


Spring 2013

An Epistemological Inquiry into the Incorporation of Emergency Management Concept in the Homeland Security with a Post-Disaster Security Centric Focus

Mehmet Secilmis
Old Dominion University

Follow this and additional works at: https://digitalcommons.odu.edu/emse_etds

 Part of the [Defense and Security Studies Commons](#), [Emergency and Disaster Management Commons](#), [Organizational Behavior and Theory Commons](#), and the [Systems Engineering Commons](#)

Recommended Citation

Secilmis, Mehmet. "An Epistemological Inquiry into the Incorporation of Emergency Management Concept in the Homeland Security with a Post-Disaster Security Centric Focus" (2013). Doctor of Philosophy (PhD), dissertation, Engineering Management, Old Dominion University, DOI: 10.25777/a15w-r069
https://digitalcommons.odu.edu/emse_etds/109

This Dissertation is brought to you for free and open access by the Engineering Management & Systems Engineering at ODU Digital Commons. It has been accepted for inclusion in Engineering Management & Systems Engineering Theses & Dissertations by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

**AN EPISTEMOLOGICAL INQUIRY INTO THE INCORPORATION OF
EMERGENCY MANAGEMENT CONCEPT IN THE HOMELAND SECURITY
WITH A POST-DISASTER SECURITY CENTRIC FOCUS**

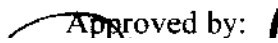
by

Mehmet Secilmis
B.S. August 1994, Military Academy, Turkey
M.A. July 2008, Army War College, Turkey

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY
ENGINEERING MANAGEMENT
OLD DOMINION UNIVERSITY
May 2013

Approved by: 



Adrian V. George (Director)

Reşit Unal (Member)

Sebastian Bawab (Member)

Ariel Pinto (Member)

ABSTRACT

AN EPISTEMOLOGICAL INQUIRY INTO THE INCORPORATION OF EMERGENCY MANAGEMENT CONCEPT IN THE HOMELAND SECURITY WITH A POST-DISASTER SECURITY CENTRIC FOCUS

Mehmet Secilmis
Old Dominion University, 2013
Director: Dr. Adrian V. Gheorghe

The historical roots of the Emergency Management concept in the U.S. date back to 19th century. As disasters occurred, policies relating to disaster response have been developed, and many statutory provisions, including several Federal Disaster Relief Acts, conceptually established the framework of Emergency Management. In 1979, with the foundation of the Federal Emergency Management Agency (FEMA), disaster relief efforts were finally institutionalized, and the federal government acknowledged that Emergency Management included mitigation, preparedness, response and recovery activities as abbreviated 'MPRR.'

However, after 2000, the U.S. experienced two milestone events - the September 11 terrorist attacks in 2001 and Hurricane Katrina in 2005. Following the foundation of the Department of Homeland Security (DHS) in 2002, the definitional context of Emergency Management and its phases/components, simply its essence, evolved and was incorporated into many official documents differently, creating contextual inconsistencies. Recent key official documents embody epistemological problems that have the potential to traumatize the coherence of the Homeland Security contextual framework as well as to impose challenges theoretically to the education and training of Homeland Security/Emergency Management stakeholders. Furthermore, the conceptual

design of the Emergency Support Functions (ESF) which have been defined within the context of the *National Response Framework* (NRF) displays similar problematic symptoms, and existing urban area Public Safety and Security planning processes have also not been supported by methodologies that are aligned with the post-disaster security requirements.

To that end, the conceptual framework of Emergency Management and its incorporation in the Homeland Security global architecture should be revised and redefined to enhance coherence and reliability. Coherence in the contextual structure directly links to the system's organizational structure and its viability functions. Also, holistic multi-dimensional system representations/abstractions, which would support appreciation of the system's complex context, should be incorporated in policy documents to be utilized to educate the relevant stakeholders (individuals, teams, etc.) during the training/orientation programs.

In addition, the NRF and its ESFs should be reviewed through a post-disaster security centric focus, since the post-disaster environment has unique characteristics that should be addressed by different approaches. In that sense, this dissertation develops a Post-Disaster Security Index (PDSI) Model that provides valuable insights for security agents and other Emergency Management and Homeland Security stakeholders.

Keywords: Emergency Management, Homeland Security, National Response Framework, Public Safety and Security, Post-Disaster Urban Security, Law Enforcement, Hurricane Katrina, Systems Thinking, Multi-Criteria Decision Making.

This dissertation is dedicated to my courageous classmate, Yilmaz Uyanik who sacrificed his life for the sake of our country.

ACKNOWLEDGMENTS

It was a great journey for me to work with many outstanding scholars at Old Dominion University, traveling through the vivid, inspiring and instructive corridors of academia again after a long time away. It was thrilling to distill the relevant knowledge sets that I needed to integrate in my dissertation, and make them ready with appropriate contributions while thinking that they would be helpful for other researches.

During this endeavor, I have found the great support of Dr. Adrian V. Gheorghe and Dr. Resit Unal. I am grateful for their invaluable direction and guidance, which empowered me to work harder. I would also like to thank Dr. Sebastian Bawab and Dr. Ariel Pinto, who provided great insights at the beginning of my research that catalyzed the dissertation process efficiently.

Although I regret not receiving any official response and support from U.S. Department of Homeland Security to my requests through emails during the research, I hope the discussions and analysis results in my dissertation make valuable contributions to the U.S. Homeland Security enterprise in the context of enhancing its resiliency and preparedness.

However, notwithstanding the dissertation topic refers to U.S. Emergency Management and relevant frameworks, the conclusions and recommendations of this research provide some generalizable insights for the people who need to deal with complex systems and security in any organization around the world.

Finally, I would like to thank to my dearest family: my wife - Ilknur; my son - Tarik; and my daughter - Vildan; the great trio who have made the most significant contribution to this endeavor and let this challenging process be completed. I will never forget their devoted support, and promise that I will try to compensate for what I have missed.

LIST OF ACRONYMS AND ABBREVIATIONS

BCI	Basic Criticality Index
BCV	Basic Criticality Value
CIKR	Critical Infrastructure and Key Resources
DHS	Department of Homeland Security
ECIP	Enhanced Critical Infrastructure Protection
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
HSPD	Homeland Security Presidential Directive
ICP	Incident Command Post
ISR	Intelligence, Surveillance and Reconnaissance
JFO	Joint Field Office
MCDM	Multi-Criteria Decision Making
MDMP	Military Decision Making Process
NIPP	National Infrastructure Protection Plan
NIMS	National Incident Management System
NRF	National Response Framework
QHSR	Quadrennial Homeland Security Review Report
PDSI	Post-Disaster Security Index
PDSFI	Post-Disaster Security Fuzzy Index
PKEMRA	Post Katrina Emergency Management Reform Act
PPD	Presidential Policy Directive

TABLE OF CONTENTS

	Page
LIST OF TABLES	xii
LIST OF FIGURES	xv
 Chapter	
1. INTRODUCTION	1
1.1 BACKGROUND	1
1.2 PROBLEM DOMAIN	4
1.3 PURPOSE AND ANTICIPATED SIGNIFICANCE OF THE STUDY	5
1.4 RESEARCH METHODOLOGY	8
1.5 HYPOTHESES	9
1.6 LIMITATIONS AND DELIMITATIONS OF THE STUDY	10
1.6.1 LIMITATIONS	10
1.6.2 DELIMITATIONS	10
 2. LITERATURE REVIEW	12
2.1 TODAY'S SECURITY ENVIRONMENT	13
2.1.1 URBAN ENVIRONMENT	14
2.1.2 RISK AND VULNERABILITY	16
2.1.3 THREAT SPECTRUM	18
2.2 HOMELAND SECURITY AND KEY MANDATES	19
2.2.1 HOMELAND SECURITY	19
2.2.2 NATIONAL INFRASTRUCTURE PROTECTION PLAN (NIPP)	21
2.2.3 NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS)	24
2.2.4 NATIONAL RESPONSE FRAMEWORK (NRF)	26
2.2.5 PUBLIC SAFETY AND SECURITY (ESF-13)	29
2.3 HURRICANE KATRINA	31
2.3.1 CLIMATOLOGICAL SUMMARY	32
2.3.2 FORENSIC CONTINUUM OF THE CRISIS	33
2.4 SYSTEMS THINKING AND COMPLEXITY	38
2.4.1 CHALLENGES OF COMPLEX SYSTEMS	38
2.4.2 SYSTEMS PHILOSOPHY AND THINKING	40
2.5 EPISTEMOLOGY AND PHILOSOPHICAL PERSPECTIVE OF MODELING	44

