NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CONCEPT OF OPERATIONS FOR CBRN WIRELESS SENSOR NETWORKS

by

Robert W. Nelson

March 2012

Thesis Advisor:	Richard Bergin
Second Reader:	Lauren Wollman

Approved for public release; distribution is unlimited

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 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Concept of Operations for CBRN Wireless Sensor Networks		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Robert Nelson			
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. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Wireless sensor detection is readily accessible, easily deployable, and usable technology that provides public-safety personnel with an early-warning and identification tool in the event of a Chemical Biological Radiological Nuclear (CBRN) incident. This is accomplished by incorporating wireless sensor detection capability into the Los Angeles Fire Department's (LAFD) hazardous-materials operations. Due to the relative ease of use and low cost of deployment, it makes sense that the LAFD employ wireless technology, capitalizing on the advantages.

The question regarding CBRN wireless sensor network capability is whether this technology is suitable, reliable, user friendly, and quickly deployable. Furthermore, will this technology provide critical early warning, detection, and subsequent notification in real time? The goal of this thesis is to determine CBRN wireless sensor detection capability in terms of reliability, deployment, early warning, and notification. The objective is to outline a concept of operations document providing the need structure for incorporating wireless sensor detection capability into public-safety operations.

Through field deployments and exercises using sensor detectors, standardized equipment, and software, the LAFD will have better access to early detection and notification of CBRN material releases. The end result means a more efficient, cost-effective tool that readily detects hazardous products, providing an early warning capability.

14. SUBJECT TERMS Wireless sensor networks, CBRN detection, concept of operations, hazardous materials, joint operations, emergency response, notifications, chemical warfare agents, toxic industrial chemicals, early warning			**15. NUMBER OF PAGES** 91
			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** UU

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CONCEPT OF OPERATIONS FOR CBRN WIRELESS SENSOR NETWORKS

Robert W. Nelson
Battalion Chief, Los Angeles Fire Department
B.S., California State University, Long Beach, 2007
M.S., California State University, Long Beach, 2010

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
March 2012**

Author: Robert W. Nelson

Approved by: Richard Bergin
Thesis Advisor

Lauren Wollman
Second Reader

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Wireless sensor detection is readily accessible, easily deployable, and usable technology that provides public-safety personnel with an early-warning and identification tool in the event of a Chemical Biological Radiological Nuclear (CBRN) incident. This is accomplished by incorporating wireless sensor detection capability into the Los Angeles Fire Department's (LAFD) hazardous-materials operations. Due to the relative ease of use and low cost of deployment, it makes sense that the LAFD employ wireless technology, capitalizing on the advantages.

The question regarding CBRN wireless sensor network capability is whether this technology is suitable, reliable, user friendly, and quickly deployable. Furthermore, will this technology provide critical early warning, detection, and subsequent notification in real time? The goal of this thesis is to determine CBRN wireless sensor detection capability in terms of reliability, deployment, early warning, and notification. The objective is to outline a concept of operations document providing the need structure for incorporating wireless sensor detection capability into public-safety operations.

Through field deployments and exercises using sensor detectors, standardized equipment, and software, the LAFD will have better access to early detection and notification of CBRN material releases. The end result means a more efficient, cost-effective tool that readily detects hazardous products, providing an early warning capability.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CAP	Common Alerting Protocol
CBRN	Chemical Biological Radiological Nuclear
CBRNE	Chemical Biological Radiological Nuclear Explosive
CFD	Chicago Fire Department
CFR	Code of Federal Regulation
ClCN	Cyanogen Chloride
ConOps	Concept of Operations
CWA	Chemical Warfare Agent
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
EDX	Electronic Data Exchange
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FIRE	Fire Information and Rescue Equipment
GAO	Government Accountability Office
GIS	Global Information System
GPS	Global Positioning System
HazMat	Hazardous Materials
HCN	Hydrogen Cyanide
HMOP	Hazardous Materials Operational Plan
ICD	Improvised Chemical Device
IDLH	Immediately Dangerous to Life or Health
IrDA	Infrared Data Association
IP	Internet Protocol
JHAT	Joint Hazard Assessment Team
LAFD	Los Angeles Fire Department
LC	Lethal Concentration
NIEM	National Information Exchange Model

NRC	Nuclear Regulatory Commission
OSHA	Occupational Safety and Health Administration
PPE	Personal Protective Equipment
PPM	Parts Per Million
RDD	Radiological Dispersal Device
SME	Subject Matter Expert
SMS	Short Message Service
SWAT	Special Weapons and Tactics
TCP	Transmission Control Protocol
TIC	Toxic Industrial Chemical
TIH	Toxic Inhalation Hazard
TIM	Toxic Industrial Material
TTL	Time-To-Live
USAF	United States Air Force
VX	Nerve Agent
WHO	World Health Organization
WMD	Weapons of Mass Destruction
WSN	Wireless Sensor Networks
WTC	World Trade Center
XML	Extensible Markup Language

ACKNOWLEDGMENTS

A number of individuals have been instrumental throughout my academic journey. First, I would like to express my gratitude to my family for their support and assistance. To my wife, Ann, who has provided encouragement through all my academic and professional pursuits while creating an environment that allowed me to concentrate on my studies. I also need to thank my two children, Colton and Caitlin, for accepting my inability to spend quality time with them on their projects and activities. This includes a heartfelt thanks to my mother and father-in-law who helped provide the key ingredients necessary in keeping the family grounded. This includes a special acknowledgement and thanks to Dan Napier, my friend, mentor, and surrogate father for his undying perspective, knowledge, and technical competence. Without their love, patience, encouragement, and support, none of my accomplishments would have been possible.

I would like to acknowledge and thank all the CHDS instructors, who helped guide my cohort through the past 18 months. The experience was outstanding, having a profound effect on my professional and personal life. This includes a sincere thank you to my thesis advisor, Richard Bergin, who spent a tremendous amount of time providing direction, guidance, and insight. In addition, the thanks extend to my second reader, Lauren Wollman for her support, responsiveness, meticulous nature, and academic advice throughout the entire process.

Finally, I would like to thank the Los Angeles Fire Department, especially Assistant Chief Mike Little, for opening up the many homeland security possibilities and opportunities. Without his guidance, knowledge, and faith, I would not have been exposed to the magnitude of challenges and prospects that have taken the LAFD to higher ground, making the department a true leader within the fire service and a pioneer in the homeland security field.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Wireless technology has changed the way we communicate, function, and conduct business. This capability is finding a way into public-safety applications. The technology expands accessibility and productivity, introducing new opportunities, complexity, and challenges and making wireless networked systems and devices capable of accessing a wide array of equipment, resources, and information. Wireless capability has become the "anywhere/anytime" technology that provides the framework for the future of public safety operations. Delivering services effectively and efficiently is expected from our public in this new society that demands immediate data delivery to our fingertips in any way and anywhere it is needed (Federal CIO Council, 2010, p.1). For the Los Angeles Fire Department (LAFD) to take advantage of this technology requires the development of a concept of operations for wireless sensor networks (WSNs), specifically within the hazardous-materials domain. The LAFD hazardous-materials mission must change, adapt, and improvise if the organization plans to advance its operation using wireless sensor detection technology.

There has been a great deal of research directed toward wireless sensor networks due to the rapidly growing nature of this field, its accessibility, and its interoperability aspects. The ability to adapt wireless sensor networks into an operational tool for public safety presents unique opportunities and challenges, especially when chemical, biological, radiological, and nuclear (CBRN) sensors are concerned. The ability to take advantage of this technology means the ability to support LAFD hazardous-material operations more efficiently and safely by incorporating wireless sensor capability into the deployment models. Areas of concern include interoperable wireless sensor networks, cost, power requirements, wireless platforms, and sensor reliability.

There have already been incidents in which wireless sensors have been deployed without a solid operational foundation, thus limiting their overall use and application. The LAFD cannot be complacent in this digital, fast-paced, increasingly wirelessly connected world. The world is changing, and the LAFD must adapt to these changes in the post-

9/11 era. We must understand the capabilities and take steps to properly incorporate CBRN wireless sensor technology into our operations.

This thesis is organized as follows: Chapter I introduces the need, research questions, possible solutions, and methodology used to define a concept of operations (ConOps) within the LAFD regarding CBRN wireless sensor detection. Chapter II presents the background of the various CBRN threats and hazards that guided the design and implementation of a possible wireless technology. This includes the background on LAFD hazardous-materials operations. Chapter III describes the literature and research documentation regarding wireless sensor networks, national strategies related to homeland security, and ConOps supporting real-time environmental monitoring. Chapter IV presents an analysis of wireless sensors networks, including the goals and objectives, constraints and tactics, policies and governance, and supporting organizations. The components, exercises, and case studies are discussed to provide deployment benefits and challenges. Chapter V provides the findings, which include a summary of impacts from an operational and organizational perspective. Chapter VI presents the recommendations, conclusions, and future work.

A. PROBLEM STATEMENT

Weapons of Mass Destruction (WMD),[1] including chemical, biological, radiological, and nuclear materials, pose a great threat to our homeland. The National Security Strategy issued in March 2006 notes that there are few threats greater than a terrorist attack with WMD (White House, 2006, p. 18). Evidence indicates that terrorist organizations aspire to obtain and use chemical, biological, radiological, and even nuclear weapons. Mass-gathering locations create an attractive target for terrorists, and a WMD

[1] In 1998, the GOA defined WMDs as any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release of toxic or poisonous chemicals or their precursors, a disease organism, or radiation or radioactivity. The definition varies depending on the agency.

attack on such a gathering could have a devastating effect that could overwhelm our emergency-response systems. Furthermore, WMD attacks in densely populated urban areas could be devastating and induce chaos.

The current LAFD model used for responding to CBRN threats incorporates a tremendous amount of personnel and equipment. These resource-intensive incidents are not efficient and result in redundant operations and an increase in response times. Furthermore, these types of emergencies are time consuming due to the potential hazards, location, set-up time, and equipment necessary to determine a safe environment. To further exacerbate the situation, a majority of the CBRN responses are deemed "false," with no immediate threat to the public. Early and accurate detection, characterization, and warning of a chemical or biological event are critical to an effective response by the emergency-response personnel (Barrett & Goure, 2008, p.1). In the monitoring of CBRN threats in urban areas and in mass-gatherings scenarios, an early-warning system can make the difference between life and death (Barrett & Goure, 2008, p.1). In an effort to address the CBRN threat, the LAFD has begun using wireless sensor technology to provide for early warning and detection.

The LAFD is in the initial stages of incorporating wireless sensor technology into its hazardous-materials procedures, but it lacks an operational doctrine to standardize the process. There is no architecture or overarching document that delineates wireless capability, the components required, or the supporting agencies necessary to meet mission objectives as they relate to CBRN detection. Despite using wireless sensor detection, the LAFD has not developed a "concept of operations" (ConOps) regarding their use. Without a proper ConOps, the ability to design, plan, develop, and integrate wireless sensor technology into the hazardous-materials operations is limited. The ConOps document is a prerequisite for determining the necessary goals, objectives, tactics, constraints, authority, components, application, and role of supporting agencies.

B. RESEARCH QUESTION

The fire service is faced with the realities of terrorism, as it pertains to CBRN threats and possible devices that could be deployed. This has influenced a change in the overall fire service mission. The LAFD has taken a proactive approach and is taking steps to advance its capability regarding wireless sensor technology in order to detect potential hazards and to alert authorities and the public accordingly. The LAFD is moving forward with a wireless sensor network and is looking to enhance existing CBRN detection capabilities. Along that continuum, the LAFD leadership has recognized the importance of promoting a functional and interoperable CBRN detection system.

In the process of assessing the LAFD hazardous-materials operations and its application of a CBRN detection system, it is important to understand how to develop a concept of operations that addresses WSNs for CBRN detection. This leads to the following research questions:

1. What concept of operations for CBRN wireless sensor networks will support the LAFD's hazardous materials operations?

2. What LAFD goals and objectives will enable a concept of operations for CBRN detection utilizing a wireless sensor network?

3. What are the constraints and tactics that are associated with LAFD's CBRN wireless sensor networks concept of operations?

4. What policies are needed to govern the application of a concept of operations for LAFD's CBRN wireless sensor networks?

5. What enabling infrastructure can support a concept of operations for the LAFD's Wireless Sensor Network CBRN detection plan?

C. TENTATIVE SOLUTIONS

The ability to rapidly detect and identify hazardous CBRN materials equates to faster response times, reduced exposure potential, and more efficient use of limited resources. This thesis advocates the use of wireless sensor networks to become more efficient and capable when monitoring for, or responding to, incidents that involve CBRN

materials. The traditional LAFD response models for CBRN events result in valuable time being used to verify the hazard and determine the nature and scope of the threat. The implementation of wireless detection sensors, networked together, can provide instant feedback on environmental conditions, prompting a more focused response and providing the ability to make use of specific equipment to isolate and mitigate the hazard.

Early and accurate detection of a CBRN event is critical to a safe, well-organized response. An effective CBRN detection program will ensure that hazardous materials are rapidly detected and identified and that critical locations, events, and incidents are safely managed. By their nature, CBRNE[2] materials differ in detection and characterization methodologies (United States Department of Homeland Security [USDHS], 2007). With this new emerging capability the need for training, policy, and standardization becomes a necessity. By incorporating CBRN wireless sensor technology into the LAFD HazMat operational environment, greater situational awareness and real-time environmental monitoring can be achieved.

Weapons of mass destruction pose a great threat to our communities and national security. As early as the 1990s, the U.S. government recognized WMD as a potential threat. A GAO report on combating terrorism stated that federal, state, and local officials generally agree that a WMD incident involving chemical agents would constitute a major HazMat emergency (United States Government Accountability Office [GAO], 1999, p.7). The report further indicated that local HazMat teams will be the first to reach the scene and begin actions to mitigate the hazards. Through the proper application and use of wireless sensors, strategically placed and remotely monitored, CBRN hazards can be detected and identified at levels where emergency response personnel have an advantage.

