution photos from the scene and transmit situation reports (SITREPS) to EOCs and USNORTHCOM in the relative comfort of an air-conditioned cabin of the support vehicle on a 96-degree summer day.

The final assessment of whether the MITOC and it concept of operations achieves this goal is "Yes."

3. Real-Time Collaborative Information Sharing across Jurisdictions and Agencies

The MITOC and its collaboration tools demonstrated the ability to access, share, and conduct real-time collaboration across jurisdictions, agencies, and locations. Several software tools were utilized as the user-interface to accomplish this task during the nine months of the initial phase of the project. Some products performed better than others, some were more user-friendly, and some were poorly designed from an efficiency standpoint—both for the user and the handling of information.

The key aspect to this goal is that the MITOC was the transmission medium and a method to present selected collaboration tools to the Incident Commander. The various collaboration technologies to perform this task exist in the marketplace in various levels of performance and costs. The MITOC did prove, however, to be an effective modality to receive, input, and share information in a collaborative fashion among the people and organizations involved in the exercises and demonstrations.

Once again, the issue of policy is more central to the ability for the Incident Commander to gain value from this ability. The technology to achieve collaboration is not the primary need, since solutions are readily available and the MITOC serves as an excellent way to present the technology to the Incident Commander. A policy by the participating agencies, on what collaboration tools to use and the training to properly use them, is the larger issue to address.

For example, the Department of Homeland Security has the HSIN, which was designed to serve as a standardized collaboration tool. Its collaboration module, based on a proven collaboration platform, would be able to accomplish this goal. What is needed is a policy to take this tool deeper into the response chain—to the Incident Command level—and encourage its use in everyday responses requiring collaboration across various agencies. These would include large HAZMAT events, as well as responses to natural disasters such as wildfires, tornadoes, floods, or hurricanes. By utilizing HSIN everyday, users and agencies would not have to break open the instruction manual in the event of a catastrophic disaster or terrorist attack.

The final assessment of whether the MITOC achieves this goal is "Yes." The caveat is that *effective* collaboration and information sharing is dependant upon agency and jurisdiction policy, plus the users' acceptance, training, and familiarity— as opposed to the technology.

4. Better Project and Resource Management Capability

"Project management" could be construed, for the purpose of this thesis, as the ability of the Incident Commander to manage the incident (the project). In that case, the MITOC's performance in the field supports this notion. Project Management at the Incident Command level requires information and situational awareness, which the MITOC is well-equipped to deliver.

Resource management is one of the key roles of the Incident Commander, whether those resources are personnel, fire trucks, medical supplies, or Level A HAZMAT gear. The MITOC illustrated that its technology capability was ideal to provide the Incident Commander with robust radio interoperability for on-site resource management across agencies. It also demonstrated the ability to reach back to off-site providers of additional resources via its Internet and telephony applications. The ability to determine the availability of off-site resources from the incident scene, and then be able to determine where to stage and deploy them, was accomplished with the mapping and database access capability of the MITOC.

To be realistic, this stated goal, as gleaned from the commission reports referenced in the Introduction, most likely refers to attributes the authors saw as needed at a level well above the Incident Commander. The final assessment, as these attributes relate to the MITOC providing them to the Incident Commander, however, is "Yes."

5. Mapping and Visual Graphic Support

The old idiom that "a picture tells a thousand words" is applicable to the needs of the Incident Commander and those offsite who need to understand the situation at the incident scene.

The mapping capability tested in the MITOC was a combination of Internet-accessible GIS data from central resources and/or databases, as well as maps locally resident on laptop computers. For example, a GPS navigation system with its on-board map was utilized on several occasions to find the way to the incident scene in an unfamiliar area. It was also utilized to mark a "waypoint," or marker, on its internal map to indicate the location of buildings or a specific site that could be referenced by latitude and longitude to be used for later reference. This data can also be shared with other responders on their way to the incident scene so they can pull up maps of the site to plan their deployment locations.

One discovery in the process of testing the GIS mapping applications was that dynamic data pulled from a central database may require more bandwidth than necessary in some software applications. The MITOC had sufficient bandwidth with its satellite capability; however, if it was not functional, the back-up cellular or satellite telephone data connection would not be able to deliver acceptable performance. Therefore, the MITOC research team's recommendation in later demonstrations was to load all relevant mapping data for the jurisdiction being serviced by the MITOC on its resident server and laptop computers to speed performance. That being said, however, GIS mapping tools proved to be a critical and very useful tool in the Incident Commander's arsenal for situational awareness and planning.