2.5.1	EPISTEMOLOGY	44
2.5.2	SYSTEM REPRESENTATION AND MODELING	48
2.6	MULTI-CRITERIA DECISION MAKING (MCDM)	51
2.6.1	OVERVIEW OF MULTI-CRITERIA DECISION MAKING (MCDM)	52
2.6.2	FUZZY SETS THEORY	54
2.6.3	RECOGNITION HEURISTIC AND ELIMINATION BY ASPECTS	56
3.	ANALYSIS OF THE INCORPORATION OF EMERGENCY MANAGEMENT, AND PUBLIC SAFETY AND SECURITY	59
3.1	INTRODUCTION	59
3.2	ANALYSIS METHODOLOGY	60
3.3	SYSTEM OF INTEREST IDENTIFICATION (PHASE 1)	62
3.4	RELEVANT ENVIRONMENT SPECIFICATION (PHASE 2)	63
3.5	SPECIFICATION OF PROBLEMS (PHASE 3)	66
3.6	CONTEXTUAL IDENTIFICATION (PHASE 4)	67
3.6.1	EMERGENCY MANAGEMENT WITHIN THE HOMELAND SECURITY CONTEXTUAL STRUCTURE	68
3.6.2	PUBLIC SAFETY AND SECURITY	77
3.7	SYNTHESIS AND ASSESSMENT (PHASE 5)	82
3.7.1	INCORPORATION OF EMERGENCY MANAGEMENT CONCEPT	82
3.7.2	PUBLIC SAFETY AND SECURITY	97
3.8	CONCLUSIONS (PHASE 6)	100
4.	POST-DISASTER SECURITY INDEX (PDSI) MODEL	105
4.1	INTRODUCTION	105
4.2	REQUIREMENT FOR BETTER PLANNING AND COORDINATION	106
4.3	EXISTING SECURITY PLANNING PRACTICES	111
4.4	CONCEPTUAL BACKGROUND OF THE PDSI MODEL	116
4.5	SIGNIFICANCE OF THE PDSI MODEL	117
4.6	PDSI MODEL ALGORITHM	119
4.6.1	INTRODUCTION	119
4.6.2	IDENTIFY BOUNDARIES	121
4.6.3	IDENTIFY CRITICAL ASSETS	123
4.6.4	MEASURE BASIC CRITICALITY INDEX (BCI)	125
4.6.5	MEASURE POST-DISASTER SECURITY FUZZY INDEX (PDSFI)	127

4.6.6	MEASURE POST-DISASTER SECURITY INDEX (PDSI).....	134
4.7	SAMPLE MEASUREMENT	134
4.7.1	SCENARIO.....	134
4.7.2	MEASUREMENT RESULTS.....	135
4.8	RELIABILITY AND VALIDITY OF THE CONSTRUCTS.....	136
4.9	CONCLUSION.....	139
5.	CONCLUSIONS AND RECOMMENDATIONS	142
5.1	CONCLUSIONS.....	143
5.1.1	HOMELAND SECURITY CONTEXTUAL STRUCTURE.....	143
5.1.2	POST-DISASTER SECURITY.....	146
5.2	RECOMMENDATIONS	147
	REFERENCES	157
	APPENDICES	175
A.	BACKGROUND INFORMATION FOR THE SPECIFICATION OF ANALYSIS PROBLEMS.....	175
B.	SECURITY OPERATIONS	180
C.	URBAN AREA DEFENSE.....	188
D.	MEASUREMENT OF BASIC CRITICALITY INDEX (BCI)	192
E.	MEASUREMENT OF INPUT VARIABLES.....	198
F.	SAMPLE MEASUREMENT	214
G.	PDSI MODEL FACE VALIDITY QUESTIONNAIRE	222
H.	BASIC REALITY FACE-OFF DECISION TREE	223
I.	A ROADMAP FOR COMPLETE COMPLEX ORGANIZATIONAL SYSTEM ANALYSIS.....	227
J.	RESPONSIBLE CONDUCT OF RESEARCH FOR ENGINEERS CURRICULUM COMPLETION REPORT.....	230
	VITA.....	231

LIST OF TABLES

Table	Page
1. Sector-Specific Agencies and CIKR Sectors.....	23
2. Emergency Support Functions.....	28
3. Definitions of Complex Systems and System of Systems.....	40
4. Definitions of Philosophical Paradigms.....	47
5. Focus of the Analysis.....	62
6. Emergency Management Core and Day-to-Day Program Functions	76
7. A Brief Summary of the Analysis Problem	83
8. Evolutional Adaption of the Emergency Management Phases/Components	85
9. Potential Types of Critical Assets.....	124
10. Basic Criticality Index (BCI) Equations.....	126
11. Ambient Criteria of Merit and Possible System States.....	127
12. Post-Disaster Security Fuzzy Index (PDSFI) Matrix.....	129
13. Fuzzy Matrix Variables.....	132
14. Equations for the Measurement of Fuzzy Matrix Variables.....	132
15. PDSI of the Critical Assets	135
16. Performance Sensitivity	135
17. Security Operations.....	182
18. Security Operations Techniques/Missions.....	184
19. Patrolling in the Urban Areas	185
20. Approximate Defensive Frontages and Depths	190
21. Basic Criticality Index (BCI) Assessment Matrix	192
22. Scaling Constant Matrix	193

23.	Service Relativity Weight Assessment Matrix	194
24.	Employment Weight Assessment Matrix	194
25.	Occupancy Weight Assessment Matrix	195
26.	Size Weight Assessment Matrix	196
27.	Investment Weight Assessment Matrix	196
28.	Student Capacity Weight Assessment Matrix.....	197
29.	Seating Capacity Weight Assessment Matrix.....	197
30.	Scaling Constants per each Criterion.....	198
31.	Physical Security Vulnerability Index	198
32.	Perimeter Security Index.....	199
33.	Building Envelope Wall Type Index	199
34.	Building Envelope Fenestration Index.....	200
35.	Inhabitant/Visitor Number Vulnerability Index.....	200
36.	Size/Area Vulnerability Index	201
37.	Traffic Access/Mobility Vulnerability Index.....	202
38.	Periphery Road Width Index	202
39.	Adjacent Primary Roads Proximity Index	203
40.	Bridge Dependency Index.....	203
41.	Transportation Terminals Proximity Index	203
42.	Vulnerability Index Modifier for Offences against Property.....	204
43.	Vulnerability Index Modifier for Offences against Persons	205
44.	Vulnerability Index Modifier for Terrorist Attacks/Warfare Threats.....	206
45.	Generalizability Grades of Membership for Physical Security	206

46.	Seismicity Vulnerability Index	207
47.	Hurricane Vulnerability Index	208
48.	Flood Vulnerability Index	208
49.	Generalizability Grades of Membership for Number of Inhabitants/Visitors	209
50.	Generalizability Grades of Membership for Size/Area	210
51.	Generalizability Grades of Membership for Traffic Access/Mobility.....	211
52.	Road Length Index	211
53.	Transportation Lines Index	211
54.	Bridges Index	212
55.	Generalizability Grades of Membership for Offences against Property.....	212
56.	Generalizability Grades of Membership for Offences against Persons.....	213
57.	Generalizability Grades of Membership for Terrorist Attacks/Warfare Threats.....	213
58.	Scaling Constant Matrix	215
59.	Basic Criticality Values	216
60.	Scaling Constants per each Criterion.....	217
61.	Vulnerability Indexes.....	217
62.	Vulnerability Index Modifiers	218
63.	Generalizability Grades of Membership per each Criterion	218
64.	Generalizability Grades of Membership per each Possible System State	219
65.	PDSFI Matrix of BSC.....	219
66.	PDSFI Matrix of DHC.....	220
67.	PDSFI Matrix of CDD.....	220
68.	PDSI of the Critical Assets	221

LIST OF FIGURES

Figure	Page
1. Origination of the Emergency Management Concept	1
2. DHS Capstone Documents	3
3. Major Components of the Dissertation	6
4. Research Methodology	9
5. Conceptual Design of the Literature Review	12
6. Urban Area Systems	15
7. Vulnerability Mapping	18
8. Sources of Threat	19
9. Incident Command System	25
10. Area Command Structure	26
11. Joint Field Office	29
12. Hurricane Katrina: Cone of the Uncertainty	33
13. Systems (Re)Visioning Perspective	43
14. Relationships between Philosophical Paradigms	46
15. Contextual Analysis Methodology	61
16. Elements of the Security Sector	65
17. Relationship between Crisis Management and Consequence Management	72
18. Public Safety and Security Metaphors	80
19. Key Elements of Homeland Security Evolution Process	88
20. Required Military Capability in Typical and Catastrophic Incidents	108
21. National Guard Response to Hurricane Katrina	109
22. NIPP Risk Management Framework	113