The LAFD is operating without a clear mission as it moves forward with wireless sensor technology that involves CBRN detection. There is a need to develop a “concept

[2] The Department of Defense (DoD) characterizes weapons of mass destruction in terms of chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) materials. Incidents involving CBRNE could range in magnitude from chemical spills that likely could be addressed by local responders to catastrophic incidents such as terrorist attacks involving nuclear material that could result in extraordinary levels of casualties and property damage.

of operations" that integrates CBRN wireless detection into the LAFD's protocols, strategic assessments, and response plans, especially for mass gathering and special high-profile events. By incorporating these factors into the operational structure, WSNs will propagate to other agencies and expand the awareness, capabilities, application, and understanding related to CBRN wireless sensor detection.

D. SIGNIFICANCE OF RESEARCH

This thesis will define the framework for developing a concept of operations to fill the gap in the literature that relates to the application of wireless sensor networks for CBRN detection within the public-safety sector. In addition, important aspects of early warning, detection, identification, and notification will be discussed. There is ample documentation supporting various WSNs and describing how this technology can be applied to a multitude of uses involving a great number of field applications. However, there does not appear to be a body of literature that addresses the use of wireless sensors for CBRN detection within the first-responder domain. Furthermore, there appears to be a limited body of literature that discusses the need for real-time environmental sensor detection and monitoring at mass-gathering locations and venues. This thesis will discuss the CBRN threat, possible WSN applications within the public-safety sector, current program development, and different bodies of literature covering wireless sensor capability within the homeland security architecture.

As the LAFD looks to the future of wireless technology, it becomes clear that the availability and diversification of this technology enhances the ability to respond more quickly, more effectively, and more safely. There is an ever-increasing need for ubiquitous wireless systems, which indicates the growing potential for public-safety agencies to seek out and evaluate new WSN applications and services. Public safety also needs the data capabilities and efficiencies that newer technologies can provide (House Homeland Security Subcommittee, 2010, p.1). Therefore, this thesis may be useful to other first-responding agencies that are exploring possible applications of WSN to detect CBRN hazards in order to improve readiness, increase response, and provide a tool for alerting allied and partner agencies when dealing with hazardous products.

E. METHODOLOGY

This thesis employed appreciative inquiry to better understand how current LAFD hazardous-materials plans and procedures and CBRNE-sensor network best practices can be used to build a framework for integrating wireless sensor capability into the LAFD hazardous-materials operational framework. This method was chosen because it focuses on discovering what has been done in the public-safety arena using CBRN wireless sensors, followed by what is working in other sectors.

The LAFD has a well-defined hazardous-materials operational plan and emergency operational plan. These documents provide the background for developing a concept of operations for CBRN wireless sensor detection for the LAFD's hazardous-materials program.

1. Sample

Academic publications on wireless sensor networks, government documents from the Department of Homeland Security, trade journals on emerging technology, and LAFD operational manuals were examined for wireless sensor network best practices to frame a concept of operations for CBRN wireless detection. For example, the LAFD hazardous-materials manual helps frame the goals and objectives for CBRN wireless detection. The text book *Wireless Sensor Networks, Technology, Protocols, and Application* provided information on the constraints and tactics associated with wireless sensor networks. The National Preparedness Guidelines help establish the policies and governance in the area of CBRN detection. Trade journals and white papers aided in defining necessary components, applications, interactions, and collaboration between participants and stakeholders.

Test bed information related to sensor capabilities, wireless connections, and notification methods was also explored, looking for trends and operational procedures used outside the public-safety sector that could be tailored to enhance operational efficiency within LAFD's hazardous-materials program. Actual deployments, case

studies, and exercises were used to better understand current applications for real-time hazard detection and examine how that knowledge can be applied to developing a concept of operations for the LAFD.

2. Data Analysis

The research questions helped provide the framework for analyzing the information available and contributed to establishing the criteria used in the data analysis. The objective was to analyze existing research, case studies, actual deployment information, and exercise evaluations to identify important elements, system requirements, best practices, and lessons learned necessary for developing a ConOps document for CBRN wireless sensor detection.

II. BACKGROUND

The U.S. population's vulnerability to a CBRN attack has been highlighted by past activities and communicated intentions from terrorist organizations involved in clandestine operations looking to attack America. It is not a secret that terrorist groups are lying in wait attempting to coordinate another attack on U.S. soil. Since the terrorist attacks of September 11, 2001, there is heightened concern that terrorists may attempt to smuggle nuclear materials or a nuclear weapon into the United States or may try to use chemical or biological agents to attack the homeland (GAO, 2010). Terrorist groups have demonstrated the ability to adapt and take advantage of techniques and methods to produce weapons using readily available products and commodities. The greatest threats are posed by the most effective and simple means of mass destruction, whether these means consist of nuclear, biological, or other forms of asymmetric weapons (Mowatt-Larssen, 2010, p. 7). There are numerous chemical agents that are relatively simple to synthesize or produce from easily obtained, over-the-counter products. These chemicals can be used either as dispersants, aerosolized weapons, or explosives. Preventing terrorists from synthesizing or obtaining small quantities of deadly chemicals or radiological material is a daunting task. Chemical or radiological agents in the hands of a terrorist could have enormous consequences in terms of casualties, fear, and economic loss.

One of the responsibilities of the federal government is to assess the relative risks associated with chemical, biological, radiological, and nuclear (CBRN) terrorism in the homeland. The Department of Homeland Security (DHS) is tasked with assessing the threat levels to determine which CBRN agents present the greatest risk to the U.S. population sufficient to affect national security. In the Los Angeles area targets such as public entertainment venues (Hollywood), transportation infrastructure (LAX), and critical supply chains (Los Angeles and Long Beach Harbor) are vulnerable to attack. It is vital to appropriately capture the CBRN terrorism landscape to help prioritize resources and identify areas that may need additional focus (Pillai, 2011).

A. CBRN THREAT PERSPECTIVE

In the early 1990s, DoD officials recognized that the proliferation of chemical, biological, and nuclear materials that could be used to develop WMD was a growing threat (GAO, 2004). This perspective was confirmed by the 1995 Aum Shinrikyo sarin attack in Tokyo's subway system. The event caught the attention of the U.S. government and first responders, increasing concerns about our vulnerability to a terrorist attack involving WMD.

> Incidents such as the Sarin attack on the Tokyo subway in 1995 and the Anthrax campaign in the US in 2001 show that CBRN terrorism poses a grave threat. According to the "Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence", which was released in February 2010, US intelligence agencies believe that if Al-Qaeda can develop CBRN capabilities it will use them to attack Western targets. (Bharat Book Bureau, 2010)

The 2001 attacks on the World Trade Center and the Pentagon highlighted the destructive potential of terrorists groups and their intentions to target the United States infrastructure, its economy, and its citizens. These events illustrate their intention, their capabilities, and their committed efforts toward disrupting the American economy. In 2006, the United States National Security Strategy stated, "There are few greater threats than a terrorist's attack with WMD." The 2007 *National Strategy for Homeland Security* highlighted the continuing threat posed to the United States by the potential use of weapons of mass destruction by terrorist organizations. To that end, CBRN issues present a challenge for homeland security professionals. For years, senior U.S. officials and government reports have expressed concern that if terrorist organizations acquired unconventional materials, they would not hesitate to use them against U.S. friends and allies. The United Nation, the United States, the European Union and the G-8 all agree that nuclear, biological, and chemical weapons of mass destruction represent one of the greatest threats to the security of all nations (Doane & DiRenzo, 2007). Since the terrorist attacks of September 11, 2001, there has been a proliferation of extremist groups whose

explicit intention is to engage in high-profile and sophisticated attacks targeting civilians that include the use of CBRN together with stolen or rudimentary weapons of mass destruction (Campbell, 2007, p. 25).

The Commission on the Prevention of WMD Proliferation and Terrorism completed a report entitled "World at Risk" in 2008. That report stated, "The Commission believes that unless the world community acts decisively and with great urgency, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013." It further pointed out that "terrorists are more likely to be able to obtain biological weapons than a nuclear weapon." The attacks in the United States and the threat potential since 9/11, including the anthrax events of 2001, indicate that the threat is real.

> On October 12, a case of cutaneous anthrax was reported in New York City. At NBC News, a person was exposed to a letter containing a suspicious powder. The Federal Bureau of Investigation (FBI) reported that four recovered envelopes containing Bacillus anthracis spores were postmarked at the U.S. Postal Service Trenton Processing and Distribution Center in Hamilton Township, New Jersey. A total of 22 confirmed or suspect cases of anthrax infection occurred; 11 were inhalation cases, and 11 were cutaneous cases. Five persons died. (Allegra et al., 2005)

These types of terrible events have motivated many countries to focus their defense and security-related research toward the detection of explosives, hazardous liquids, and chemical agents that can be used by terrorist organizations as WMD threats against troops or civilians (Ortiz-Rivera, Pacheco-Londoño, & Hernández-Rivera, 2010). In an effort to provide adequate protection measures, public safety organizations in conjunction with federal and state agencies must develop new and innovative ways to address this threat.

Unconventional weapons, including those commonly referred to as weapons of mass destruction, which may involve chemical, biological, radiological, and nuclear agents, add a degree of complexity to defense measures. Homeland Security Presidential Directive 18: "Countermeasures against Weapons of Mass Destruction" states that, "Weapons of Mass Destruction (WMD)—chemical, biological, radiological, and nuclear

agents (CBRN)—in the possession of hostile states or terrorists represent one of the greatest security challenges facing the United States." The report further highlights the fact that "an attack utilizing WMD potentially could cause mass casualties, compromise critical infrastructure, adversely affect our economy, and inflict social and psychological damage that could negatively affect the American way of life." (White House, 2007)

1. Chemical Warfare Agents

Chemical warfare agents (CWAs) are chemicals manufactured to incapacitate, harm, or kill. Chemical warfare agents include gases, liquids, or solids that can poison people, animals, and plants. The severity of the resulting injuries depends on the type of chemical, the amount, and the length of exposure. The principal chemical warfare agents are sulfur mustard (mustard gas) and nerve agents such as sarin and VX. These agents are typically released as a vapor or liquid. During a chemical attack, the greatest danger arises from breathing the vapors. If a large amount of chemical is released as an aerosol, the skin of humans could be exposed to the chemical agent as droplets. In addition to producing potentially horrific effects, chemical weapons are of great concern because they are cheaper and easier to manufacture than nuclear or biological weapons.

The level of threat from terrorist attacks using CBRN varies depending on the chosen agent, the technical expertise of the user, and the means of delivery available to terrorist groups. Toxic and cyanide compounds, including hydrogen cyanide (HCN), cyanogen chloride (ClCN), mustard agents, nerve agents (VX), and toxic industrial chemicals, are considered to be the most likely choice of chemical that terrorists might seek to acquire .

2. Toxic Industrial Chemicals

Toxic industrial chemicals (TICs) include chemicals manufactured for use in industrial, commercial, or medical processes. TICs can be in gas, liquid, or solid form (including particles), but those of particular concern tend to be gases because gas spreads easily. TICs are manufactured, stored, transported, and used throughout the world. They

include chemical hazards such as carcinogens, reproductive hazards, and corrosives. They also present a physical hazard because they can be flammable, combustible, explosive, or reactive.

The type of product or agent used by a terrorist can include any product that is capable of irritating, incapacitating, or producing lethal consequences. Common industrial chemicals and products, or combinations of various products, may be used, including chemical, biological, radiological, or nuclear materials. In a world of asymmetric threats, toxic industrial chemicals fit well into a terrorist's method of attack: they are easily accessible, readily available, and relatively easy to convert into a weapon (Jakucs, 2003).

> While the most frequently used chemical warfare agents number about 70, approximately 70,000 TICs are produced, used and stored in large amounts and circulated around us by hundreds of thousands of vehicles, and/or they enter our environment as toxic wastes (6). Therefore, the likelihood of exposure to them in large amounts is relatively high. (World Health Organization [WHO], 1999)

All these products present unique hazards for first responders. The ability to recognize them early helps to reduce casualties.

Anhydrous ammonia and chlorine have been a concern for homeland security because of their unique characteristics, their ability to produce large, toxic vapor clouds, and their common use and availability. These products are considered toxic inhalation hazards, (TIH)[3] and they can rapidly cover a large area at toxic concentrations. A TIH is a gas or volatile liquid that is known to be so toxic to humans as to pose a hazard to health during transportation or, in the absence of adequate data on human toxicity, is presumed to be toxic to humans because when tested on laboratory animals it has a Lethal Concentration 50 (LC50) value of not more than 5000 ppm (United States Department of Transportation, 2008).

[3] Under the Hazardous Materials Regulations (49 CFR 171–180), TIH materials are gases or liquids that are known or presumed on the basis of tests to be so toxic to humans as to pose a hazard to health in the event of a release during transportation. See 49 CFR 171.8, 173.115, and 173.132.

> In March 2004 a plot involving Osmium Tetroxide was discovered in Britain. Counter-terrorism police had foiled a plot in the UK to lace a conventional bomb with osmium tetroxide. The chemical can damage the eyes, cause skin rashes, and burn the throat and lungs (2004, New Scientist). Osmium Tetroxide (OsO 4) serves legitimate functions in biological research and in specialized chemical industry, but its suitability as a terrorist agent—a dual-use compound—is limited, despite the characterizations of it generating "chemical fallout." (Taylor & Wright, 2004)

The reason that TICs present a high risk is because they are readily available in large quantities in business, commercial, retail, and private settings. Industrial chemicals have become an integral part of daily life in modern societies following the industrial revolution that started after World War II (Hincal & Erkekoglu, 2006, p. 221). TICs can be used as improvised chemical weapons when combined to form other toxic chemicals. Chemical terrorism is typically described as a "high probability" event, and the threat potential of TICs cannot be underestimated (Hincal & Erkekoglu, 2006, p. 227).

3. Improvised Chemical Devices

An improvised chemical device (ICD) is a method that brings together the toxic properties of a chemical designed to release lethal toxic products in enclosed spaces, such as restaurants, theaters, or public transportation to induce fear or behavior modification. These devices have been labeled "mubtakkar,"[4] a device that can deliver lethal gases. Such devices may be fabricated in a completely improvised manner or may be an improvised modification to a U.S. or foreign weapon (Finegan, 2008).