Visual Graphic Support allows the Incident Commander to "see the common operating picture" whether it is the big picture, such as a satellite orthographic view of

the layout and terrain at the incident scene or a video image from a remote surveillance camera being beamed back to the MITOC and simultaneously shared with other relevant observers. To achieve maximum visual fidelity, the MITOC was equipped with a daylight viewable screen on a 17-inch, high-resolution monitor within its portable transit case. For use inside the support vehicle's cabin, or a building where the MITOC is set up as an ad-hoc EOC, a high-resolution 32-inch LCD screen that can display computer data or video imagery is recommended. Even if the Incident Commander preferred to stand outside the CTU's cabin, the display screen's articulated arm would allow the unit to be positioned at the door of the cabin for the Incident Commander and others at the Incident Command Post to view.

The final assessment whether the MITOC accomplished this goal is "Yes."

6. Access to Intelligence Analysis

This attribute was not tested during the MITOC research project, only due to the fact that the research team did not have access to intelligence resources during the exercises and demonstrations. The MITOC research demonstrated the ability to utilize commercially available, high-level encryption and encryption utilized by military and government intelligence agencies. The MITOC can provide the modality to access such intelligence reports securely in the field if available to the Incident Commander, and if an effective policy is developed on how it is to be used and protected once accessed in the field.

The final assessment of whether the MITOC achieved this goal is theoretically "Yes," however, it was not actually demonstrated with real intelligence in practice.

7. Decision Support Technology

Decision Support System (DSS) technology could be used as a descriptor for most of the Information Technology, both hardware and software, utilized with the MITOC project. A specific example would be the on-scene weather and plume dispersion modeling capability that would support a decision on where to stage resources or evacuate an area. Another example would be the MITOC's advanced imagery capability

that was demonstrated, with both satellite and aerial photography, to provide better decision making on staging an assault or re-routing traffic.

One of the future capabilities that MITOC could support via its on-board computing and remote database access capability would be advanced decision-support technology, which would utilize intelligent agents and predictive modeling software, coupled with input from on-site sensors and other situational awareness data to provide the Incident Commander with options for action. Coupled with the Incident Commander's intuitive capacity to make decisions, the options presented with multiple outcomes, based on real-time data may allow for more effective decision-making. This technology is in its infancy, yet offers a great subject for future research, testing, and a thesis.

The final assessment of whether the MITOC achieved this goal is theoretically "Yes," however, it was not actually demonstrated with a sophisticated DSS tool in practice.

8. Interoperability of Voice and Data Communications among Local, State, and Federal Resources

Nearly every congressional study, think-tank article, and commission report on shortcomings in emergency response capabilities since the Murrah Federal Building bombing in Oklahoma City in 1995, refer to communications problems and the lack of interoperability among first responders of various agencies involved in the event.[94] Over ten years after the Oklahoma City bombing the problem is still being addressed.

Some of these reports, such as the FEMA report entitled "Responding to Events of National Significance," specifically recommend portable communications capability as a potential solution, illustrated by a description of a FDNY project similar to the proposed MITOC.[95]

---

94 Alfred P. Murrah Federal Building Bombing, April 19, 1995: *Final Report*, 10, http://www.mipt.org/pdf/okcfr_part1.pdf accessed February 2006.

95 FEMA, *Responding to Incidents of National Consequence, Recommendations for America's Fire and Emergency Services based on the Events of September 11, 2001, and Other Similar Incidents*, 59. http://knxup2.ad.nps.navy.mil/homesec/docs/dhs/nps03-060104-03.pdf last accessed February 2006.

Interoperability of voice and data was one of the key capabilities that the research team addressed with the concept and design of the MITOC. Various products for radio interoperability were investigated and tested. They all performed the job; however, vastly different price points and varying ease of use were noted.