23.	Components of the Post-Disaster Security Index Model.....	120
24.	Unique Characteristics of Post-Disaster Urban Environment	120
25.	Identification of Boundaries	122
26.	Identification and Enumeration of Critical Assets.....	123
27.	Three Main Components of PDSFI Matrix	127
28.	Visual Representation of the Triangulation Process.....	138
29.	Relative Performance Sensitivity of Normalized Indexes.....	141
30.	Synopsis of the Dissertation.....	142
31.	Optimal Design of the System Context	149
32.	Facilitation of Functional Areas.....	150
33.	Multi-Dimensional Holistic System Representation	151
34.	Post-Disaster Security Environment Characteristics and Principal Drivers for Potential Planning Solutions	153
35.	Depiction of PDSIs in Color Code.....	155
36.	Key Joint Security Functions and Nodes.....	181
37.	Steps of Intelligence Preparation of the Battlefield (IPB)	191
38.	Seismicity Regions of the Conterminous United States	207
39.	Boundaries of Alfa Subsector	214
40.	Critical Assets Identified in Alfa Subsector.....	215
41.	Basic Reality Face-off Decision Tree	224

CHAPTER 1

INTRODUCTION

1.1 Background

Emergent threats, like natural and man-made disasters (including acts of terrorism), have the potential to bring uncertainty and complexity to the security of urban environments, while the requirement for resiliency and emergency preparedness is increasing in the context of Homeland Security. As Little (2004) has discussed “we find ourselves in a time where former contexts of threat, vulnerability, and target have all changed and continue to do so” (p. 57).

Against this threat spectrum, which is getting more challenging every day, Emergency Management has been the focal point of local and federal authorities for framing disaster response activities in the U.S. Since the 1800s, exhaustive efforts have been rendered to cope with the hard times of post-disaster periods while many disaster policies and statutory provisions have been promulgated to coordinate the decentralized initiatives scattered around the country. During the time represented in Figure 1, the disaster response framework at federal level was institutionalized with the foundation of FEMA in 1979, and the federal government acknowledged the four major components - mitigation, preparedness, response and recovery (MPRR) - of Emergency Management.

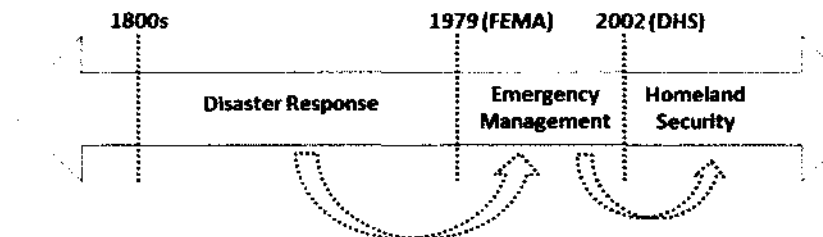


Figure 1 Origination of the Emergency Management Concept

Since 1979, studies to enhance preparedness and resiliency against different types of disasters have increased. In the last decade, after the terrorist acts of 9/11, parallel with the increase in the vulnerability of urban areas, myriad efforts, including public, state or private initiatives (policy/strategy development, legislation, academic research and activities, administrative regulations, exercises, etc.) have been put in place to enhance the national preparedness. These studies which are mostly under the oversight of the Homeland Security enterprise have incorporated the essence of the Emergency Management concept differently, and it is assumed that all those efforts performed in some partially decentralized networked groups have ended with some epistemological inconsistencies regarding the Homeland Security contextual domain, which comprises diverse contextual, structural and functional complex systems and sub-systems. Due to overwhelming complexity and epistemological problems, the outstanding initiatives in different scales and scopes which aimed to sustain a high level of resiliency against all types of threats, have consequently created some more contextual inconsistency. However, the initiatives were supposed to be controlled, coordinated and unified with a common terminology as it required by the recent *Presidential Policy Directive of National Preparedness* (2011).

The official capstone documents that identify the boundaries of the Homeland Security enterprise are depicted in Figure 2. The concept of Emergency Management, which can be traced back to the 19th century with the beginning of disaster response activities, was incorporated in these documents after 2000, following the establishment of the DHS, and Emergency Management continued to evolve during this time in line with the development of Homeland Security context.

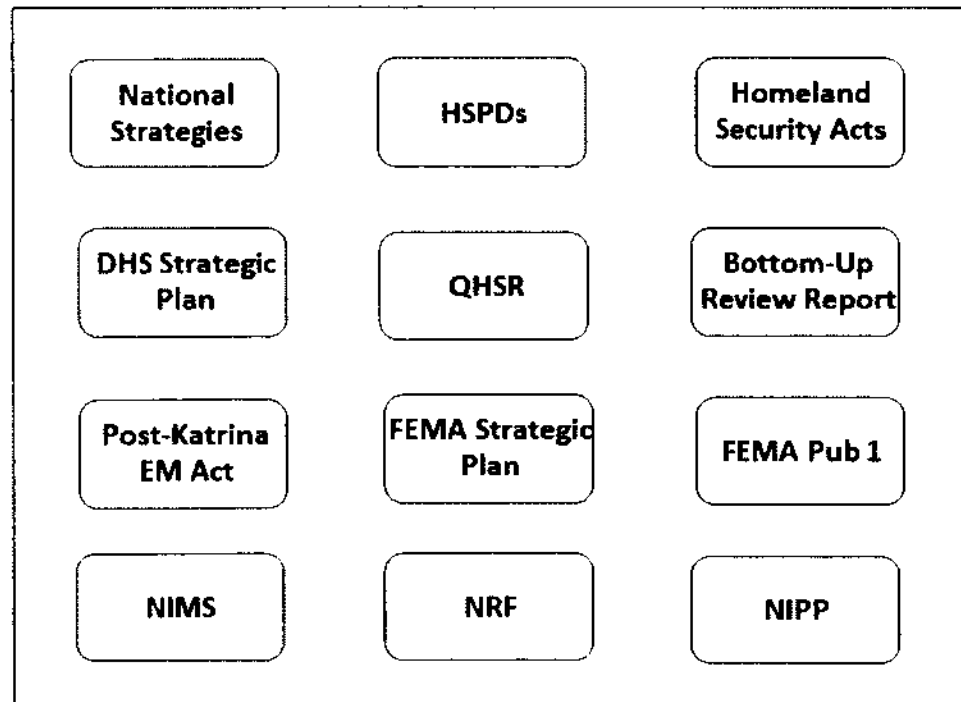


Figure 2 DHS Capstone Documents

To some extent, the National Incident Management System (NIMS) and NRF, which are the core mandates of the Homeland Security response/recovery architecture, have adapted the essence of Emergency Management. NIMS “works hand in hand with NRF and provides the template for the management of incidents, while the NRF provides the structure and mechanisms for national-level policy for incident management” (National Incident Management System, 2008, p. 1). NRF “specifies incident management roles and responsibilities, including emergency support functions designed to expedite the flow of resources and program support to the incident area” (National Infrastructure Protection Plan, 2009, p. 78).

However, when all the documents illustrated in Figure 2 are reviewed from a holistic perspective (as they are specified in the next chapters), serious contextual

inconsistencies are revealed regarding the theoretical mission areas, functions and definitions of Emergency Management, Homeland Security, and their major components.

In a similar vein, two of the fifteen support functions within the NRF, Emergency Management Support Function (ESF-5) and Public Safety and Security Support Function (ESF-13) have links to the problem domain identified in this dissertation. Their design in the existing framework requires further analysis to minimize the collateral deficiencies.

1.2 Problem Domain

In the U.S., before DHS, disaster response activities were coordinated within the context of Emergency Management. During the period theoretically starting from September 11, DHS has been the single authority for the coordination of all response missions. Following its establishment in 2002, DHS has overseen the development and evolution of Emergency Management in line with the development of the Homeland Security contextual framework. However, the incorporation of the definitional context of Emergency Management and its phases/components within the official documents (contextual structure) of Homeland Security indicates serious epistemological problems.