Hydrogen cyanide, chlorine, and other TIHs are dangerous without any special modifications and are considered ready-made chemical agents. Although the focus has been on chlorine, other toxic gases and liquids have lethal chemical properties that make them viable agents for use in a terrorist attack.

> The men were arrested in August 2006 after officials uncovered the plot targeting jets departing London's Heathrow Airport and destined for cities

[4] This device is designed to release lethal quantities of hydrogen, cyanide, cyanogen chloride, and chlorine gases (Sullivan, 2006).

> in the United States and Canada. The failed plan involved bringing on board homemade bombs filled with hydrogen peroxide and disguised in soft drink bottles, and using parts of light bulbs and chemicals hidden in batteries to detonate them almost simultaneously. (Faiola & Karla, 2009)

When considering plans to deal with CBRN devices and emerging threats, responders need to be prepared to deal with the aftermath of such an event. This requires embracing technologies that can rapidly detect, recognize, and subsequently integrate response capabilities from multiple local, regional, state, and federal organizations and disciplines.

4. Biological Threat/Hazard

Biological agents are dispersed or employed as pathogens or toxins that cause disease in humans, animals, and plants. Pathogens require an incubation period to establish themselves in the body of the host and produce disease symptoms. The onset of visible symptoms may occur days or weeks after exposure. Some toxins can remain active for extended periods in the natural environment. This stability creates a persistent transfer hazard. Unlike chemical, radiological, and nuclear hazards, biological hazards are unpredictable, and it is difficult to classify the extent of the hazard.

The operational considerations for biological agents include the various dissemination methods, such as dispersal or deposit of an aerosol, liquid droplets, or dry powders. Live microorganisms usually grow in a moist environment; therefore, these agents may be disseminated in a liquid medium as wet aerosols. However, microbiological materials may also be stored and released in more stable powder media. In general, agents dispersed as dry powder will survive longer than those dispersed as wet aerosols.

Biological agents are unlike chemical and radiological agents due to the slower reaction time. Biological agents are not as quickly recognized and consequently management can be delayed because people do not become sick immediately. Most biological agents have an incubation period, which means that the signs and symptoms are usually not apparent for several days. **5. Radiological Threat/Hazard**

Radiological events, including incidents of terrorism, continue to be a real threat to the public and to emergency personnel. Radiation can only be detected by radiological detectors. Other problems associated with a radiological release include, but are not limited to, terrorist attack, system failure, fire, and transportation accidents.

A radiological dispersal device (RDD) or dirty bomb is a mix of explosives, such as dynamite, with radioactive source material, such as a powder or pellets. The explosive is used to blast or spread the radioactive material into the surrounding area. If an explosive device is used, the majority of radiological material or dust will settle within a relatively short time frame, leaving a larger area contaminated. Our ability to detect the radiation hazard requires the use of radiological detection equipment.

6. Nuclear Threat/Hazard

The nuclear threat is not very likely to occur; however, the severity of a nuclear incident depends on many factors that include weapon yield, emission spectrum, and distance from the initial blast. Residual radiation effects are based on the emissions from particles that may include alphas, beta, and low-energy gamma radiation. These sources are called fallout.

B. LAFD HAZARDOUS MATERIALS OPERATIONS

The responsibilities of the Los Angeles Fire Department for hazardous materials are managed and governed by regulations at the federal, state, and local levels. These include establishing the necessary requirements for emergency response plans, hazardous operations, certifications, training, and tactical configurations. The City of Los Angeles's primary emergency response plan is the City of Los Angeles Emergency Operations Master Plan and Procedures. This document is augmented by the City's Hazardous Materials Annex and the fire department's Hazardous Materials Operational Plan. The documents provide the foundations for HazMat operations within the city. The fire department's primary guidance regarding hazardous materials incident response and

planning is found in the Hazardous Materials Operational Plan. These plans are designed to coordinate the overall response capability of the city's departments.

The fire department's Hazardous Materials Operational Plan establishes the foundation for standard operating guidelines outlining the responsibilities of LAFD members tasked with the prevention, preplanning, and response to hazardous materials incidents. The Hazardous Materials Annex assigns responsibility for emergency response and coordination for dynamic hazardous materials incidents to the LAFD. The Los Angeles Police Department supports HazMat operations by providing force protection, technical expertise, and perimeter control. If there is a nexus to terrorism or criminal activity, the LAFD will establish a unified command with the LAPD to facilitate the criminal investigation. The Hazardous Materials Annex of the Emergency Operations Master Plan is activated when an incident grows in scope to the point where activation of the Emergency Operations Center (EOC) is warranted.

> Emergency response or responding to emergencies means a response effort by employees from outside the immediate release area or by other designated responders (i.e., mutual aid groups, local fire departments, etc.) to an occurrence which results, or is likely to result, in an uncontrolled release of a hazardous substance. Responses to incidental releases of hazardous substances where the substance can be absorbed, neutralized, or otherwise controlled at the time of release by employees in the immediate release area, or by maintenance personnel are not considered to be emergency responses within the scope of this standard. Responses to releases of hazardous substances where there is no potential safety or health hazard (i.e., fire, explosion, or chemical exposure) are not considered to be emergency responses. (OSHA, 29 CFR 1910.120(q)(3))

The purpose of the Hazardous Materials Annex is to provide direction and guidance when city resources are tasked with responding to incidents involving hazardous materials releases and the incident has exceeded the capabilities normally managed at the field level. This annex includes the concept of operations for a hazardous material incident that may include an accidental release, an intentional release, or use of a chemical, biological, radiological, nuclear, or explosive (CBRNE) agent, or result in a secondary incident to another natural or manmade incident (City of Los Angeles, 2010a).

The Hazardous Materials Operational Plan and Hazardous Materials Annex contain procedures and protocols to be used as guidelines for approach, recognition, containment, hazard assessment, and mitigation by city resources. These documents provide additional guidelines on monitoring and decontamination procedures for exposed personnel. However, with new technology being introduced into the public-safety sector, there are no policies or procedures that discuss wireless sensor detection.

It is not possible to address all the hazards associated with each CBRN product that may be encountered by firefighters. A great deal of information relevant to hazardous and toxic substances in the workplace often depends on the classification of the agent and agency terminology. Hazardous materials, hazardous substances, and hazardous waste are defined and regulated in the United States through various governmental organizations using statutes, rules, laws, and regulations. These guidelines are administered by the following agencies:

- U.S. Environmental Protection Agency (EPA);
- U.S. Occupational Safety and Health Administration (OSHA);
- U.S. Department of Transportation (DOT); and
- U.S. Nuclear Regulatory Commission (NRC).

Each agency has its own definition of what constitutes a "hazardous material," based on the agency's regulatory issues and Congressional mandates regarding their specific function. These terms are usually not interchangeable and often are used in the context of the specific agency having authority or jurisdiction.

> The Los Angeles Fire Department defines a hazardous material as "any chemical, chemical mixture, or contaminant which is toxic, corrosive, volatile, reactive, explosive, or flammable that has the capacity of inducing great bodily injury or illness or which has been determined to be capable of posing an unreasonable risk to health, safety, or property. Hazardous materials include all chemical, biological, and radiological substances, including those also referred to as Weapons of Mass Destruction (WMD), whether accidentally or intentionally released." (Los Angeles Fire Department Hazardous Materials Operational Plan [LAFD-HMOP], 2003)

C. LAFD HAZARDOUS MATERIALS TASK FORCE

The LAFD has specially trained firefighters that are assigned to one of four hazardous materials task forces. These task forces are responsible for performing the tactical operations at hazardous materials incidents. Their primary functions include but are not limited to:

- Safety for responders and public;
- Hazard identification;
- Hazard assessment;
- Establishing control zones;
- Control of the hazard;
- Decontamination procedures;
- Notifications to key agencies;
- Technical reference;
- Hazard mitigation; and
- Environmental cleanup.

In the event of a release of a CBRN material, the operational objectives of the Los Angeles Fire Department's hazardous material response team are to have technically trained and experienced personnel working in concert with allied agencies to stabilize and mitigate the release. The LAFD's hazardous materials task forces provide technical assistance, specialized equipment, and detection and identification tools that help mitigate the incident.

At the operational level, all firefighters have basic hazardous materials awareness training, and they act in a defensive fashion with readily available equipment and resources. They are tasked with the initial evacuation and isolation of the incident, containment of the release from a safe distance, limiting the spread, and preventing exposure to people, property, and the environment. The Los Angeles Fire Department's first-responder operational objectives for a hazardous materials incident are categorized as follows:

- Safety of first responders;
- Evacuation;
- Isolation;
- Denial of entry;
- Rapid extraction of victims;
- Victim decontamination;
- Medical evaluation and treatment (triage);
- Medical transportation; and
- Safe refuge (release and reunite).

These activities are often performed in conjunction with other agencies, including the Los Angeles Police Department. The Los Angeles Police Department's operational objectives for hazardous materials incident are categorized as follows:

- Life safety;
- Crime scene investigation;
- Force protection;
- Technical reference;
- Hazardous material mitigation; and
- Site security.

The purpose of the LAFD notification policy is to promote prompt and accurate reporting to all the stakeholders, key officials, allied agencies, and response teams of a release or threatened release of hazardous materials that may result in injury or damage to the community and/or the environment. The primary reason for prompt and accurate notification is to enable response and authoritative agencies to take measures to mitigate the impacts of a hazardous materials release. This will enable the appropriate dispatching of emergency response teams with the appropriate equipment and personnel. It is imperative that all agencies that may have responsibility in handling the incident be

contacted and that an agency representative be requested to the scene. The incident commander is responsible for assuring that the appropriate agencies are contacted. This could include any of the following agencies:

- Fire Department
- Police Department
- California Highway Patrol
- Federal Bureau of Investigations
- Cal Trans
- City Public Works Department
- Department of Environmental Health
- Department of Fish and Game
- Department of Health Services
- Hazardous Materials Response Team
- Civil Support Teams

THIS PAGE INTENTIONALLY LEFT BLANK

III. LITERATURE REVIEW

The review of the literature focuses on understanding what has been done in terms of developing a concept of operations for the integration of CBRN wireless sensor networks into LAFD hazardous materials (HazMat) operations. The literature examined helped to determine the necessary goals and objectives that would enable a concept of operations for CBRN detection utilizing a wireless sensor network within the LAFD. This included viewing the documentation to assess the constraints and tactics associated with CBRN wireless sensor networks. The literature was also explored to ascertain those policies and procedures that may be needed to govern CBRN wireless detection applications. Due to the variety of applications, it became necessary to look at the literature so as to determine the value of supporting organizations and the interactions among participants and stakeholders. The objective is to improve the concept of operations for the LAFD's CBRN detection program by taking a multidisciplinary approach to wireless sensor networks.

The literature on WSNs in support of a concept of operations for the LAFD's hazardous materials program is segregated into the following categories:

1) Documents written and established by the Los Angeles Fire Department provide the framework for establishing the goals and objectives to enable the development of a concept of operations for CBRN wireless sensor networks within the fire service. The source documents are the Los Angeles Fire Department Hazardous Materials Operational Plan and the Emergency Operational Plan. These documents provide the foundation for incident action plans, planned response, emergency procedures, communications, and specific competencies.

2) Documents written by academic institutions or designed as an educational resource help identify the constraints and tactics associated with wireless sensor networks. A good source document is *Wireless Sensor Networks, Technology, Protocols, and Applications* (Sohraby, Minoli, & Znati, 2007). This resource covers a wide range of design features and discusses challenges and considerations when deploying a WSN. Another resource is the *Joint Forces Quarterly*, produced by the National Defense University. This source is meant to inform and educate national security professionals on joint and integrated operations, security policy, strategy, guidance, and training to meet tomorrow's challenges.

3) Research material by government agencies such as the Department of Homeland Security's National Preparedness Guidelines. This document provides some guidelines regarding detection, response, and decontamination for CBRN incidents. Another example is material produced by the Domestic Nuclear Detection Office, which discusses the importance of sharing information regarding sensor detection. The literature provides a foundation for policy and governance as it relates to strengthening detection capabilities for CBRN-related events.

4) Literature from trade and professional journals provides information on the importance of interagency collaboration, supporting roles, and joint operations. For example, an article in *Homeland Security Affairs* titled, "Firefighters and Information Sharing: Smart Practice or Bad Idea?" focuses on the National Strategy for Homeland Security and stresses the importance of a formalized collaboration within the homeland security community. This is further emphasized in an article titled "Coordinating Expertise Among Emergent Groups Responding to Disasters," where interactions between organizations are discussed as being essential to efficient coordination during emergencies (Majchrzak, Jarvenpaa, & Hollingshead, 2007).

A. LAFD OPERATIONAL MANUALS

The LAFD's written documentation for HazMat operations provides the necessary framework for ensuring a safe and efficient operation for firefighters during emergency incidents. These documents help define the goals and objectives that will enable the development of a ConOps for CBRN detection. This forms the basis for safe performance through proper use of equipment, apparatus, and proven practices by technically trained personnel working in concert with supporting agencies.

The documentation that supports operations in a hazardous environment includes the Los Angeles Fire Department Hazardous Materials Operational Plan and Emergency Operations Master Plan and Procedures. Together, both of these documents outline and define the tactics and strategy needed when dealing with CBRN incidents within the city of Los Angeles. While these plans coordinate the overall response capability of the city's departments, each department maintains its own detailed procedures (LAFD-HMOP, 2003, p.10). A review of these documents revealed a lack of any information related to wireless sensor networks, their capability, application, or procedure. Between these two

documents, the Hazardous Materials Operational Manual provides a more thorough assessment of the CBRN threat, terrorism warning signs, detailed operations, and required action. The Emergency Operations Master Plan outlines a strategy and provides guidance for the fire department when dealing with significant incidents involving hazardous materials. Strategic planning, continuous training by a properly equipped workforce, and the routine exercise of response plans are all key components in assuring the Los Angeles Fire Department's ultimate success in the management and control of emergency events (City of Los Angeles, 2010b, p. 2). Together, these documents include terrorism indicators, risk assessments, and control measures important for emergency responders when dealing with CBRN events.