The research team's conclusions agree with the assessment of the National Association of State Chief Information Officers (NASCIO) who stated that true interoperability requires far more than just patching radio channels together.[96] Indeed, an argument can be made that usage protocols, policies regarding standardization of both equipment and channel allocation, along with other human factors, are more important than new technologies. Indeed, a department or agency can put an untrained operator at a scene with sophisticated radio interoperability equipment and create even more chaos by patching together already overtaxed radio channels. A detailed communications plan for all departments expected to work together in a jurisdiction, and adherence to that plan, is critical until a national template or standardization of at least tactical channel allocation is provided. Otherwise, all the technology that the MITOC, or any other mobile command post, can bring to the scene for the Incident Commander will be useless.

The final assessment of whether the MITOC achieved this goal is theoretically "Yes."

B. VALIDATION OF THE MITOC AND ITS CONCEPT OF OPERATION

The MITOC field research results, and relevant literature discovered, provide a strong argument that a portable, cost-effective, and easy-to-use tactical operations center would be a valuable tool to address the initial problem statement of this thesis. Hurricane Katrina's impact on the communications infrastructure of the Gulf Coast provided the strongest endorsement and irrefutable evidence that rapidly-deployable portable communications systems that provide command and control, information sharing, and collaboration are critical in responding to major disasters. One of the key

[96] NASCIO Research Brief, "We Need to Talk: Governance Models to Advance Communications Interoperability", November 2005, 2, https://www.nascio.org/nascioCommittees/interoperability/Interop.%20Gov.%20Research%20Brief%20Final.pdf , last accessed February 2006.

recommendations from the White House Report on Lessons Learned from Hurricane Katrina describes a MITOC-like capability as a critical technology to field in response to major disasters.[97] The same justification for the need of such a resource can be attributed to lesser emergencies as well.

The MITOC should be viewed as an integrated suite of the best tools to provide the technological solutions to the challenges faced by the Incident Commander. It is not a new invention, since mobile command posts have been around as long as four wheels supported a wagon. What is important is that its concept is flexible and accessible to smaller jurisdictions. For example, rather than use Homeland Security grant money to buy an $800,000 police command bus like neighboring Montgomery County, Virginia; Maryland's Prince Georges County spend $140,000 on four Chevy Tahoe SUVs equipped with communications systems that provided many of the same capabilities.[98] The MITOC concept of operations embodies that kind of fiscal responsibility.

The research project found that some of the technologies, such as mobile satellite Internet and phones, do not seem to have the stability and reliability required for a public safety response without alternate back-up capability. Customer service is reminiscent of the early days of the split-up of AT&T when dozens of start-up telephone equipment "interconnect" companies joined the marketplace overnight, selling telephone equipment to newly liberated businesses and consumers. Many of them, however, had no concept of customer service or quality of service. The public safety satellite and communications provider quality will undoubtedly improve over time, but lives can be at stake; therefore, the service provider that understands this first will come out a winner.

Perhaps even more important is the concept of operations that the MITOC research validated. The technology is available to address the problem statement; however, the implementation rests with the ability of someone to act as the man-machine

---

[97] U. S. Government, The White House, "The Federal Response to Hurricane Katrina: Lessons Learned," 23 February 2006, Appendix A, http://www.whitehouse.gov/reports/katrina-lessons-learned/appendix-a.html, accessed February 2006.

[98] J. Becker, S. Cohen, S. Hsu, "Anti-terrorism Funds Buy Wide Array of Pet Projects," *Washington Post*, November 23, 2003, http://www.washingtonpost.com/wp-dyn/articles/A6311-2003Nov22_5.html, last accessed February 2006.

interface for the Incident Commander. The MITOC concept, combined with the proposed Incident Command Support Specialist (ICSS), fulfills that objective.

In the end, providing more effective communications and information sharing to support the Incident Commander still comes down to the human factor; people are the ones doing the talking, sharing, and collaborating—not machines. The MITOC is a relatively simple, yet elegant integration of the best of breed technologies to *assist* the process of human interaction, both verbal and visual, in a package that is not technically intimidating, and that is easy to get to when it is needed the most.

The research conducted for the MITOC project, both in the field and from the relevant literature, validates the proposal posited within this thesis. To provide better support to the Incident Commander, the agency or jurisdiction should first make sure they thoroughly understand their communications and information needs. They should then establish strong relationships with neighboring jurisdictions using memorandums of understanding on communication protocols. They should comply with emerging communications standards as they make new equipment procurements. Then they will be well-prepared to implement the proposed *Incident Command Support Specialist* position with properly trained staff or volunteers. Once this is accomplished, a MITOC and its proposed concept of operations, as described and proposed within this thesis, would serve as an excellent method to enhance the situational awareness and information sharing at the Incident Command Level.