In addition, the official documents addressing both the Homeland Security enterprise and Emergency Management (which should be a process or function within Homeland Security) lack of figurative top-down holistic, multi-dimensional system representations/abstractions. These should have depicted the contextual structure (of all levels) of the system holistically for the situational awareness and training of individuals/leaders and other system stakeholders.

The aforementioned epistemological problems have also negatively affected the conceptual design of the ESFs defined within the context of NRF. Although Emergency Management Support Function (ESF-5) should be an overarching function or process to lead, coordinate and synchronize the other functions that use the Public Safety and Security Support Function (ESF-13) as a base platform, all the support functions are depicted as independent. In addition, the interaction and interdependency among them have not been delineated clearly throughout the texts.

Furthermore, regarding Public Safety and Security of an urban environment in a post-disaster state, new criticality and vulnerability assessment tools/models should be developed to better support the security planning process, since security and public order in a post-disaster urban environment play a significant role for the execution of other follow-up response and recovery missions as it was evidenced during Hurricane Katrina. The lack of law enforcement and public security during the first week after Hurricane Katrina seriously hurt the execution of other Emergency Management missions in coherence, completely halting some of the response efforts in some places.

1.3 Purpose and Anticipated Significance of the Dissertation

The dissertation includes two separate major components, which theoretically stay in the contextual framework of U.S. Homeland Security, and have an inextricable link to each other, as depicted in Figure 3. The focal discussions of these components follow:

- An epistemological inquiry (questioning the contextual consistency) of the incorporation of Emergency Management concept within the Homeland Security contextual structure.

- Discussion that highlights the requirement for post-disaster security centric planning approach within the NRF.

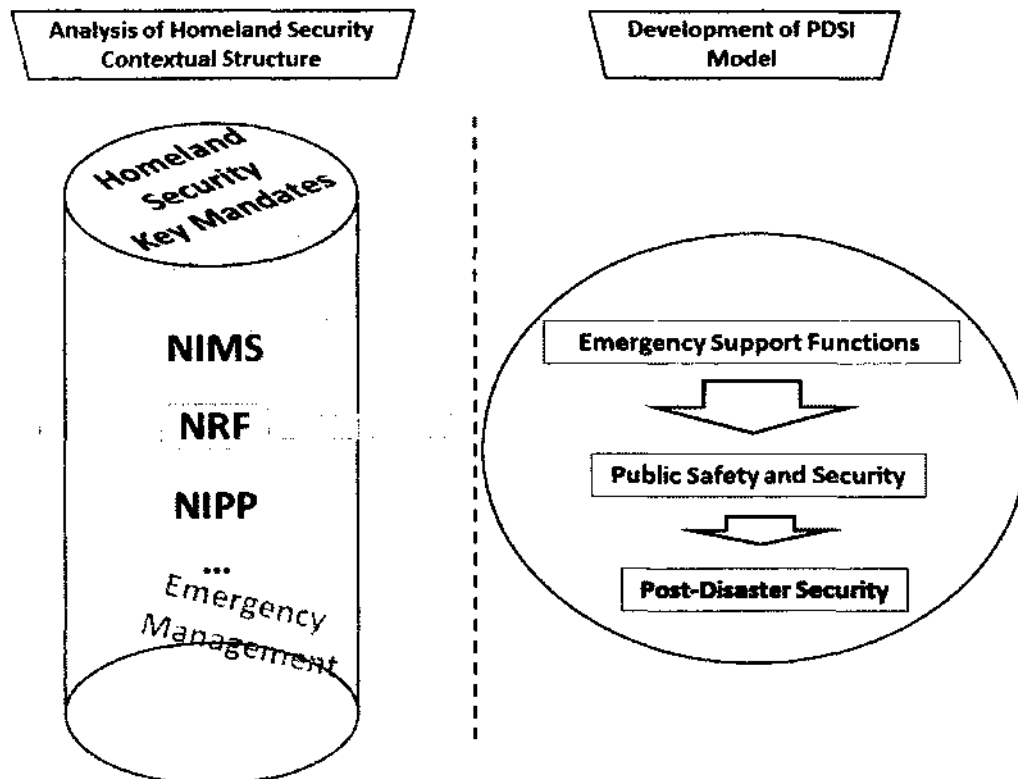


Figure 3 Major Components of the Dissertation

In line with these topics, the purpose of the dissertation is to contribute to existing literature providing some factual inferences (articulated as Conclusions and Recommendations in Chapter 5) by achieving the following goals;

- Analyze the U.S. Homeland Security contextual structure underlining the significance of:
 - Contextual coherence in a complex system,
 - Utilization of common terms, taxonomies and figurative top-down holistic multi-dimensional system representations/abstractions,

- Public Safety and Security within the National Response Framework.
- Develop a vulnerability assessment model which can be utilized to address tactical level post-disaster urban area security requirements, promoting the post-disaster security centric planning perspective as well as providing generalizable indices for the high level (operational or strategic) security planning purposes.

Pursuant to significance of the dissertation, Chapter 3 clarifies and underlines the potential implications of contextual inconsistency upon the organizational and functional structures of the systems, and upon Public Safety and Security. This chapter includes a contextual analysis supported by an extensive literature review through a unique methodology culminating with critical conclusions specified in Chapter 5.

Chapter 4 introduces a unique prescriptive vulnerability assessment model - Post-Disaster Security Index (PDSI) Model, which would support post-disaster security planning of urban areas. The concept design of the PDSI Model is a combination of the epistemological perspective of modeling, Multi-Criteria Decision Making (MCDM), and relevant aspects of the military literature, including Military Decision Making Process (MDMP). The variables used in the model have been developed to specifically address the post-disaster security requirements.

The vulnerability index (PDSI), to be obtained through the use of the PDSI Model, not only provides a prioritization index for the criticality and vulnerability assessment but also gives valuable insights for post-disaster force tailoring, unit positioning and the determination of the possible security operations techniques to be

implemented in a jurisdiction. If the PDSI Model is implemented in a broad area of responsibility at state or federal level by the lead of a central authority, it would also be possible to derive operational and strategic level inferences of the higher level decision making processes, as specified in Chapter 5.

Furthermore, this dissertation explores today's security environment and the philosophical paradigms from the perspective of modeling, and promotes the systems thinking and top-down multi-dimensional holistic system representation.

1.4 Research Methodology

While the research methodology principally relies on literature review, the phases adopted in the continuum of the research - which are facilitated in a non-linear approach - have been depicted in Figure 4. Generally mixed methods have been utilized during the research. The dissertation content, which has been addressed by both quantitative and qualitative research characteristics, includes two major components. One of the components (Chapter 3) analyzes the problem domain with a descriptive methodology, while the other (Chapter 4) focuses on the PDSI Model development with a prescriptive approach. Both deductive logic and inductive reasoning methods have been applied during the analysis.