B. WIRELESS TECHNOLOGY

Wireless technology has been around for many years and has increased in popularity, versatility, and capability. The available literature focuses on private industry and business applications that enable organizations to deliver services more efficiently, enhance performance, augment security, or monitor conditions. This type of information provides the basic understanding of wireless capability that is crucial in developing a concept of operations for WSNs; it was reviewed to determine the constraints and tactics associated with CBRN detection. Current research in the area of WSNs is found in *Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions* (Ananda, Chan, & Ooi, 2006). This book is an excellent resource that represents the most thoughtful solutions to the challenges in wireless networks, including architecture, protocols, modeling, and analysis. The book highlights some key aspects central to wireless detection, such as trends and cutting-edge applications that help to define possible tactical elements when deploying this equipment. In the years ahead, wireless sensors will be employed by businesses, military, and public-service agencies to provide a wide array of services. This will include numerous applications that have yet to be implemented. The material provides a background and understanding of the practical approach to the many applicable possibilities establishing a foundation for developing a concept of operation around CBRN wireless sensor networks. Furthermore, the combined

literature helps to bridge the gap in understanding between the different uses of wireless sensor networks, taking their limitations and tactical applications into account and thereby establishing a solid foundation for developing a ConOps around this technology that is suitable for the LAFD's HazMat program.

Wireless technology has developed rapidly in the past decade, and new mobile applications are continually being proposed (Shim et al., 2007, p. 450). Within the last 10 years, WSNs have increased their application, diversity, and value, leading to featured articles in trade magazines and journals that highlight this emerging technology. In 2009, the trade journal *Sensors* discussed the evolution of WSNs, pointing out that the information on WSNs is relatively new (Buratti et al., 2009). Although technically orientated, the article covered applications for environmental monitoring and discussed design strategies important for CBRN detection scenarios. An important element for WSNs is power management, which has also undergone an evolution. Power consumption remains one of the limitations, especially for long-term deployment. Academic articles discuss the most relevant issues of WSNs, from application and deployment to custom design possibilities. The recent advances of wireless sensor networks create new opportunities for innovative applications, but new technical challenges for constructing such applications remain (Cheour, Lahma, & Abid, 2011).

As the field of WSNs continues to evolve, the challenge is to keep pace with the rapid changes, advances, and technology that continue to make sensor components more compact, robust, and energy efficient. Ubiquitous and embedded, often invisible and silent, sensing technologies will be one of the hallmarks of this century (Nagel, n.d.). Network designers and planners from emerging telecommunication networks face specific challenges in finding the best way to integrate new networks with existing network systems.

> Engineers are adding a new dimension to the wirelessly connected world. They are extending networks connecting people anywhere at any time to also connect anything. In other words, people are being connected to things, and things themselves are being interconnected. (Shim et al., 2007, p. 448)

The field of WSNs is growing rapidly. This poses additional challenges to adapt and produce wireless devices that are smaller, more compact, efficient, and robust. The literature that addresses some of those challenges is discussed in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems* (Ilyas & Mahgoub, 2004), a book that captures the current WSN climate and deals with the particular technical challenges associated with this technology, including elements such as software protocols, data processing, security, and limited power sources, which are important factors when configuring a wireless sensor network.

There is not much literature that focuses on WSNs and public safety, especially in the area of CBRN detection. One reason for this stems from the traditional uses of WSNs, such as military, environmental, home, health, and commercial applications. Another reason centers on the unique requirements of first-responder agencies. Fire rescue is a special application that is different from the previous WSN-supported applications, such as environmental or habitat monitoring, or object tracking. Thus, there are some specific requirements for the design of a WSN system (Sha, Shi, & Watkins, 2006). Fire and law enforcement are both changing from response services to services capable of response. This means having the ability to anticipate problems and forecast possible solutions from a strategic vantage point. Fire and police agencies can improve their effectiveness by forecasting the operational environment, anticipating problems, identifying vulnerabilities, and developing plans to address those issues. Wireless technology is the vehicle to reaching those goals and objectives. To further illustrate this point, the mechanical engineering department at UC Berkeley worked on a WSN project for incident command interface for urban and industrial firefighting. The intent of the FIRE project[5] is to create hardware and software tools to improve firefighting safety, efficiency, and effectiveness (Wilson et al., 2007).

This stance is continuing to gain prominence within the public-safety arena; focusing on technology demonstrates those attributes. The necessity to enhance

[5] Fire Information and Rescue Equipment (FIRE) is a project with the Chicago Fire Department (CFD) at UC Berkeley's mechanical engineering department. The project addresses challenges by applying and designing new technologies such as wireless sensor networks (WSNs).

operational efficiency and reduce costs means taking advantage of wireless technology to become more capable, efficient, and cost effective.

> The majority of the research effort into wireless sensor networks have been on the hardware and software configurations and the modeling of the network performance, there has not been a great deal of work into the application of these sensor networks, especially when chemical sensing is concerned. At present, research into chemical sensors and wireless sensor networks are still essentially discrete fields despite the requirement in merging these two disciplines for applications such as environmental monitoring. (Hayes et al., 2008)

The military is in the forefront regarding CBRN detection capabilities and innovation. Effective, timely, and accurate CBRN reconnaissance is essential to protect the public and the first responder. In an article on innovation technology, CBRN detection is gaining momentum, with the military leading the way for rapid technological advancements that provide near-real-time environmental monitoring. As operational realities shift, the development and demonstration of new defensive capabilities in the CBRN arena become even more urgent to ensure that the military can fight and win in any condition and properly prepare for the threats of tomorrow (Galarraga et al., 2009, p. 16). This is not surprising since our military faces the CBRN threat every day. The existing literature on CBRN detection concerns itself with efficient and practical applications in hazard environments, with an emphasis on recognizing limitations, portability, enhanced threat detection, and urbanized terrain. The issue can be framed by simply trying to transition from military applications to civilian operations.

The need for WSN in public safety has emerged as a potential tool for providing early detection and recognition of CBRN materials. Now sensor, environmental, and incident data is available to meet emergency response objectives and provide incident commanders and subject matter experts with the real-time data necessary for decision making. Wireless sensor capability is the next step toward becoming more efficient and providing first responders and command elements with a tool that can monitor and detect CBRN hazards in real-time.

C. DEPARTMENT HOMELAND SECURITY AND TECHNOLOGY

An important aspect in developing a concept of operations for CBRN wireless detection involves the Department of Homeland Security (DHS). In 2007, DHS published a report on the National Preparedness Guidelines. One of the guidelines discussed centers on the ability to strengthen detection, response, and decontamination capabilities to a chemical, biological, radiological, nuclear, or explosive incident (USDHS, 2007a, p. 18). Due to the threat of such an incident, DHS has been working to deploy a nationwide sensor network to provide a real-time early-warning system for a plethora of chemical, biological, and nuclear threats across the United States (Sohraby, Minoli, & Znati, 2007, p. 88). These efforts underscore the need for an effective, real-time wireless sensor detection program to increase the probability that CBRN materials are rapidly detected, identified, and safely managed at critical locations and events.

The terrorist threat has remained high and requires innovative ways to meet and address the challenge it presents. Overall, experts agree that in the twenty-first century CBRN materials may be utilized and deployed as weapons in novel ways, both in the military and civil domains (Frinking et al., 2009). It is the technology applied by the terrorist—the explosive device that destroys a target, the automatic weapon that intimidates, and potentially the chemical or biological weapon that inflicts mass casualties—that makes today's "high impact" terrorist strikes possible and makes the threat of future violence credible to a mass audience (Jackson, 2001, p. 3).

A government report, *National Technology Plan for Emergency Response to Catastrophic Terrorism,* provides a technology roadmap for federal planners to fill gaps in emergency responder capability against CBRN terrorism. This document lays out a strategy that uses technology to improve responders' capabilities to deal with all types of catastrophes, whether man-made, natural, or accidental. The document's main mission to develop a national technology plan, which has culminated in this report. While the report covers a wide range of technological issues related to terrorism prevention, chapter three is dedicated to detection, identification, and assessment of potential and ongoing terrorist attacks. This document provides a "technological roadmap" of new initiatives in an effort

to close the gaps in responder capabilities. However, each community relies on its own expertise and technical capability, which various from region to region. Thus, there has been little motivation or funding available to pursue integrated devices (Garwin, Pollard, & Tuohy, 2004). Nonetheless, the report recommends technology programs for the federal government with an all-hazards viewpoint.

With the threat of a CBRN incident, there are a variety of ways that wireless technology can contribute to improve the detection, identification, and monitoring of CBRN materials. The goal is to incorporate "best practices" and to develop a methodology to create a universal framework with specific measures to evaluate, test, and monitor CBRN detection capabilities. This will help to improve the strategies for prevention, preparedness, and response to CBRN incidents.

> A dispassionate analysis of the still growing number of terrorist attacks that have occurred and are continuing to occur around the world should demonstrate that the United States is still not immune from many of the major CBRN threats now facing the nation—and may never be. For that reason alone, there must be not merely continued, but increased, concern over chemical, biological, radiological, and nuclear (CBRN) terrorism. (Rudner, 2010, p. 6)

The use of WSNs is a viable resource for CBRN detection and provides public-safety agencies with the capacity to protect and warn the public against the release of hazardous materials. The possible applications are discussed in many articles in the context of homeland security—often on the heels of an innovative technologic idea. For example, in 2006, a consortium of WSN experts authored a document titled, *Scenario Definition and Initial Threat Analysis*. A section of this report focused on the promising applications within the homeland security environment, including using wireless sensor networks for early CBRN detection and identification. In various scenarios, WSNs can be easily deployed permanently (e.g., in public places) or on demand (e.g., high-risk events) in a very short time, at low cost, with little or no supporting communications infrastructure (Casaca & Westhoff, 2006, p. 29). In these scenarios, the purpose of WSNs is early detection, and this can be factored into prevention and preplanning activities. Once those aspects are addressed, there are three operational phases: detection before,

during, and after a CBRN event. Before the event, CBRN detectors allow continuous monitoring either to prevent an incident or to facilitate early warning. During the event, detectors help first responders identify and isolate the precise nature and extent of the release. After the event, WSNs are essential in order to confirm the results of early identification, evidence collection, and monitoring of decontamination efforts. Timely detection, locating, and tracking of CBRN devices in public places are key issues in homeland security and require robust sensor networking (Grilo, Casaca, & Nunes, 2009, p. 391).

The Science and Technology Division of DHS has identified the need to factor CBRN sensor capability into risk assessment and response. The literature from DHS outlines the need to improve and integrate technologies that will enhance our ability to deter, protect against, detect, mitigate, and recover from biological and chemical attacks. One of the stated objectives is to integrate CBRN sensor reporting capability—in particular, the integration of sensors into a common operating picture for easy integration of future detection systems (USDHS, 2009, p. 15). Wireless technology has evolved to a point where the LAFD can now use this know-how to establish a functional concept of operations for CBRN wireless sensor networks. The report identifies the need to focus on public-safety agencies and to take advantage of the benefits that innovative technology can bring. For example, the Chemical/Biological Division seeks out the science needed to reduce the CBRN probability and potential consequences. The division develops and implements early detection and warning systems for attack characterization (USDHS, 2009, p. 4).

Recent work on CBRN sensors addresses wireless capabilities and demonstrates operational effectiveness for hazard detection. Supplemental literature from DHS involves interoperability and communication challenges involving WSNs. For instance, a 2008 FEMA article, *NIMS Standards Case Study: Los Angeles Regional Interoperability*, states that agencies and jurisdictions rely on disparate equipment and communications platforms, resulting in responders having difficulty integrating the various public-safety

agencies into a combined response (USDHS, 2008). This highlights the need for interagency cooperation as it relates to CBRN detection capabilities and the associated network that brings public safety together.

Interoperability is a factor that is addressed at all levels of government. In order to support the evolution of a fully integrated, modernized CBRN detection system, interoperability means working together, uniting resources, and exchanging data and information in a standardized fashion. A DHS report from 2007, titled *Tactical Interoperability Communications Scorecards, Summary Report and Findings*, indicates that barriers to interoperable communications are both technical and operational. Furthermore, the literature suggests that, in addition to addressing technology and disparate communications systems, achieving interoperability requires that agencies examine governance, procedures, training, exercises, and usage (USDHS, 2007b, p. 5). This reinforces the need to coordinate activities in a collaborative manner with industry experts and other public-safety stakeholders to ensure the viability of a CBRN wireless detection system.

The literature extensively covers technological advancements with very little documentation on activity specific to the public-safety and response fields. Therefore, we must keep in mind that policies are associated with governance and tend to lag behind operational objectives. This is emphasized in the document *Tactical Interoperability Communications Scorecards, Summary Report and Findings* (USDHS, 2007b). The report addresses interoperability issues and the importance of collaboration on policies and strategic planning. This is further emphasized in a report published by the Joint Program Executive Office for Chemical and Biological Defense on the readiness of the CBRN network sensor:

> Currently, there are no standards for how Chemical, Biological, Radiological, or Nuclear (CBRN) sensors communicate in terms of protocol or in what they communicate in terms of status (alert, alarm, faults, built in-test, etc.) or commands (mode, state, configuration, etc.). Furthermore, many of the sensors require additional intermediate hardware devices to “network enable” them directly as an Internet

> Protocol (IP) addressable entity or to allow them to be plugged directly into a host platform via modern physical interfaces such as standard USB connections. (Godso et al., 2006, p. 25)

Nearly all of the research on wireless sensor networks and detection deals with military, industrial, commercial, and environmental applications. When addressing emergency-response applications, the literature falls short, even though these systems can easily be adapted to assist the emergency-response community when facing a CBRN threat. Improvements in chemical detection and identification could assist the responders in knowing whether they are experiencing a chemical attack and what chemicals they are encountering (Houghton, 2004, p. 173). Such improvements would include adapting applications that will monitor the environment and provide an early warning when hazardous products are introduced.

D. CONCEPT OF OPERATIONS

The "Concept of Operations" is a functional document that describes the goals, objectives, tactics, strategy, policy, procedures, and governance that is prepared in conjunction with the various stakeholders focusing on wireless CBRN detection and response. The goals and objectives for CBRN detection present challenges for the LAFD's first responders and HazMat teams. Without the use of a WSN, there is a delayed technical response, reduced notifications, and increased time frame before advanced mitigation efforts can begin because real-time environmental data needs to be established, which takes time. Wireless technology is a recent development within the LAFD. The objective is to develop a predictive model and concept of operations for employing, monitoring, and maintaining CBRN wireless sensor capability.