LIST OF REFERENCES

9/11 Commission. *The 9/11 Commission Report*. New York: W.W. Norton & Company, Inc., 2004.

Alfred P. Murrah Federal Building Bombing. *Final Report*. April 19, 1995. http://www.mipt.org/pdf/okcfr_part1.pdf. Accessed February 2006.

Brill, Steven. *After*. New York: Simon & Schuster, 2003..

Cooper, Steven. "Interview with Steven Cooper." *Journal of Homeland Security (*2002). http://www.homelandsecurity.org/journal/Interviews/displayInterview.asp?interview=18. Accessed April 2004.

Eisenberg, Jon and Craig Partridge. *The Internet Under Crisis Conditions: Learning from September 11*. Telecommunications Policy Research Conference, 2003. http://tprc.org/papers/2003/195/net911.pdf. Accessed February 2006.

FDNY Strategic Plan. 2004. Goal 6.0. *Advance Technology*. http://www.nyc.gov/html/fdny/pdf/pr/2004/strategic_plan/goal_6.pdf. Accessed December 2005.

Frank, Diane. "Bringing broadband to public safety." *Federal Computer Week*, 2004. http://www.fcw.com/fcw/articles/2004/1018/feat-dcbroad-10-18-04.asp. Accessed June 2005.

Gilmore Commission V. *Forging America's New Normalcy*. Arlington: The Rand Corporation, 2003.

Gordon, Ellen. Emergency Information Infrastructure Project Virtual Forum. Transcript of Forum Presentation: *Homeland Security in the Heartland*, 2001. http://www.emforum.org/vforum/lc011128.htm. Accessed April 2004.

Harvard University. *Beyond the Beltway: Focusing on Hometown Security, Recommendations for State and Local Domestic Preparedness Planning A Year After 9-11*. 2002. http://bcsia.ksg.harvard.edu/BCSIA_content/documents/beyond_the_beltway.pdf. Accessed April 2005.

Hoffman, Thomas. "After Katrina Valero Energy Turns to Satellite Communications." *Computerworld*, 2005. http://www.computerworld.com/mobiletopics/mobile/story/0,10801,104477,00.html. Accessed November 2005.

Incident Dispatch.Net. http://www.incidentdispatch.net/intro.htm. Accessed December 2005.

Incident Dispatch Teams. www.springhillfire.com/class_of_1999.htm. Accessed December 2005

Jamieson, Gil. Emergency Information Infrastructure Project Virtual Forum, Transcript of Forum Presentation: *The NIMS Integration Center Implementing the National Incident Management System.* 2004. http://www.emforum.org/vforum/lc040825.htm. Accessed July 2005.

Larsen, Randall. "Incident Dispatchers Can Lighten an IC's Load." *Homeland Protection Professional*, 2004.

_____. "More than Just Connecting Radios." *Homeland Protection Professional*. 2005.

_____. "Roomier, tougher, better: If there were an Olympics for mobile comm. centers, the latest models would be real contenders." *Homeland Protection Professional*. 2004.

Leiner, Barry et al. *A Brief History of the Internet*. Internet Society, 2003. http://www.isoc.org/internet/history/brief.shtml#Authors. Accessed April 2004.

Martin, Robert. Emergency Information Infrastructure Project Virtual Forum. Transcript of Forum Presentation: *Emergency Provider Access Directory (EPAD); Empowering Emergency Communication.* 2004. http://www.emforum.org/vforum/lc040602.htm. Accessed December, 2005.

Mateson, Robert. "Supporting the Incident Commander: The Command Post Forward/Incident Response Team Approach." *International Association of Emergency Management Bulletin.* 2004.

McQueary, Charles. "Meeting the Challenge of Protecting the Homeland." *TechComm National Journal of Technology Commercialization.* 2004. http://www.techcommjournal.com/PDFSVol2No1/10-12HOMELAND,10,12.pdf. Accessed June 2004

NASCIO Research Brief. *We Need to Talk: Governance Models to Advance Communications Interoperability*. 2005. https://www.nascio.org/nascioCommittees/interoperability/Interop.%20Gov.%20Research%20Brief%20Final.pdf. Accessed February 2006.