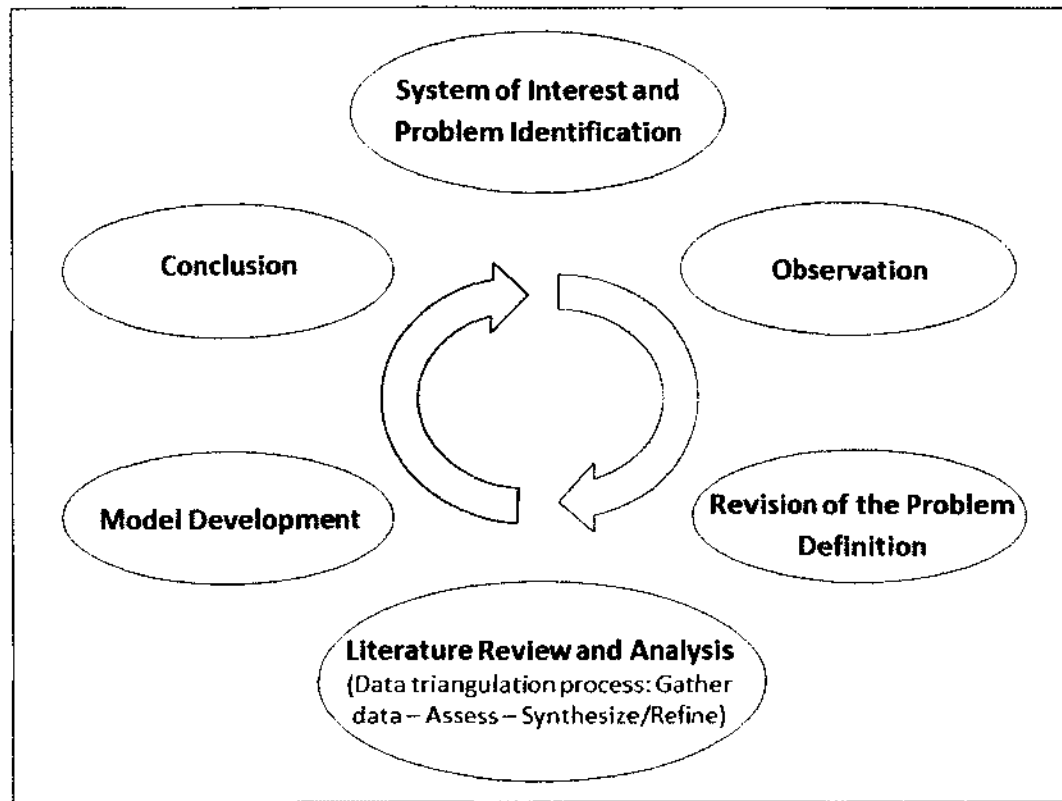


Figure 4 Research Methodology

1.5 Hypotheses

A research hypothesis is a proposed statement, which includes predictions or explanations that should be proven through various methods. In that sense, the following hypotheses would be proven through the analysis and model development to achieve the dissertation goals outlined in Chapter 1.3;

- The complex system's contextual structure (which utilizes common terms and taxonomies, as well as content knowledge that epistemologically complies with the historical development of the conceptual framework) requires coherence to optimize the system's organizational structure and let its viability functions run properly.

- Figurative top-down multi-dimensional system representations or abstractions that delineate the system architecture holistically at all levels play a key role in maintaining the situational awareness of relevant stakeholders.
- Redefining the ESF-5 as overarching and the ESF-13 in a backdrop role (since maintaining public safety and security, including law enforcement, seriously affects the other response/recovery missions to be executed in harmony) would enhance the resiliency of the NRF.

1.6 Limitations and Delimitations of the Study

1.6.1 Limitations

- The fuzzy matrix conceptual design in the PDSI Model provides a unique approach for vulnerability assessments of key assets; however, the measurement matrixes and variables are subject to change/modification in the future based on the feedback to be provided through extensive empirical studies.
- In the dissertation, post-disaster urban environment security requirements have been exemplified only with the Hurricane Katrina case.

1.6.2 Delimitations

- The research analysis scope is limited to the U.S. Emergency Management context.

- Contextual analysis primarily addresses the incorporation of the Emergency Management definition and its phases/components in the official capstone DHS references. Full context analysis is beyond the scope of this dissertation.
- Chapter 4 delineates the conceptual design and step-wise algorithm of the PDSI Model. However, a software program supported by Geographic Information Systems (GIS) should be developed in future for the practical use of the model.

CHAPTER 2

LITERATURE REVIEW

As discussed in Chapter 1, major components of the dissertation focus on the analysis of the Homeland Security contextual structure (theoretical content created by referential documents) regarding the incorporation of the Emergency Management concept - its definition, phases/components, etc., and the development of a vulnerability assessment model to support Public Safety and Security planning with a post-disaster security centric focus.

The literature review is organized under six main titles. The conceptual design of the literature review has been depicted in Figure 5.

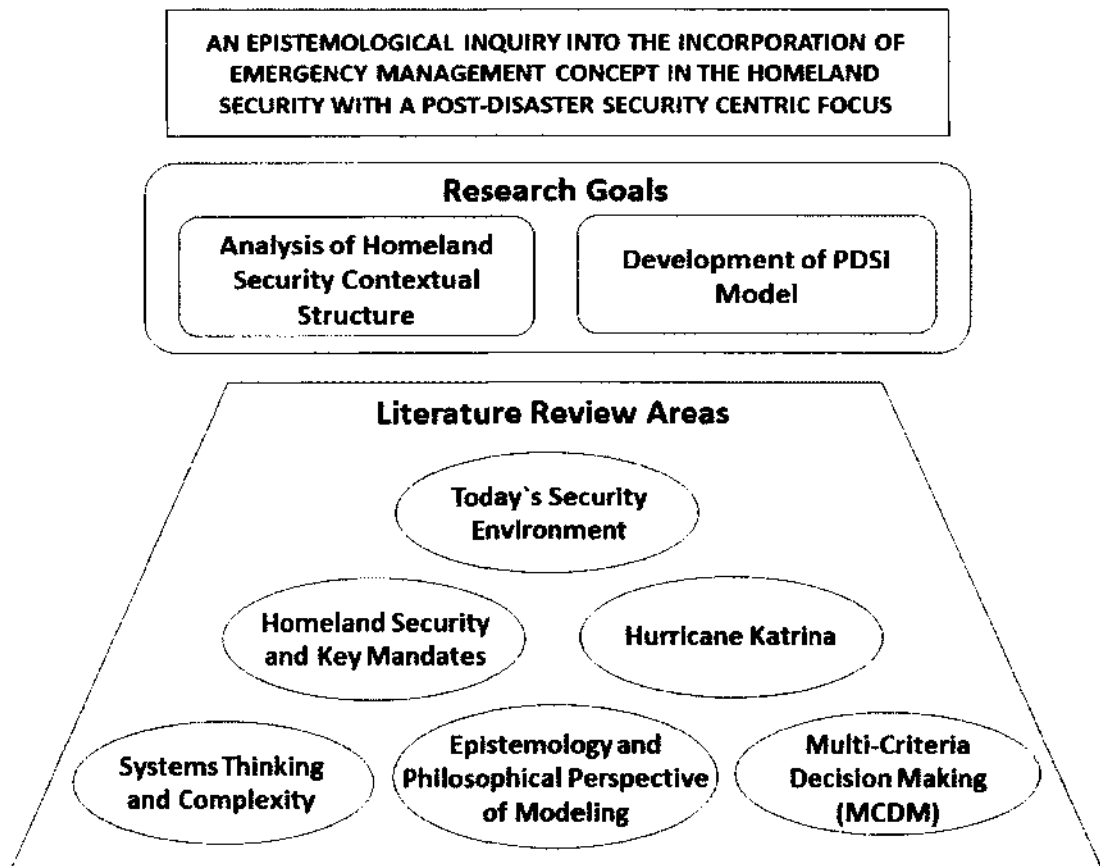


Figure 5 Conceptual Design of the Literature Review

After the terrorist attacks of 9/11, following the foundation of DHS, all internal security, including Emergency Management activities, came to be overseen by DHS. During this time, DHS evolved into a complex system with numerous entities and a broad context, mainly comprised of the key mandates promulgated by the government. To explore the aforementioned discussions, Chapter 2.1 and Chapter 2.2 review 'Today's Security Environment' and 'Homeland Security and Key Mandates', respectively.

This research adopts a post-disaster security centric focus for both the analysis of the Homeland Security contextual structure and PDSI Model development with the aim of promoting the significance of the Public Safety and Security function (including security, public order, law enforcement, etc.) within the NRF. Since the Hurricane Katrina case embodies many lessons learned regarding post-disaster security and law enforcement failures, its forensic history is included in Chapter 2.3 to materialize the assumptions.

Since the contextual analysis is addressing a complex system with numerous functions and entities, Chapter 2.4 reviews 'Systems Thinking and Complexity' discussions to highlight the scholarly aspects of existing knowledge.

Finally, to support the conceptual framework of the PDSI Model delineated in Chapter 4, 'Epistemology and Philosophical Perspective of Modeling' and 'Multi-Criteria Decision Making (MCDM)' topics have been explored in Chapter 2.5 and Chapter 2.6.

2.1 Today's Security Environment

Human beings have been exposed to a vast number of natural and man-made disasters or threats since the creation of the earth in the universe. The foremost types of

disasters humanity has suffered include: hurricanes, earthquakes, floods, tsunamis, wildfires, radiological or hazardous material releases, acts of terrorism, and wars.

However, “the threats to the people and the people’s interests have shifted dramatically in the last 20 years” (National Security Strategy, 2010, p. 17), and now “we find ourselves in a time where former contexts of threat, vulnerability, and target have all changed and continue to do so” (Little, 2004, p. 57). Today, threats resulting from the catastrophic impacts of natural and man-made disasters, especially from asymmetric terrorist acts, continue to impose great challenges to people who live in urban areas.