There is abundant literature regarding "Concepts of Operations" that covers a variety of applications, disciplines, and procedures, including the necessary components required to deploy the equipment. Unfortunately, there is a lack of any specific public-safety documentation concerning the concept of operations for CBRN wireless sensor networks. However, the information that does exist was examined for insight regarding the development of a CBRN ConOps document. For example, at the national level there

is documentation that supports the use and implementation of new technology as an efficient, cost-effective, and reliable solution for detecting and responding to CBRN incidents. The reference documents listed below are resources that help support a comprehensive LAFD ConOps for CBRN wireless sensor networks document:

- Counter-Chemical, Biological, Radiological, and Nuclear Operations, USAF;
- Energy-Efficient Networking Techniques For Wireless Sensor Networks, U.S. Army;
- Assessment of Chemical and Radiological Vulnerabilities, U.S. DOE;
- Domestic Terrorists' Intent and Capability to Use CBRN Weapons, U.S. Government;
- High Priority Technology Needs, U.S. Government;
- National Preparedness Guidelines, U.S. Government; and
- National Strategy for Combating Terrorism, U.S. Government.

These documents have detailed and specific information relating to the CBRN threat, vulnerabilities, emerging technology, and wireless capabilities. These reference materials also reinforce the policies and procedures related to CBRN wireless detection and further emphasize training and response protocols.

The 2007 National Preparedness Guidelines report states, "It is critical that all levels of government coordinate the development of interagency response protocols prior to the deployment of detection technology" (USDHS, 2007a, p. 18). One reason for the lack of policy and procedural plans is that CBRN wireless networks are new, innovative, and not widely utilized in the public-safety sector. With regard to literature that establishes CBRN wireless sensor network policy, procedures, and recommended practices for public-safety agencies, the documentation does little more than reinforce the need to head in that direction.

The review of available literature indicates there is considerable material covering a wide array of WSN applications. In the book titled *Wireless Sensor Networks. Technology, Protocols, and Applications,* many practical uses for WSN are discussed

(Sohraby, 2007). This includes coordinating with DHS to establish a nationwide sensor network to provide a real-time early-warning system for CBRN threats in the United States. A 2006 article in *USA Today* regarding homeland security indicated that DHS is focused on national security events, including athletic venues and arenas, which are considered viable targets in the planning scenarios (Andy, 2006). Wireless sensor applications and detection platforms are a practical tool within the homeland security architecture. Due to the relatively new expansion into the first-responder community, gaps exist in understanding, deployment, components, and design, leaving opportunity to increase the knowledge base within the public-safety domain. The literature elucidates the use of technology and reveals the ability to enhance homeland security and strengthen CBRN detection and response capabilities. Furthermore, policy and procedures need to be developed and introduced as part of an overall ConOps document as this technology moves forward and becomes part of the CBRN prevention and detection environment.

The literature addresses the challenges and advancements in the rapidly changing technological environment of WSNs. This thesis forms the basis for policy recommendations involving wireless CBRN sensor deployment with an emphasis on standardized procedures. The literature helps to define the conceptual landscape for practical applications in public safety, CBRN threat potential, and the operational environment. The objective is to develop a ConOps for the LAFD regarding CBRN wireless detection to enable the ability to optimally deploy assets to deter, detect, prevent, and respond to hazardous-materials threats. The goal is to determine the best way to utilize CBRN wireless sensors to maximize resources, provide early detection and notification, and ensure that public safety remains a top priority. WSNs provide a viable option towards that important endeavor. When complete, the LAFD ConOps for CBRN wireless sensors networks will outline an operation for future and existing systems, procedures, training, and maintenance that includes interagency roles and responsibilities.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

The concept of operations for CBRN wireless sensor networks within the LAFD supports current hazardous-materials operations. This analysis provides needed data and guidance for developing operational doctrine for LAFD HazMat teams to effectively manage deployment, information acquisition and distribution, and response. By focusing on what has been done in terms of developing a ConOps for CBRN wireless sensor networks, the LAFD's HazMat operations are able to determine the correct trajectory for implementing this technology. This requires examining various academic, professional, and government documents that discuss this emerging technology. In addition, LAFD operational manuals were evaluated to properly frame a ConOps for CBRN wireless detection and to determine goals and objectives. Technical reports and academic publications provided information on the challenges associated with this wireless detection and the proper tactics to ensure optimum performance. Standards are being applied to wireless sensor networks, and by working with the federal government, the LAFD can establish policies and govern these systems accordingly. This is a critical element due to the multidisciplinary, multijurisdictional nature of incidents involving CBRN materials or devices. This forms the basis for interaction among participants and stakeholders and is vital to the development of a concept of operations for CBRN wireless sensor networks.

The development of a concept of operations for CBRN wireless sensor networks includes examining the vulnerabilities and potential threats associated with the consequences of CBRN attacks on public facilities and critical locations. The potential threat requires the development of defensive strategies aimed at recognizing, detecting, and responding to CBRN threat and attacks. The implementation of specific countermeasures designed to provide early warning and identification of an attack in real-time is critical to reducing adverse health effects and limiting property damage. The goals, objectives, challenges, tactics, strategy, policies, governance, support agencies, and components are all central to implementing a CBRN wireless sensor network.

Wireless technology has developed rapidly in the past decade, and new applications are continually being introduced and implemented. The analysis involves highlighting the equipment required and capturing data along with the issues encountered to gain a better understanding of how wireless CBRN detection will enhance operational efficiency and increase safety. Through the analysis process, a formal concept for operational readiness took shape, identifying this technology as a viable early-warning and recognition tool vital for hazardous-materials prevention and response.

The analysis identified the need for command and control elements to have direct access to sensor data, response teams, and subject matter experts. Operational review and analysis of sensor displays and data collected during the actual deployments provide a baseline for future tactical operations, adaptation, and lessons learned. The wireless sensor framework is a mixed-initiative environment that supports HazMat activities with a multiagency, multidisciplinary approach to hazardous-materials response. This includes support for joint operations and command staff from different agencies, all working together in an effort to provide and maintain a safe environment based on threat information, trends, and capabilities. In the context of this work, operational elements include a wide variety of possible interactions among the various stakeholders, agencies, and response personnel. This includes real-time data acquisition and visualization of deployed sensors. Postdeployment review is a side benefit that allows a thorough critique of the operation, the hazards presented, and possible response options, based on environmental information collected.

A. GOALS AND OBJECTIVES

The goal of a CBRN wireless sensor network is to detect, collect, synthesize, distribute, and monitor the environment for hazards in real time. The objective is to assess that information, take appropriate action as early as possible, and make key notification to personnel. A WSN can accomplish these objectives in real time while providing first responders and subject matter experts a safe working environment. The ConOps document can serve as a reference for designing, deploying, and implementing a CBRN wireless sensor network in the public arena, where the threat potential is great.

> No longer could firefighters, police officers, emergency medical technicians and other emergency responders restrict their disaster planning and preparation to resolving the results of hurricanes, earthquakes, fires and the like. They could not be content knowing what to do in the event of a terrorist or criminal act involving guns, bullets and bombs. Now there was a new threat, that of a terrorist [with] a weapon containing toxic chemicals, biological pathogens or radioactive material. (Eifried, 2004)

Policies are necessary to govern the application of CBRN wireless sensor networks. The analysis from events, exercises, and deployments helps frame what is needed, the trajectory the technology should follow, and rapidity with which the change should occur. Due to the emergent nature and rapid growth of WSNs, many LAFD members have opinions, positions, and demands related to WSN capability.

The likelihood of ongoing technological change within the LAFD points to the value of establishing an adaptive learning system associated with new policies involving new equipment. This should include the ability to track and anticipate advances in CBRN wireless technology along with ways of implementing and using emerging wireless CBRN detection sensors. The development of a ConOps for CBRN wireless sensor networks must take these aspects into consideration. In addition, training and exercises can be augmented to include wireless sensor networks to help prepare personnel and to inform assisting agencies about this technology. The purpose of this analysis is to provide LAFD command structure and key agencies with reference material when it becomes necessary for strategic planning, team configuration, equipment acquisition, maintenance, training, and costs.

B. CONSTRAINTS AND TACTICS

The constraints and tactics associated with CBRN wireless sensor networks deal with the challenges and limitations associated with this technology. This requires the development of a standardized deployment model, security, notification protocols, information sharing, and training requirements. The environmental sensor application has special characteristics, such as high mobility, real-time monitoring, and maintenance requirements. This requires a set of protocols that takes into consideration the challenges of communication and interoperability and the manner in which those factors are

integrated and assessed for wireless sensor network applications. The tactical constraints associated with CBRN wireless sensor detection highlight the need for interoperability functionality. Wireless interoperability is important because it dramatically improves operational effectiveness and personnel safety. In order to take advantage of broadband applications and achieve interoperability, public safety systems must migrate to shared Internet protocol-based next-generation networks that are part of an "ecosystem" with commercial providers (Report Recommends Actions, 2007). This is especially true when performing in conjunction with allied fire and police agencies, regional resources, and specialized units to establish a common operating picture. What this means is that new protocols and support for both the hardware and software are needed to build a robust wireless sensor system. There is clearly a void in this area, largely due to the fact that there is no formal guidance structure that illustrates the correct sequence of equipment, personnel, training, or technology that should be acquired. The problem arises from multiple agents, confusing information, conflicting values, and competing interests.

Empirical analysis of ongoing CBRN wireless sensor network efforts is largely absent, and no independent comprehensive study of WSNs has been conducted for this purpose. This is not to say that these systems are not being explored, designed, and deployed in other areas. However, there is limited knowledge about setting up such systems, where or why they are forming, and the benefits realized. Based on data from private sector applications, some specific challenges related to wireless sensor networks include, but are not limited to, the following:

- Limited functional capabilities, including problems of size;
- Power factors;
- Node costs;
- Environmental factors;
- Transmission channel factors;
- Topology management complexity and node distribution;
- Standards versus proprietary solutions; and
- Scalability concerns. (Sohraby, Minoli, & Znati, 2007, p. 29)

WSNs have evolved from hard-wired systems into an ad hoc wireless network that shares many commonalities with those previous systems and yet has some unique characteristics. Due to these circumstances, WSNs that focus on CBRN detection have specific design and implementation requirements. In order to meet operational needs, these requirements can present certain challenges such as power requirements, communications, interoperability, and weather limitations. By understanding the limitations experienced in similar applications and by incorporating alternatives into our operational plans, these challenges can be managed accordingly.

Although there is an overall objective when deploying wireless sensor equipment, the focus is on the tactical and strategic elements in support of command staff and operational personnel. Planning and preparation for large public-gathering and high-profile events involve a combination of resources and equipment. Two modalities for deploying wireless sensor equipment are both tactical and strategic in nature.

Tactical Considerations:

- Specific site information;
- Controlled access to available sensor data;
- Detailed real-time sensor and environmental information;
- Data collection and analysis; and
- Instant situational awareness.

Strategic Considerations:

- Multidisciplinary, multiagency buy-in;
- Developed response. mitigation, and recovery data;
- Notifications (email, phone, SMS, etc.);
- Scenario-based planning; and
- Lessons learned and best practices.

A CBRN wireless sensor network can provide needed situational awareness for key locations, taking a preventive stance that incorporates environmental monitoring with technically trained emergency-response personnel. The application and deployment

potential for wireless sensor networks are limitless, and their use depends on the specific need, location, objective, sensor configuration, and system infrastructure requirements. The primary application for a CBRN wireless sensor network within the LAFD focuses on maintaining situational awareness, monitoring the atmosphere for contaminates, making notifications, connecting subject matter experts, and providing first responders and command personnel with real-time data on environmental conditions. Actual deployment and operational functions help define ease-of-use parameters.

> In literally hundreds of discussions with emergency responders during training sessions and other venues, some commonly desired characteristics of field detectors were frequently stated. Equipment needs to be user friendly, easy to train on and easy to use when the responder is in full protective gear. Because detectors of chemical and biological toxic material are not going to be used on a daily basis, the skills required to use them will be fragile, so the simpler the better. (Eifried, 2004, p. 16)

Terrorists have declared their intention to acquire and use weapons of mass destruction to inflict catastrophic attacks against the United States and its allies, partners, and other interests **(**Homeland Security Council, 2007). This type of threat poses a significant risk to the U.S. homeland and demands innovative ways to reduce our vulnerability in this area. The potential that chemical, biological, radiological, or nuclear materials will be used inappropriately or by terrorists requires a unified national response. This is especially true if CBRN devices are employed in crowded places, enclosed buildings, stadiums, subways, shopping malls, and other high-occupancy locations. To adequately address this threat requires taking advantage of available technology and incorporating faster and more reliable methods to detect, identify, and assess potential hazards. The objective is to utilize innovative solutions to connect hazardous detection equipment to a wireless system, creating a network of sensors accessible by an Internet connection.

There are numerous commercial and public-safety applications covering a wide spectrum of uses for WSNs. A sensor network is an infrastructure made up of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified

environment **(**Sohraby, Minoli, & Znati, 2007, p.1). These can include agriculture, road service, traffic, military, border patrol, maintenance, and building automation. The focus is on using WSNs for CBRNE detection within the homeland security environment, paying particular attention to mass-gathering special events and critical public locations.

An important aspect of homeland security at the local level addresses securing public areas, buildings, and mass-gathering locations from terrorist attacks, as emphasized in the 2007 National Preparedness Guidelines. An effective, real-time wireless sensor detection program will increase the probability that CBRN materials are rapidly detected, identified, and safely managed at critical locations and events. The integration of WSNs into the LAFD HazMat operations is a viable solution and provides response personnel with the right technology to protect the public against intentional hazardous materials releases. Within the homeland security environment, CBRN detection and identification is a promising WSN application, easily deployable, in a very short time. The proper use and implementation of a WSN reduces response and mitigation costs because of the early warning and product identification features. This is an efficient, cost effective, and reliable solution for detecting and responding to CBRN incidents. Rapid identification—a qualitative and quantitative determination of the unknown agent—is necessary for the selection of adequate protective measures (protective masks and clothing, as well as medical treatment), the mapping of the contamination area, and the identification of decontamination procedures (Vijayaraghavan, Ganesan, & Raza, 2010).