National Commission on Terrorist Attacks Upon the United States. *Testimony of the Former Commissioner of the New York City Office of Emergency Management, Richard J. Sheirer*. 2004.http://knxup2.hsdl.org/homesec/docs/dhs/nps03-052004-06.pdf. Accessed January 2005.

National Institute of Justice. *When They Can't Talk, Lives Are Lost*. National Task Force on Interoperability. 2003. http://www.safecomprogram.gov/SAFECOM/library/interoperabilitybasics/1160_nationaltask.htm. Accessed April 2005.

National Institute of Justice. *Why Can't We Talk*. National Task Force on Interoperability. 2003. http://www.agileprogram.org/ntfi/ntfi_guide.pdf. Accessed April 2005.

Proctor, Steven. "First Responders Lack Radio Training." *Primedia Business Magazines and Media*. 2004. http://www.findarticles.com/p/articles/mi_m0HEP/is_6_22/ai_n6067591#continue. Accessed 13 December 2005.

Public Entity Risk Institute. *Local Government Preparation for Bioterrorist Acts*. 2001. http://www.riskinstitute.org/ptrdocs/LocalGovernmentPreparationforBioterroristActs.pdf. Accessed June 2005.

Rockwell, Mark. "Rural Carriers Key To Broadband Vision." *Wireless Week*. 2004. http://www.wirelessweek.com/article/CA440742?spacedesc=Departments&stt=001 Accessed June 2005.

Tobin, Rick. The Emergency Information Infrastructure Project Virtual Forum. Transcript of Forum Presentation: *Improving Homeland Security: Continuing Challenges and Opportunities*. 2004. http://www.emforum.org/vforum/lc040324.htm. Accessed July 2005.

U.S. Department of Homeland Security. *Homeland Security Information Network*. http://www.dhs.gov/dhspublic/display?theme=43&content=3648&print=true. Accessed December 2005.

U.S. Department of Homeland Security, *National Response Plan*. 2004. http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml. Accessed June 2005.

U.S. Federal Emergency Management Agency. *Mobile Operations Capability Guide for Emergency Managers and Planners*. http://www.fema.gov/rrr/mers01.shtm. Accessed December 2005.

U.S. Federal Emergency Management Agency. *National Incident Management System*. 2004. http://www.fema.gov/pdf/nims/nims_doc_full.pdf. Accessed June 2005.

U.S. Federal Emergency Management Agency. *Responding to Incidents of National Consequence. Recommendations for America's Fire and Emergency Services based on the Events of September 11, 2001, and Other Similar Incidents*. N.d. http://knxup2.ad.nps.navy.mil/homesec/docs/dhs/nps03-060104-03.pdf. Accessed February 2006.

U.S. Government. The White House. *The Federal Response to Hurricane Katrina: Lessons Learned.* 2006. Appendix A. http://www.whitehouse.gov/reports/katrina-lessons-learned/appendix-a.html. Accessed February 2006

U.S. House of Representatives. *Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, A Failure of Initiative.* 2006. http://www.gpaccess.gov/congress/index.html. Accessed February 2006.

U.S. Northern Command. *First Responders – Role of NORTHCOM*. http://www.northcom.mil/index.cfm?fuseaction=s.first_role. Accessed January 2006.

Yagerman, Barbara. Emergency Information Infrastructure Project Virtual Forum, Transcript of Forum Presentation: *The National Response Plan: An Update.* 2004. http://www.emforum.org/vforum/lc040915.htm/ Accessed July 2005.

Zeichner Risk Analytics, LLC. *Critical Infrastructure Protection Project*. National Center for Technology and Law, George Mason University School of Law, 2003. http://techcenter.gmu.edu/programs/cipp/cip_report/cip_report_2.4.pdf. Accessed October 2005.

Zykowski, John. "First Responders Gear Up." *Federal Computer Week*. 2003. http://www.fcw.com/supplements/homeland/2003/sup3/hom-edit-08-25-03.asp. Accessed March 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Tom Housel
   Naval Postgraduate School
   Monterey, California

4. Dr. Richard Bergin
   Naval Postgraduate School
   Monterey, California

5. Dr. David Simpson
   University of Louisville
   Louisville, Kentucky

6. Dr. James Gantt
   Murray State University
   Murray, Kentucky