2.1.1 Urban Environment

Manning (2012) discusses “for the first time in history, the majority of the human race lives in cities” (p.12). “The world is undergoing a massive urbanization” (Urban Operations, 2006, p.1-1). “An overall trend of migration from rural to urban areas is occurring throughout the globe” which is creating “massive urban areas that hold the centers of population, government, and economics in their respective regions” (Urban operations, 2006, p.1-1).

Hidek (2010) contends the revolution of security affairs today makes the analysis of urban security policy a complex endeavor, stating that “it is a story of a machine with countless moving parts, only some of which operate in public view” (p. 43). As Kiefer (2001) has discussed, it is extremely challenging to strengthen the potential targets in urban areas, although we have more capabilities in terms of effective physical security and technological countermeasures today.

Desch (2001) notes the problems that urbanization poses for political leaders which include “untrammeled growth, overcrowding, pressures on urban services, the growth of slums and other poor areas, transportation bottle-necks, atomization of society, unemployment, racial and/or ethnic conflict, pollution, loss of agricultural areas, and increased adverse consequences of natural or man-made disasters” (p. 5).

The urban environment “is made up of adaptive systems with a wide range of structures, processes, and functions that have evolved to sustain concentrated human societies in confined space” (Joint Urban Operations, 2009, p. II-2). “Each system has a critical role in the smooth functioning of the urban area; whether they are simple or complex, all systems fit into six broad categories” as it is depicted in Figure 6 (Urban operations, 2006, p. 2-19).

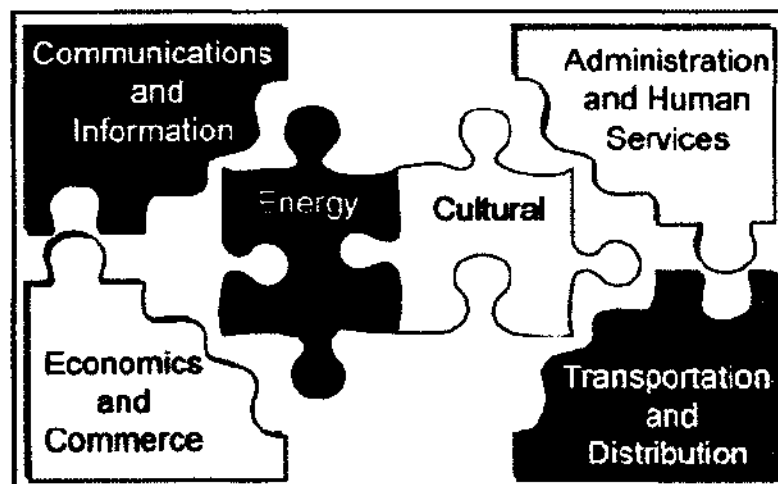


Figure 6 Urban Area Systems (Urban Operations, 2006, p. 2-19)

Urban areas “present an extraordinary blend of horizontal, vertical, interior, exterior, and subterranean forms superimposed on the natural relief, drainage, and vegetation” (Urban operations, 2006. p. 2-2). “They present the most complex

environment for military operations. This complexity is derived from numerous factors such as location, history, economic development, climate, available building materials, the natural terrain, the cultures of their inhabitants, and many other factors” (Joint Urban Operations, 2009, p. VII).

Regarding the development of a successful strategy for urban security, Little (2004) discusses that the interactions between all involved stakeholders should be understood and enabled. He further contends that “robust and effective security will require that dialogues be initiated and sustained between and among the various stakeholders using terms of reference that all can relate to and act upon” (p. 56).

2.1.2 Risk and Vulnerability

Risk is the “potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences” (National Infrastructure Protection Plan, 2009, p. 27). It is the “expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss” (National Infrastructure Protection Plan, 2006, p.104).

In the context of Homeland Security, the National Infrastructure Protection Plan (NIPP) Framework assesses the risk as a function of consequence, vulnerability, and threat (National Infrastructure Protection Plan, 2006). In a similar way, Bridging the Gap (2010) defines the risk assessment as a comprehensive process:

Risk assessment is the comprehensive process for the identification and characterization of threat, consequences, and vulnerabilities. While each element is important for capabilities based planning and national

preparedness, determinations of vulnerability are important because they include an assessment of exposure, sensitivity, and resilience. (p.111)

Johansson (2010) defines the vulnerability as “the consequences that arise when a system is exposed to a strain of a given type and magnitude” (p.19). Vulnerability is a “weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or disrupted by a natural hazard or technological failure” (National Infrastructure Protection Plan, 2006, p.105). It is “a state inherent in the manifestation of physical, organizational, and cultural properties of a system that can result in damage if attacked by an adversary or subjected to a natural disaster or some other form of threat” (Bridging the Gap, 2010, p.112).

Vulnerabilities are “gaps in the assets’ protection; they are identified by considering the tactics associated with the threat and the levels of protection that are associated with those tactics” (Physical Security, 2001, p. 2-4). National Infrastructure Protection Plan (2006) provides a further definition for vulnerabilities:

Vulnerabilities are the characteristics of an asset, system, or network’s design, location, security posture, process, or operation that render it susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks, or other malicious acts. They identify areas of weakness that could result in consequences of concern; taking into account intrinsic structural weaknesses, protective measures, resiliency, and redundancies. (p.38)

Vulnerability assessment is a “process to identify physical, organizational, or cultural characteristics or procedures that render populations, assets, areas, or special events susceptible to a specific hazard or set of hazards” (Bridging the Gap, 2010, p. 112). Vulnerability articulates the relationship between the set of initiating events and the set of outcomes as shown in Figure 7.

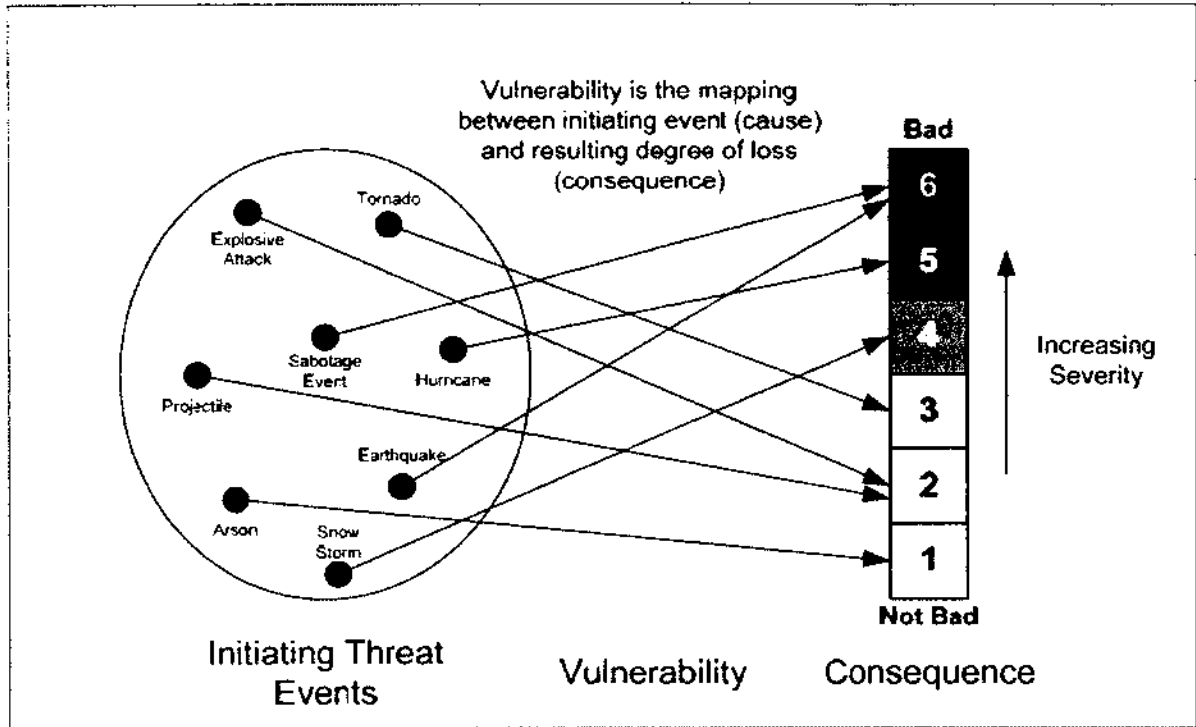


Figure 7 Vulnerability Mapping (McGill, 2008, p. 9)

2.1.3 Threat Spectrum

The National Security Strategy (2010) underlines the change in the threat spectrum, which has shifted dramatically in the last 20 years, as “the post-9/11 era has yielded to a low level, but persistent terrorist threat, more focused to date on U.S. interests abroad than on the homeland, which is likely to persist to 2030” (Manning, 2012, p.11).