C. POLICIES AND GOVERNANCE

The policies and governance required by the National Preparedness Guidelines helps to establish the need to standardize detection methods and formalize wireless sensor applications. The necessary policies and governance begin with the premise that continual effort must be made to improve efficacy in the area of CBRN detection. This new technology requires guidelines and universally accepted applications.

This source is meant to inform and educate national security professionals on joint and integrated operations, security policy, strategy, guidance, and training to meet

tomorrow's challenges. Rapid technological change in the CBRN detection arena combined with improved communications and reduced costs has significant opportunities. Against this background, policies need to be established, and governing bodies must recognize that traditional HazMat operations need to be upgraded with more appropriate instruments. Of particular concern are the labor-intense, time-consuming models used to detect and assess CBRN hazards. Indeed, with fire departments relying increasingly on commercial, off-the-shelf sensor equipment, developing guidelines for this technology is economically justified. Although the technology has moved forward, the documentation specific to the public-safety arena has not kept pace. Policies associated with governance are needed.

Planning and procedures include the necessary functions that foster authority, operating guidelines, communications, and emergency actions. The equipment and personnel must meet established principles for operating wireless sensor detection apparatus. The LAFD hazardous-materials personnel must have a developed CBRN wireless sensor network plan. The ConOps lays down a set of principles that address the desired goals and objectives set within a policy that governs the stakeholders working on CBRN detection. The literature helps to define the practical applications associated with this technology and helps to maintain standards applied to wireless sensor networks. This includes providing a safe and healthy workplace for all responders.

D. ENABLING INFRASTRUCTURE

1. Remote SME Collaboration

One of the benefits of using Wireless Sensor Networks is the ability to bring together different subject matter experts from fire, law, and health personnel, all capable of monitoring the sensor data from a remote and safe location. WSNs allow multiple SMEs to detect, identify, measure, locate, and track CBRN products as they enter or are released within an environment.. The sensor information can be made immediately available to any supporting agency, providing real-time situational awareness on environmental conditions. The ability to maintain situational awareness and make real-

time decisions relies on the ability to have accurate and timely information. The deployment of a WSN provides allied agencies with the information necessary to deploy or redirect their assets as conditions warrant. Response times are reduced because any activation or trigger immediately notifies all stakeholders with site-specific data, facilitating a more thorough assessment of the conditions and resources that might be needed. Information exchange, coordination among the participating entities, allocation of available resources, and decision making are byproducts of a WSN ConOps document.

This dynamic is emphasized by the formation of joint hazard assessment teams (JHATs). One of the steps taken toward addressing the threat of terrorism involving CBRN materials was the formation of a JHAT in Los Angeles. This process involved the assembly of technical experts from different agencies, such as fire, police, health, FBI, and military. The JHAT performs as a single entity with joint operational capability irrespective of agency affiliation. In the event of a real threat, the JHAT team provides immediate on-scene technical assessment capability that can be deployed rapidly, has already been integrated into the command structure, and has established liaisons with special operations teams assigned to support the event (Hawley, Noll, & Hildebrand, 2009, p. 3).

A JHAT is a multidisciplinary, multijurisdictional team working in concert and capable of providing the incident command team with the best intelligence and specialized skills as a unified team. This provides the incident commander and supporting agencies with a force capable of providing the best possible options for incident resolution. The combination of resources provides all the stakeholders with the critical data and threat information to more effectively manage the incident. The team performs as a single entity with joint operational capability. Specific duties include the ability to provide:

- Credible assessment of the threat and the strategic impact of the event;
- WMD and CBRNE tactical information;
- Technical data on the type of hazard or agent present;

- Recommended size of the perimeter, exclusion zones, and evacuation distances;
- Options for mitigation (HazMat), render safe procedures (bomb squad), and the control of active shooter(s) (SWAT);
- Patient viability, decontamination, and rescue potential;
- Personal protection equipment (PPE) selection; and
- Specialized resource needs and location.

In Los Angeles, a networked approach such as the JHAT, combined with wireless sensor equipment, Internet conductivity, and subject matter experts, means public safety interests are addressed using available technology directed toward achieving a common objective. Typically, only command post personnel would have access to incident data; however, by utilizing technology and working jointly with supporting agencies, information can be shared and accessed by all stakeholders.

2. Flexible System Configuration

The deployment of WSNs is a vital instrument that can be used for fixed facilities and mobile units and on an ad hoc basis for special events. Early detection, mapping, and monitoring hazardous products in public places are key homeland security priorities. The ability to deploy these systems quickly, at relatively low cost, provides early detection for first responders. Taking advantage of this technology improves environmental coverage and detection capabilities at predefined and designated locations. The net effect of this arrangement is reduced false alarms and quicker response. This equates to better decision making and more efficient use of limited resources. Evolving requirements for new WSNs include, among others:

- The ability to respond to new toxic chemicals, explosives, and biological agents;
- Enhanced sensitivity, selectivity, speed, robustness, and fewer false alarms; and
- The ability to function, perhaps autonomously, in unusual, extreme, and complex environments (Sohraby, Minoli, & Znati, 2007, p. 87).

Advancements in wireless technology and sensor equipment allow public-safety agencies the ability to predeploy a WSN, in an ad hoc fashion, if necessary, and in a highly dynamic environment. The mobility and transportability allows this technology to be applied anytime and anywhere there is a CBRN threat to a specific location or venue.

The ability to ensure public safety at large-scale, high-profile, mass-gathering events such as the Grammy Awards, Golden Globe Awards, Emmy Awards, Academy Awards, Rose Bowl, NBA Finals, and other special events presents challenges to response personnel. As a result, federal and local agencies are now working together for high-profile events like the Emmys and Oscars in a way they never had before because the world changed on September 11, 2001 (Wang, 2002). Security, emergency response, evacuation, and event planning have been forever changed when dealing with large groups of people gathered in one location. The Department of Homeland Security has established a priority classification for national security–special events of this nature. This includes athletic events and arenas, which were identified as viable marks in a Department of Homeland Security (DHS) planning scenario (Andy, 2006). DHS is coordinating an effort for the end-of-decade deployment of a nationwide sensor network to provide a real-time early-warning system for a plethora of chemical, biological, and nuclear threats across the United States (Sohraby, Minoli, & Znati, 2007, p. 88). These plans include developing capabilities for mass transit and other public gathering locations to deal with CBRN threats targeted at airports, subways, and buildings.

It is unfortunate, but a fact of modern life includes the existence of terrorist groups and individuals. Mass-gathering locations provide an opportunity to make a statement by setting off a device or by releasing a hazardous substance. Key historical dates and events, large public gatherings, and locations or meetings with political, social, or ethnic agendas are only a few of the targets likely to provide terrorists with a means to present their message (United States Army, 2000).

3. Open Architecture and Components

The WSN architecture incorporates technology, wireless components, and existing sensor equipment to provide environmental and threat monitoring of specific locations. There are four basic components in a sensor network:

1. An assembly of distributed or localized sensors;
2. An interconnecting network (usually, but not always, wireless-based);
3. A central point of information clustering; and
4. A set of computing resources at the central point (or beyond) to handle data correlation, event trending, status querying, and data mining. (Sohraby, Minoli, & Znati, 2007, p. 1).

The equipment and technology is configured, so that it can be portable and adaptable to meet building and environmental parameters. This is accomplished by deploying different sensing equipment in key positions within target buildings, special events, and transportation areas. The technical competency is enhanced by involving the different public-safety disciplines. This allows for a more thorough assessment of the vulnerabilities and potential threats associated with each location. From a situational awareness perspective, the goal is to produce a virtual environment by strategically placing sensor, GSP, video, and weather monitoring equipment at designated locations where large groups of people will gather.

In order to achieve the intended functionality, several components and their characteristics must be identified and taken into consideration. WSNs are a combination of sensors, communication elements, software, hardware, and personnel to monitor, interpret, analyze, and respond to the data. The system components include:

- Sensors (CBRNE, temperature, humidity, wind, GPS, video);
- Connection (Ethernet, IrDA, analog, TTL, RS232);
- Communications (network, gateway, router, Internet, WiFi, cellular, satellite);
- Software (GIS, Plume, Live Sensor, video, Hazard Guidance, reference);

- Destination (command post, subject matter experts);
- Notifications (web service, email, TCP/IP, phone, radio);
- Information Sharing (NIEM, EDX/CAP, XML); and
- Alerts (text to voice, SMS, email, pager, radio).

The individual components all function together, establishing a network that can detect, measure, locate, track, and report on a hazardous substance release, fire, oxygen level, flammable environment, and the presence of radioactive particles. This framework has the capability to maintain historical data in order to replicate events and detection alarms for future evaluation and analyses. There are two sensor deployment configurations that can provide environmental coverage. Sensors and monitors can be stationary, positioned in a fixed, clandestine position, and deployed prior to an event. This allows for testing and dry runs to be conducted, which helps to establish a baseline for environmental conditions. Another deployment model uses mobile sensors attached to personnel and vehicles. The mobile configuration provides detection coverage over a wider area and allows for manual adjustments due to changes in conditions. A potential drawback of mobile configurations deals with the potential to lose connectivity to network infrastructure. This can occur for a number of reasons, such as the distance, range, signal strength, obstructions, and power supply. The ideal scenario incorporates both fixed and stationary sensors coupled with mobile sensors to provide the best detection capability.

THIS PAGE INTENTIONALLY LEFT BLANK

V. FINDINGS

Employing a wireless CBRN detection network will support the LAFD's hazardous materials response, enabling better coordination and communication among the various stakeholders. At the present time not much has been done within the context of establishing protocols for wireless sensor networks within the public-safety domain. The nation is at a critical juncture regarding the future of emergency communications (House Homeland Security Subcommittee, 2010). DHS and other government agencies have recognized the need to enhance communications systems at the local, state, and federal levels across all disciplines. We have an opportunity to change the trajectory of United States response to emergency events (House Homeland Security Subcommittee, 2010). The inclusion of this technology at the local level is a step towards enhancing communications, detecting hazardous materials early, and sharing vital information among the various constituents associated with terrorism and homeland security.

The material examined helped to outline the goals and objectives, enabling the formation of a concept of operations for CBRN detection utilizing a wireless sensor network within the LAFD. The research determined that the implementation of a wireless sensor network fell in line with DHS recommendations to strengthen the ability to detect, distribute, and share homeland security incident information across agencies. The literature reinforced the need to develop and implement a system that could help identify CBRN hazards early and provide a mechanism to make that information available to all stakeholders. The action taken in the greater Los Angeles area includes using wireless sensor technology to increase the identification and response time in the event that CBRN material is released into the atmosphere. This technology is available and being explored in different capacities, emphasizing the need for wireless sensor network protocols. Currently, immediate action by first responders is required to help victims severely impacted by a fast-acting hazardous agent. To increase the lead time, it is important that wireless sensor monitoring equipment be deployed and activated to provide as much early warning as possible in order to increase survivability and facilitate evacuation.

The research identified possible constraints with wireless sensor networks, including limitations on tactical deployments. There was considerable information that represented the best solutions to the various applications to increase effectiveness. An important finding included some challenges associated with wireless networks that focused on architecture, protocols, modeling, and analysis. Some key aspects were brought to light, such as trends in other settings and cutting-edge applications that could be tailored to work with the public-safety, emergency-response framework. This helped identify tactical elements and considerations necessary when deploying this equipment. The material researched provided the background and understanding for developing a concept of operation around CBRN wireless sensor networks suitable for the fire service. Furthermore, review of the literature helped to establish limitations, such as power supply and Internet reliability, which could interfere with deploying wireless equipment in certain locations.

There is a need to establish policies to govern the application of an LAFD concept of operations regarding wireless sensor detection. The material examined highlighted the benefits, architecture, resources, and alternatives for such a system. The policy must reflect changes and desired outcomes as the system continues to take shape. Policies will help to establish procedures that guide how decisions are made and how the tasks are performed when utilizing WSNs. A ConOps for CBRN wireless sensor networks will be a foundation document. Well-written policies and procedures will increase accountability; they are fundamental to quality assurance and improvements. This includes determining how supporting agencies should interact. In the absence of a written ConOps, unacceptable different approaches will make the LAFD inconsistent and ineffective during these operations.

The research process helped to define the enabling infrastructure that supports a concept of operations for the LAFD's wireless sensor detection plan. The framework for a WSN program is based on the technology currently being used in other areas, such as the military and within the private sector. The LAFD takes a holistic view of the technology helping to outline a practical method to wirelessly detect hazardous releases, predict product dispersion patterns, determine exposure levels, and integrate live video

feeds. The ground work previously completed allows a more precise understanding of the environment, the equipment, and the personnel required to ensure an effective wireless detection system. WSNs provide and maintain situational awareness with respect to location, anticipated threats, product identification, and weather and climate conditions. Interoperable sensor technology opens a path to fully exercise the risk assessment phase demonstrated in actual conditions. The quantitative summary of the benefits include the capabilities, enhancement to current CBRN operations, deleted tasks, and improved efficiency. With this in mind, "chemical detection in the civil market is fairly straightforward" (Winfield, 2004, p. 61). However, simply detecting CBRN materials is not enough for fire and police agencies. When such materials are released, they must respond, evacuate, treat, and take action to mitigate the effects of any release. The sort of scenario in which a civilian force will find itself, where an explosion has already taken place in an area of high population density (Winfield, 2004, p. 61) requires chemical and radiation detection systems, GIS, and weather information.

> Thus, a basic chemical agent monitor that can confirm what their eyes are seeing (people in obvious pain) is adequate for most forces. There is some interest in capital cities, City of London for example, in having a GID24/7[6] type system that can be placed on buildings and networked to provide both a situational awareness picture and a warning of chemical attack. This has already been done for large events, such as the Commonwealth Games in the UK and is likely to be chosen for the Olympics. (Winfield, 2004, p. 62)

This is a low-probability–high-consequence event that maximizes resources trying to address the CBRN threat. Based on case studies and the analysis of specific requirements for CBRN detection, wireless sensor networks offer a practical solution.

There are some disadvantages and limitations associated with this technology. The initial drawback will be the startup cost for the new equipment. Although some WSNs can be designed to utilize existing sensor equipment, there is still a need to acquire supporting hardware and software. The costs associated with establishing a WSN include

[6] The GID (24/7) is a continuously operating low "through life" cost networked fixed point CW Agent Detector System suitable for military and commercial applications inside critical facilities, buildings, and transportation systems. See www.smithsdetection.com.

the cost to train and familiarize personnel with the new equipment. This will include providing a brief understanding of the practical applications and tactics required to ensure optimum performance. Furthermore, since this is considered a specialized operation, access will need to be limited to a select group of highly trained personnel.

Another limitation will arise in having personnel take on new responsibilities, including allied agencies requiring a need to define their roles. The initial phase of implementation may bring about some anxiety, as is frequently associated with introducing new technology. User misunderstanding may also present problems because the equipment has not been exposed to all stakeholders, both internal and external, requiring close coordination with allied agencies. When looking for available equipment, interoperability, and compatibility, it will require research to identify a vendor with credibility. In addition, developing a working relationship with the vendor is essential for understanding the agency's needs and long-term requirements. This will include ensuring that service and maintenance concerns are addressed for equipment and software upgrades.

Despite the challenges, sensible wireless applications are being incorporated into the LAFD planning and operation phases. This includes utilizing the technology for mass-gathering and large, high-profile events that would results in a high casualty count if a CBRN device were deployed.

A. THE LAFD CONOPS FRAMEWORK

The process needed for a successful ConOps requires a comprehensive evaluation of elements that enables all stakeholders, both strategic and tactical, to understand the capabilities, benefits, and intent of a CBRN wireless sensor network. The key aspects should include the following:

1. The purpose and overview of a CBRN wireless sensor network;
2. When the CBRN wireless sensor network should be deployed;
3. All the necessary equipment, software, and components that allow a wireless sensor network to function;

4. The setup requirements, maintenance, and environment for operational efficiency;

5. The personnel and training needed to install, maintain, monitor, analyze, and respond to alarms and activations;

6. The interoperability features and characteristics that allow the ability to interface with other systems;

7. The system or operation that the CBRN wireless sensor network is intended to enhance; and

8. How to properly integrate a CBRN wireless sensor network into current hazardous materials operational plans.

The ConOps framework needs to address the following issues:

(1) Scope: This section should provide an overview of the system, current situation, background, objectives, application, and effectiveness.

   (a) Vision

   (b) Justification for change

   (c) Outline of the document contents, reference documentation

   (d) Purpose and need for implementing a CBRN wireless sensor network

   (e) Benefits and intended consequences

   (f) Limitations and challenges

(2) Reference and Case Studies:

   (a) Academic and operational background

   (b) Case studies from exercises and deployments

   (c) Mission requirements and operational needs

   (d) Policy and protocols

(3) Operational Roles and Responsibilities:

   (a) Hazardous-materials teams

   (b) Deployment considerations

(c) Operational procedures

(d) Response considerations

(e) Notification protocols

(f) Allied agency involvement and responsibility

(4) Component Overview:

(a) Major system components and interconnections

(b) Functionality and capabilities

(c) Interfaces and external systems requirements

(d) Interoperability and relationship to other systems

(e) Maintenance

(f) Performance characteristics

(g) Portability, reusability, survivability

(5) Policy and Protocols:

(a) Continuity of operations

(b) Privacy

(c) Safety

(d) Security

(6) Summary:

(a) Analysis

(b) Impact

(c) Costs

(d) Training

The ConOps should include the necessary information to reflect the LAFD's vision as it pertains to integrating wireless sensor technology into hazardous-materials operations. The ConOps should include expectations of the benefits that the system will

provide. This will require leadership to ensure that all stakeholders have a voice in defining the prospects for deployment, time, costs, and expertise needed for implementation. This involves technical research in order to conceptualize the system requirements and the subsystems that will make wireless sensor networks viable.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS

The LAFD's "Concepts of Operations for CBRN Wireless Sensor Networks" is an internal effort within the hazardous-materials section to assure that the proper application and capability exists for essential detection functions across a wide range of threats involving CBRN materials. There is a desire to develop and implement WSNs into LAFD operational plans, especially to detect CBRN threats early and in real time. Policy recommendations should include interoperability concerns such as governance, standard operating procedures, technology, training, and usage (USDHS, 2007b, p. 3). In the context of public safety, a ConOps document requires a holistic approach, incorporating national recommendations, and taking into account communication standards and available wireless technology.

The ConOps should involve mission-essential functions, including plans and capabilities in both emergency and nonemergency roles. This will entail delegating authority and combining subject matter experts from allied agencies to ensure that knowledgeable personnel are involved in the development process. Key elements should include equipment, tracking, monitoring, identified facilities or locations, resources, response capability, alarm thresholds, and notification protocols. This will establish a foundation for response with adequate resources necessary for the performance of hazardous-materials operations involving CBRN wireless sensor detection. The ConOps document supports the LAFD's level of readiness and capability to respond, detect hazards, make notifications, and coordinate resources with and without advanced warning.

Guidance and leadership should take a "best practice" stance to ensure that a solid research and business foundation is developed to make decisions that are financially sound and provide value to the LAFD and the public. This requires creating budgets and schedules, strategic planning and goal setting, project coordination, cost-benefit analysis, and return of investment comparisons. In today's economy these measures are becoming a fundamental element within the hazardous-materials operational process. All levels of

command within the LAFD hazardous-materials section should plan, budget, and execute their ability to support wireless sensor network operations.

It should be understood that implementing a WSN is a multidisciplinary operation requiring unified coordination among agencies. The supporting organizations and interactions among participants and stakeholders will improve the LAFD's CBRN detection operations by identifying essential functions within each agency to assure the coordination of operations, align deployment and response, and facilitate tactics and strategy. This includes providing a wireless sensor network understanding for command elements within each organization. The effort should focus on the available support within the various government authorities that have response and legal responsibilities to prevent, protect, respond, and mitigate CBRN threats.

The ConOps should determine the associated risk based on threat information, including past attack scenarios. This understanding is necessary to determine the trends and potentials, capabilities, locations of targets, vulnerabilities, and capability of resources, both internal and external. This may involve situations that require preplanning facilities, assessing public venues, and reconnaissance of surrounding infrastructure before deploying wireless sensor equipment. Response elements must understand the environment, determine the potential hazards, and alert other critical personnel. The LAFD hazardous-materials wireless sensor detection program should be designed to enhance mission effectiveness by incorporating a teamwork philosophy to apply the appropriate capabilities in concert with allied agencies to provide early detection, rapid response, identification of hazards, and control against the recognized risks.

The basis for this approach sets the stage for meeting stated goals and objectives for WSN within the LAFD's hazardous-materials program. This approach will shift the focus from a "risk aversion" to "risk management" perspective by providing access to subject matter experts across the spectrum of emergency response. A careful balance in the mitigation of a CBRN risk can be accomplished through effective integration of other critical networks, including the Los Angeles Police Department, Los Angeles County Health, the Los Angeles Sheriff Department, the Los Angeles County Fire Department, and fusion center resources. This process should evaluate the criticality of the hazardous-

materials mission and determine the degree of CBRN exposure and the severity of risk to the responders, the public, the environment, and the facility. If a CBRN sensor reaches established preset thresholds, LAFD hazardous-materials personnel should focus risk management and response activities toward these functions:

- Detection;
- Identification;
- Response;
- Notification;
- Isolation;
- Evacuation; and
- Mitigation.

These activities should focus on the ability of responding agencies to:

- Reduce the vulnerability;
- Reduce the risk; and
- Reduce the exposure.

The ConOps provides an opportunity to evaluate the wireless CBRN detection and response models while determining the risk of each capability and establishing mitigation priorities. Consideration should be given to identifying the capabilities and controls necessary to ensure mission continuation throughout the detection and response process. This will include checking for overlap and providing redundant capabilities to ensure:

- Creation of dual-use equipment based on mission priorities;
- Secure portals for routine and emergency information dissemination;
- Mission capability through enhanced communication networks;
- Security classification and need-to-know aspects when determining operational plans; and

- Fiscal accountability.

Inherent in this responsibility is the need to formulate guidance for the LAFD's hazardous-materials program. This should include the development of viable, executable wireless detection plans that take into account interagency coordination as appropriate and that oversee and assess the status of CBRN wireless sensor detection readiness. The key elements necessary to maintain continuity of operations and enhance decision making are the command and control aspects that can be achieved through organization of appropriate subject matter experts in the areas of communications, computers, intelligence, and hazardous materials.

It is important to incorporate and institutionalize CBRN wireless sensor network concepts into relevant LAFD doctrine, policies, strategies, programs, budgets, training, exercises, and evaluation methods. This will require a comprehensive and effective hazardous-material program that is adequately planned, designed, programmed, and budgeted to ensure the CBRN hazardous-material continuity that is essential for providing uninterrupted operation, irrespective of personnel changes, promotions, or retirements.

Command-level officers need to incorporate administrative requirements into the ConOps that support the planning and execution of budgets including equipment, maintenance schedules, service costs, and replacement costs, as required. These include assets and resources to develop, maintain, and operate facilities, communication, and transportation equipment. In addition, command personnel need to consider the development of plans that will validate and update operational needs based on mission requirements and new available technology.

Another key element is an outline of the decision process for determining appropriate actions in implementing operational plans and procedures, with or without warning, during duty and nonduty hours, that provides for alert and notification of response elements to include SMEs, outside agencies, and command-staff personnel. In the planning phase, consideration should be given to addressing the "stand-down" and "notification" aspects so that operations can transition back to normal. Based on a tiered

response and notification matrix, it is important to identify and prioritize mission-essential functions and personnel. Additional consideration should be directed toward equipment identification, storage, protection, and availability for use at remote sites and regional locations. An inventory and maintenance process should capture the vital records, materiel, training, and databases required and created.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

In this final chapter, a summary of the important elements, limitations in research, and suggestions for future work are discussed as they relate to the concept of operations for CBRN wireless sensor detection within the LAFD. Wireless technology helps to address the CBRN threat by being able to identify hazards early, more accurately, and with fewer resources. Moreover, this technology will allow subject matter experts to view sensor data and "weigh in" on the potential threat and environmental conditions and to make informative decisions based on real-time information. Alerts and notifications can be sent using a variety of communication formats that will ensure that the proper personnel are contacted and informed.

The research focused on establishing a concept of operations document for the LAFD's hazardous-materials program that addresses the integration, implementation, and deployment of a CBRN wireless sensor network. However, the research goes further than the LAFD's HazMat program. Based on the data analyzed, the concept extends beyond a particular wireless sensor platform or system. The essence of this research was to understand the technology involved, along with the tactical and operational capabilities to determine the feasibility and value. The end result is that the LAFD will benefit from this type of system because the technology will facilitate timely, accurate information flow to command staff and subject matter experts, allowing better decisions.

The material examined did not focus on hardware-related problems, software failures, or testing criteria. The idea was to concentrate on the possibilities and necessary elements critical to the development of a ConOps document for CBRN wireless detection, rather than specific design and equipment features. A ConOps document is extremely important for HazMat specialists to properly deploy and respond to detection alarms. A ConOps forms the basis for integrating wireless detection capability into the LAFD's hazardous-materials operations, taking key information into account. The detection capabilities are a vital element of the ConOps and should address specific TICs, TIMs, and CWA agents.

The CBRN wireless detection architecture is very important when designing and implementing an effective protection capability for the fire service. Many factors need to be weighed, such as risk assessment, performance standards, communication protocols, and detection technologies. However, the ConOps aspects focus more acutely on the capability and operational aspects, leaving the technical data for future projects. The components are an important consideration, although detailed specific information was not necessary for the operational ConOps. The research focused on the practical application of WSNs for locations and events that present a target to terrorists, such as sporting events, high-profile entertainment venues, and mass-gathering sites. The technical aspects were not discussed or researched; concentration was given instead to the possibilities and practical homeland security applications. This approach addresses the possible aspects, intended use, and agency participation.

The future of hazardous-material detection lies within technological solutions such as wireless sensor networks. Ultimately, wireless sensors will become more common and will provide for greater public safety as this technology continues to evolve and take shape within the homeland security architecture. The integration of WSN into hazardous-materials operations will enable stakeholders and other fire service organizations to obtain critical environmental data quickly and to provide a system to share that information across all disciplines. Agencies may choose to collaborate, to share information about new technology developments, to achieve the benefits of joint purchasing, to share information processing or business process services, or to develop new technologies for supporting interaction and interoperability among their participating organizations (Williams et al., 2009). Fire, police, and health agencies have recognized the value of this technology and are moving forward to incorporate wireless applications to detect and respond to a variety of threats and hazards.

The implementation of the proposed CBRN wireless sensor network may have wide-ranging impacts for the Los Angeles Fire Department, regional fire departments, and allied agencies with hazardous-materials response capability. It is anticipated that the LAFD will have to adapt the changes to the way that HazMat operations are conducted in order to achieve the agency's mission, goals, and objectives in CBRN detection. The

CBRN wireless sensor network will help facilitate these changes by demonstrating a safer, quicker, and more reliable response posture. The LAFD has been responsive to the need to integrate wireless technology into its detection capabilities, and it accepts the challenge by revising the department's HazMat processes to include conceptual CBRN modeling and architecture. The integration of a wireless sensor detection system will provide decision support for IC management for CBRN incidents.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allegra, P. C., D. Cochrane, E. Dunn, P. Milano, J. Rothman, & J. Allegra. (2005). "Emergency department visits for concern regarding anthrax—New Jersey, 2001." *Morbidity and Mortality Weekly Report*, suppl. Syndromic Surveillance, 54.

Ananda, A., M. C. Chan, & W. T. Ooi. (2006). Mobile, wireless, and sensor networks: Technology, applications and future directions. Hoboken: NJ: Wiley Interscience.