Threat is an “indication of possible violence, harm, or danger dividing it into three different types: Natural, Technological and Human-caused threats” (Fundamentals of Emergency Management, 2011, p.2-13). The threats are “unpredictable and the full range of threats probably unknowable” (Little, 2004, p.57), and “geopolitical uncertainty will

be a feature of the coming two decades” (Manning, 2012, p.11). Figure 8 depicts a visual representation of different sources of threat.

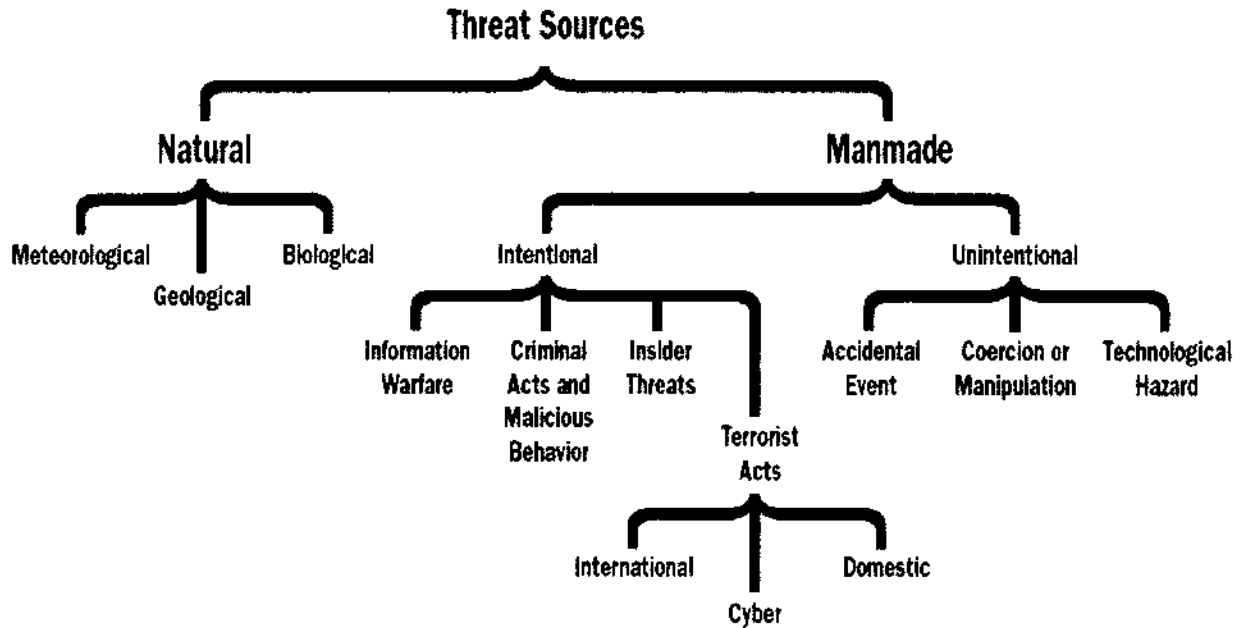


Figure 8 Sources of Threat (Emergency Services Sector, 2010, p. 43)

2.2 Homeland Security and Key Mandates

2.2.1 Homeland Security

Homeland Security “describes the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border control, and immigration” (Quadrennial Report, 2010, p. viii). Homeland Security is a “complex challenge that demands significant investment; collaboration among local, state, and federal governments; and integration with the private sector” (A Governor’s Guide, 2002, p.6). Homeland Security is a “concerted national effort to prevent terrorist attacks within the United States, reduce

America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur" (National Strategy for Homeland Security, 2007, p.3).

After the September 11 terrorist attacks, the federal government passed the Homeland Security Act of 2002, "which called for the development of a consistent infrastructure protection methodology that would be applied to guide the federal government's efforts and established Department of Homeland Security (DHS)" (Hidek, 2010, p. 109).

The DHS "has been developed to pull together many agencies that already existed in the government and to coordinate with local and state authorities for the protection of the nation" (Oscar, 2006, p. 12); and in January 2003, FEMA was subsumed under the DHS. McEntire (n. d.) further discusses the emergence of DHS:

DHS is the result of the most sweeping governmental reform since World War II and it performs many functions such as intelligence and warning, border and transportation security, domestic counter-terrorism, critical infrastructure and key asset protection, defense against catastrophic threat, and emergency preparedness and response. (p. 15)

The Quadrennial Report (2010) contends "although the integrated concept of Homeland Security arose at the turn of the 21st century, Homeland Security traces its roots to concepts that originated with the founding of the Republic" (p. 14). While 'Disaster Response' and 'Emergency Management' have been the principal terms to define the disaster response activities since the 1800s until September 11, after the foundation of DHS, the 'Homeland Security' enterprise has assumed an overarching role to oversee all security missions, including the one against terrorist attacks. National Strategy for Homeland Security (2007) points out the evolution of Homeland Security concept:

The understanding of homeland security continued to evolve after September 11, adapting to new realities and threats. The human suffering and staggering physical destruction caused by Hurricane Katrina was a reminder that threats come not only from terrorism, but also from nature. (p. 3)

Considering the National Strategy for Homeland Security (2002) - the first Homeland Security Strategy - as the starting point, the historical evolution of the Homeland Security concept could be theoretically divided into three subsequent periods:

- 2002-2007, the period which is defined by the *National Strategy for Homeland Security of 2002*.
- 2007-2010, the period which is defined by the *National Strategy for Homeland Security of 2007*.
- Post 2010, the period which is defined by the *Quadrennial Homeland Security Review Report (QHSR) of 2010*.

Although the Quadrennial Report (2010) states “the documents such as NIPP and NRF, as well as documents produced by the National Counterterrorism Center, spell out roles and responsibilities for various aspects of Homeland Security” (p. A-1), it is difficult to frame the contextual boundaries of Homeland Security within existing content knowledge incorporated in the official documents.

2.2.2 National Infrastructure Protection Plan (NIPP)

As one of the critical Homeland Security mandates, the NIPP (2009) “provides the unifying structure for the integration of existing and future Critical Infrastructure and Key Resources (CIKR) protection efforts and resiliency strategies into a single national

program to achieve the overarching goal of the NIPP” (p. 1). It “sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for the Department of Homeland Security; Federal Sector-Specific Agencies; and other Federal, State, regional, local, tribal, territorial, and private sector partners implementing the NIPP” (p. i). It further discusses the framework:

The NIPP framework supports the prioritization of protection and resiliency initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters. (National Infrastructure Protection Plan, 2009, p. 1)

The CIKR Support Annex (2008) states “the NIPP and its associated CIKR Sector-Specific Plans (SSPs) work in conjunction with the NRF and its supporting annexes to provide a foundation for CIKR preparedness, protection, response, and recovery efforts in an all-hazards context” (p. 3). The CIKR Sectors and responsible sector-specific agencies are included in Table 1. The list of CIKR which was first developed with the Homeland Security Presidential Directive 7 (HSPD-7), has established a framework for the security stakeholders to identify, prioritize, and protect the critical assets in their jurisdictions.

Table 1 Sector-Specific Agencies and CIKR Sectors (National Infrastructure Protection Plan, 2009)

Sector-Specific Agency		No	Critical Infrastructure and Key Resources Sector
Department of Agriculture Department of Health and Human Services		1	Agriculture and Food
Department of Defense		2	Defense Industrial Base
Department of Energy		3	Energy
Department of Health and Human Services		4	Healthcare and Public Health
Department of Interior		5	National Monuments and Icons
Department of Treasury		6	Banking and Finance
Environmental Protection Agency		7	Water
Department of Homeland Security	Office of Infrastructure Protection	8	Chemical
		9	Commercial Facilities
		10	Critical Manufacturing
		11	Dams
		12	Emergency Services
		13	Nuclear Reactors, Materials, and Waste
	Office of Cyber-security and Communications	14	Information Technology
		15	Communications
	Transportation Security Administration	16	Postal and Shipping
	Transportation Security Administration United States Coast Guard	17	Transportation Systems
	Immigration and Customs Enforcement, Federal Protective Service	18	Government Facilities

2.2.3 National Incident Management System (NIMS)

Origination of NIMS dates back to 2003. In 2003, “*Homeland Security Presidential Directive 5 (HSPD-5) - Management of Domestic Incidents* directed the Secretary of Homeland Security to develop and administer a National Incident Management System” (Fundamentals of Emergency Management, 2011, p. 2-6). The NIMS document was originally published in 2004 and revised in 2008 to reflect contributions from stakeholders and lessons learned during recent incidents. The NIMS framework “sets forth the comprehensive national approach” (National Incident Management System, 2008, p.5).