Andy, G. (2006). "Homeland security ready to assist colleges, sports venues if needed. *USA Today*. Retrieved July 28, 2011, from http://www.usatoday.com/sports/college/football/2006-09-07-security_x.htm

Asal, V., R. Rethemeyer, G. Ackerman, & H. Park. (2010). "Connections can be toxic: Terrorist organizational factors and the pursuit of CBRN terrorism." Retrieved August 1, 2011, from http://search.proquest.com/docview/749419592?accountid=12702

Barrett, M., & D. Goure. (2008). "Chemical and biological threats: Surveillance as the first line of defense." Retrieved August 10, 2011, from http://www.lexingtoninstitute.org/library/resources/documents/Defense/chemical-biological-threats.pdf

Bharat Book Bureau. (2010). "CBRN defence market 2010-2020." Retrieved July 8, 2011, from http://search.proquest.com/docview/89119040?accountid=12702

Buratti C., A. Conti, D. Dardari, & R. Verdone. (2009). "An overview on wireless sensor networks technology and evolution." *Sensors* 9, no. 9: 6869–96.

Campbell, J. K. (2007). "Excerpts from research study 'Weapons of mass destruction and terrorism: Proliferation by non-state actors.'" *Terrorism and Political Violence* 9, no. 2: 25.

Casaca, D., & D. Westhoff. (2006). "Scenario definition and initial threat analysis." UbiSec&Sens Project. Retrieved August 9, 2011, from http://www.ist-ubisecsens.org/deliverables/D0.1_060628.pdf

Cheour, R., K. Lahma, & M. Abid. (2011). *Evolution of wireless sensor networks and necessity of power management technique*. Sfax, Tunisia: CESlab, National School of Engineers of Sfax.

City of Los Angeles. (2010a). “City of Los Angeles hazardous materials annex.” Retrieved August 12, 2011, from http://emergency.lacity.org/stellent/groups/departments/@emd_contributor/documents/contributor_web_content/lacity/_013165.pdf

City of Los Angeles. (2010b). “Los Angeles Fire Department emergency operation plan (EOP). Critical incident planning and raining section, disaster management planning unit.” Internal fire department document available upon request.

Doane, C., & J. DiRenzo. (2007). Nuclear, biological, chemical weapons of mass destruction: Detection, warning, protection and countermeasures. *Naval Forces* 28, no. 4: 87–91. Retrieved August 6, 2011, from http://search.proquest.com/docview/199355396?accountid=12702

Eifried, G. (2004). What responders need to respond: Chemical and biological point sensors for homeland defense. Washington, D.C.: EAI Corporation.

Faiola, A. & A. Karla. (2009). “Britain convicts three in plot to rival 9/11.” *Washington Post*. September 8, 2009. Retrieved September 15, 2011, from http://www.washingtonpost.com/wp-dyn/content/article/2009/09/07/AR2009090700560.html?hpid=sec-world

Federal CIO Council. (2010). “Exchange functional standards evaluation adoption and use of the National Information Exchange Model (NIEM). Retrieved August 23, 2011, from http://www.niem.gov/pdf/AssessmentReport.pdf

Finegan, W. (2008). “The chemistry of counterterrorism.” *Law enforcement technology* 35, no. 4: 104–9. Retrieved July 28, 2011, from http://search.proquest.com/docview/229832952?accountid=12702

Fire, F. L. (2007). “Introduction to chemical warfare agents.” *Fire engineering* 160, no. 11: 125–31. Retrieved August 8, 2011, from http://search.proquest.com/docview/229086997?accountid=12702

Frinking, E., T. Sweijs, T. V. Dongen, & E. Ethembabaoglu. (2009). *Navigating the CBRN landscape of 2010 and beyond: Towards a new policy paradigm*. The Hague Centre for Strategic Studies.

Galarraga, H. E., P. F. Annunziato, S. M. Funk, & D. E. Green. (2009). Next generation sensor technology, now. *Defense AT&L* 38, no. 6: 12–16. Retrieved July 12, 2011, from www.dau.mil/pubscats/ATL%20Docs/Sep_Oct/sep-oct09_datl.pdf

Garwin, T. M., N. A. Pollard, & R. V. Tuohy. (2004). *National technology plan for emergency response to catastrophic terrorism*. National Memorial Institute for the Prevention of Terrorism. Washington, D.C.: Hicks & Associates.

Godso, D. W., C. Datte, R. Patel, F. Mirabile, & J. S. Steinman. (2006). "Network ready CBRN sensors: A way forward." Sensors Applications Symposium, Joint Project Manager Information System. 2006 IEEE Proceedings. ISBN:0-7803-9580-8.

Graham, B., T. Talent, A. Graham, R. Cleveland, S. Rademaker, T. Roemer, W. Sherman, & H. Sokolski. (2008). *World at risk: The report of the Commission on the prevention of WMD proliferation and terrorism*. Vintage Books. http://www.preventwmd.gov/report/

Grilo, A., A. Casaca, & M. S. Nunes. (2009). "The use of wireless sensor networks for homeland security." International Conference on Communication, Computer and Power (ICCCP'09).

Hawley, C., G. Noll, & M. Hildebrand. (2009). "The need for joint hazard assessment teams." *Fire Engineering*. Retrieved July 6, 2011, from http://www.fireengineering.com/index/articles/display.articles.fire-engineering.volume-162.issue-9.terrorism-and-the-fire-service.the-need-for-joint-hazards-assessment-teams.html

Hayes, J., S. Beirne, K. Tong Lau, & D. Diamond. (2008). "Evaluation of a low cost wireless chemical sensor network for environmental monitoring." IEEE Sensors Conference.

Heirston, B. (2010). "Firefighters and information sharing: Smart practice or bad idea?" *Homeland Security Affairs* 5, no. 2. Retrieved August 27, 2011, from http://www.hsaj.org/?fullarticle=6.2.6

Hincal, F., & P. Erkekoglu. (2006). "Toxic industrial chemicals (TICs)—Chemical warfare without chemical weapons." *FABAD Journal of Pharmaceutical Sciences* 31, no. 4: 220–28. Retrieved August 23, 2011, from http://search.proquest.com/docview/218196229?accountid=12702

Homeland Security Council. (2007). "National strategy for homeland security."

Houghton, B. (2004). *Gearing up and getting there: Improving local response to chemical terrorism*. Santa Monica, CA: RAND Corporation.

"House Homeland Security Subcommittee on Emergency Communications, Preparedness, and Response Hearing." (2010). Federal Information & News Dispatch, Inc. Retrieved July 8, 2011, from http://search.proquest.com/docview/858795250?accountid=12702

Ilyas, M., & I. Mahgoub. (2004). Handbook of sensor networks: Compact wireless and wired sensing systems. CRC Press. ISBN 0-8493-1968-4.

Jackson, B. (2001). Technology acquisition by terrorist groups: Threat assessment informed by lessons from private sector technology adoption. RAND Corporation.

Jakucs, R. M. (2003). "WMD with toxic industrial chemicals and the Marines Corps response." *Marine Corps Gazette* 87, no. 4: 42–43. Retrieved July 23, 2011, from http://search.proquest.com/docview/221440926?accountid=12702

"Los Angeles County Operational Area (LACOA) Operation Golden Phoenix 2010." (2010). Retrieved August 7, 2011, from http://www.cawnps.org/press.asp

"Los Angeles Fire Department hazardous materials operational plan (HMOP)." (2003). Internal fire department document available upon request.

Magnuson, S. (2011). "DHS program gives hazardous materials teams networked sensors." *National Defense* 95, no. 691: 32–33. Retrieved September 12, 2011, from http://search.proquest.com/docview/871566446?accountid=12702

Majchrzak, A., S. L. Jarvenpaa, & A. B. Hollingshead. (2007). "Coordinating expertise among emergent groups responding to disasters." *Organization Science* (Jan/Feb).

Mowatt-Larssen, R. (2010). Al Aqaeda weapons of mass destruction threat: Hype or reality? Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Mustacich, R. V. (2011). "Detection: The first line of defence." *Chemistry & Industry* 9: 23–25.

Nagel, J. (2005). "Wireless sensor systems and networks: Technologies, applications, implications and impacts." Retrieved September 12, 2011, from http://intranet.daiict.ac.in/ranjan /isn 2005/papers/APP/wireless.pdf

National Institute of Justice. (2000). "Guide for the selection of chemical agent and toxic industrial material detection equipment for emergency first responders." *Journal of Research of the National Institute of Standards and Technology* 105, no. 6: 943. Retrieved August 23, 2011, from http://search.proquest.com/docview/214772149?accountid=12702

Ortiz-Rivera, W., L. Pacheco-Londoño, & S. Hernández-Rivera. (2010). "Remote continuous wave and pulsed laser raman detection of chemical warfare agents, simulants and toxic industrial compounds." *Sensing and Imaging* 11, no. 3: 131–45. doi:10.1007/s11220-010-0055-9.

Pillai, Segaran. (2011). Testimony of Chief Medical and Science Advisor Segaran Pillai, Ph.D., Science and Technology Directorate Chemical and Biological Defense Division. "Taking measure of countermeasures (part 1)." *Targeted News Service*. Retrieved September 13, 2011, from http://search.proquest.com/docview/862246632?accountid=12702

Report recommends actions for public safety networks. (2007). *Telecommunications Reports* 73, no. 11: 17–18. Retrieved September 13, 2011, from http://search.proquest.com/docview/216947725?accountid=12702

Rudner, G.D. (2010). "Emerging trends in CBRN detection—Moving forward." *Domestic Preparedness Weekly Brief, DomPrep Journal* 6, no. 9.

Sha, K., W. Shi, & O. Watkins. (2006). "Using wireless sensor networks for fire rescue applications: Requirements and challenges." IEEE International Conference on Electro/Information Technology.

Shim, J. P., U. Varshney, S. Dekleva, & R. C. Nickerson. (2007). "Wireless telecommunications issues: Cell phone TV, wireless networks in disaster management, ubiquitous computing, and adoption of future wireless applications." *Communications of AIS* 2007, no. 20: 442–56. Retrieved July 7, 2011, from http://aisel.aisnet.org/cais/vol20/iss1/29/

Sohraby, K., D. Minoli, & T. Znati. (2007). *Wireless sensor networks: Technology, protocols, and applications*. Hoboken: NJ: John Wiley and Sons. Wiley Interscience.

Sullivan, A. (2006). "The good news is 9/11 never happened." Retrieved September 8, 2011 from http://search.proquest.com/docview/205161493?accountid=12702

Taylor, B., & S. Wright. (2004). "Britain foils chemical bomb plot." *Advertiser* (Sydney), April 8, 2004, 1A.

United States Army. (2000). "Guidelines for responding to and managing a chemical weapons of mass destruction terrorist event." Chemical weapons improved response program. U.S. Army soldier and biological chemical command. Retrieved September 18, 2011, from https://www.ecbc.army.mil/downloads/cwirp/ECBC_cwirp_playbook.pdf

United States Department of Homeland Security. (2007a). "National preparedness guidelines." Retrieved September 18, 2011, from http://www.fema.gov/pdf/emergency/nrf/National_Preparedness_Guidelines.pdf

United States Department of Homeland Security. (2007b). “Tactical interoperability communications scorecards, summary report and findings.” Retrieved August 24, 2011, from www.dhs.gov/xlibrary/assets/grants-scorecard-report-010207.pdf

United States Department of Homeland Security. (2008). “FEMA, National Preparedness Directorate. NIMS standards case study: Los Angeles regional interoperability.” Retrieved September 18, 2011, from http://www.fema.gov/pdf/emergency/nims/Los_Angeles_CAP_EDXL.pdf

United States Department of Homeland Security. (2009). “High priority technology needs: Science and technology.” Retrieved August 21, 2011, from http://www.dhs.gov/xlibrary/assets/High_Priority_Technology_Needs.pdf

United States Department of Transportation. (2008). “Emergency response guidebook.” Washington, D.C. Retrieved December 3, 2011, from http://www.phmsa.dot.gov/staticfiles/PHMSA/DownloadableFiles/Files/erg2008_eng.pdf

United States Government Accountability Office. (1999). “Observations on the threat of chemical and biological terrorism.” Washington, D.C.: GAO.

United States Government Accountability Office. (2004). “Weapons of mass destruction: Defense threat reduction agency addresses broad range of threats, but performance reporting can be improved.” Retrieved September 19, 2011, from http://www.gao.gov/new.items/d04330.pdf

United States Government Accountability Office. (2010). “Combating nuclear, biological, chemical, and radiological threats.” Retrieved September 18, 2011, from http://www.gao.gov/highrisk/agency/dhs/combating-nuclear-biological-chemical-critical-radiological-threats.php

Vijayaraghavan, R., K. Ganesan, & S. Raza. (2010). “Chemical warfare agents.” *Journal of Pharmacy and Bioallied Sciences* 2, no. 3: 166–78. doi:10.4103/0975-7406.68498.

Wang, K. S. (2002). “TV’s terrorism tax.” *Electronic Media* 21, no. 14: 26. Retrieved August 16, 2011, from http://libproxy.nps.edu/login?url=http://search.proquest.com.libproxy.nps.edu/docview/203815321?accountid=12702

White House. (2006). “The national security strategy of the United States of America.” Retrieved August 19, 2011, from http://www.whitehouse.gov/nsc/nss.html

White House. (2007). “Homeland security presidential directive/HSPD-18.” Retrieved September 19, 2011, from http://georgewbush-whitehouse.archives.gov/news/releases/2007/02/20070207-2.html

Williams, C. B., M. Dias, J. Fedorowicz, D. Jacobson, S. Vilvovsky, S. Sawyer, & M. Tyworth. (2009). “The formation of inter-organizational information sharing networks in public safety: Cartographic insights on rational choice and institutional explanations.” *Information Polity* 14, no. 1/2: 13–29. doi:10.3233/IP-2009-0170.

Wilson, J., V. Bhargava, A. Redfern, & P. Wright. (2007). “A wireless sensor network and incident command interface for urban firefighting.” Proceedings of the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous), August 6–10, 2007. doi:10.1109/MOBIQ.2007.4450980.

Winfield, G. (2004). “Nuclear spring.” *Military Technology* 28, no. 5: 55–65. Retrieved August 21, 2011, from http://search.proquest.com/docview/199063618?accountid=12702

World Health Organization. (1999). *Public health and chemical incidents*. United Kingdom: International Clearing House for Major Chemical Incidents.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California