NIMS “is not an operational incident management or resource allocation plan; NIMS represents a core set of doctrines, concepts, principles, terminology, and organizational processes that enables effective, efficient, and collaborative incident management” (National Incident Management System, 2008, p. 3). “The incident management systems described in the NIMS is the foundation for the additional response procedures described in the NRF” (Civil Support Operations, 2010, p.2-1). *Fundamentals of Emergency Management* (2011) underlines the significance of NIMS as a common template:

NIMS provides a consistent nationwide template to enable Federal, State, Tribal, and local governments, nongovernmental organizations (NGOs), and the private sector to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity. (p. 2-6)

The Incident Command System (ICS), Multiagency Coordination System (MACS), and Public Information were introduced in NIMS (2008) as the fundamental elements of incident management. NIMS (2008) states “these elements provide

standardization through consistent terminology and established organizational structures” (p.45). ICS is “normally structured to facilitate activities in five major functional areas: command, operations, planning, logistics, and finance/administration; in some circumstances, intelligence and investigations may be added as a sixth functional area” (p. 48).

As stated in NIMS (2008), Incident Command (see Figure 9) is “responsible for overall management of the incident” (p. 49). “In an incident command organization, the Command Staff typically includes a Public Information Officer, a Safety Officer, and a Liaison Officer, who report directly to the IC/UC and may have assistants as necessary” (p. 51). “The incident Command and Management organization is located at the Incident Command Post (ICP); Incident Command directs the operations from the ICP which is generally located at or in the immediate vicinity of the incident site” (p. 53).

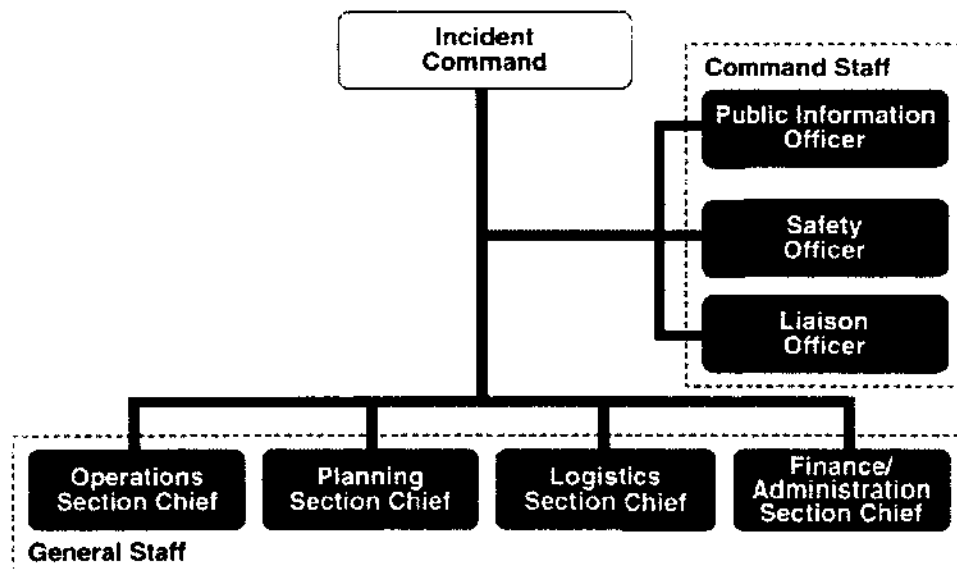


Figure 9 Incident Command System (National Incident Management System, 2008, p. 53)

The *National Response Framework* (2008) points out the requirement for the Area Command, which is “an organization to oversee the management of multiple incidents handled individually by separate ICS organizations or to oversee the management of a very large or evolving incident engaging multiple Incident Management Teams (IMTs)” (National Incident Management System, 2008, p. 61):

If necessary, an Area Command (Figure 10) may be established to assist the agency administrator/executive in providing oversight for the management of multiple incidents being handled by separate Incident Command Posts or to oversee management of a complex incident dispersed over a larger area and broker critical resources. (p. 50)

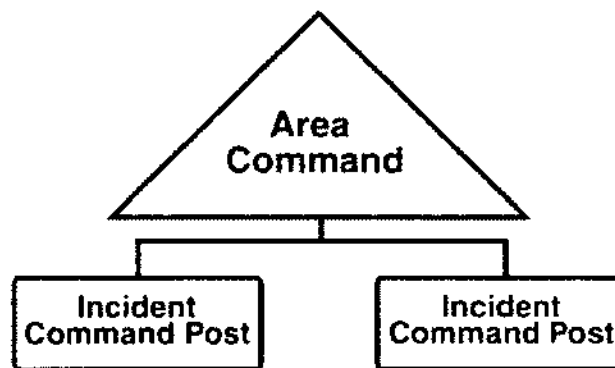


Figure 10 Area Command Structure (National Response Framework, 2008, p. 50)

2.2.4 National Response Framework (NRF)

NRF fulfills a significant role within the Homeland Security architecture. FEMA Pub 1 (2010) states “in 2008, FEMA led the development of the NRF which replaced both the National Response Plan developed by DHS in 2004” (p.12).

The *National Response Framework* (2008) is “a guide to how the Nation conducts all-hazards response” (p.1). It “establishes a comprehensive, national, all-hazards approach to domestic incident response, it provides disaster response principles to guide

and encourage all response partners to prepare for and provide a unified national response to major disasters and emergencies” (FEMA Pub 1, 2010, p.12). It “elaborates the principles in the NIMS, focusing on prevention, preparedness, response, and recovery. It provides the structure and mechanisms for coordinating federal support to state and local incident managers and for exercising federal authorities and responsibilities based on the NIMS” (Civil Support Operations, 2010, p.2-8).

The *National Response Framework* (2008) “builds upon the NIMS which provides a consistent template for managing incidents”(p. 1). It includes “the core document, the Emergency Support Functions (ESF), Support, and Incident Annexes, and the Partner Guides” (p.3). “The NRF core document and annexes, including the CIKR Support Annex, describe processes for coordination among various Federal departments and agencies; State, local, and tribal governments; and private sector partners, both for pre-incident preparedness, and post-incident response and short-term recovery” (*National Infrastructure Protection Plan*, 2009, p.78).

The NRF “specifies incident management roles and responsibilities, including emergency support functions designed to expedite the flow of resources and program support to the incident area” (*National Infrastructure Protection Plan*, 2009, p. 78). “FEMA coordinates response support from across the Federal Government and certain NGOs by calling up, as needed, one or more of the 15 ESFs” (*National Response Framework*, 2008, p. 57) (Table 2).

Table 2 Emergency Support Functions (National Response Framework, 2008)

ESF-1	Transportation
ESF-2	Communications
ESF-3	Public Works and Engineering
ESF-4	Firefighting
ESF-5	Emergency Management
ESF-6	Mass Care, Emergency Assistance, Housing, and Human Services
ESF-7	Logistics Management and Resource Support
ESF-8	Public Health and Medical Services
ESF-9	Search and Rescue
ESF-10	Oil and Hazardous Materials Response
ESF-11	Agriculture and Natural Resources
ESF-12	Energy
ESF-13	Public Safety and Security
ESF-14	Long-Term Community Recovery
ESF-15	External Affairs

The *National Response Framework (2008)* delineates the missions of Emergency Support Functions:

ESFs support access to Federal department and agency resources. They align categories of resources and provide strategic objectives for their use, and utilize standardized resource management concepts such as typing, inventorying, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident. (p. 29)

Within the National Response Framework (2008), the Joint Field Office (JFO) “is a temporary Federal facility that provides a central location for the coordination of Federal, State, tribal, and local governments, and private-sector and nongovernmental organizations with primary responsibility for response and recovery” (p. 62). It “provides the organizing structure to integrate diverse Federal authorities and capabilities and

coordinate Federal response and recovery operations; the JFO is internally organized and operated using the concepts and principles of the NIMS” (p.63). Figure 11 represents the overview of the JFO and its key components.

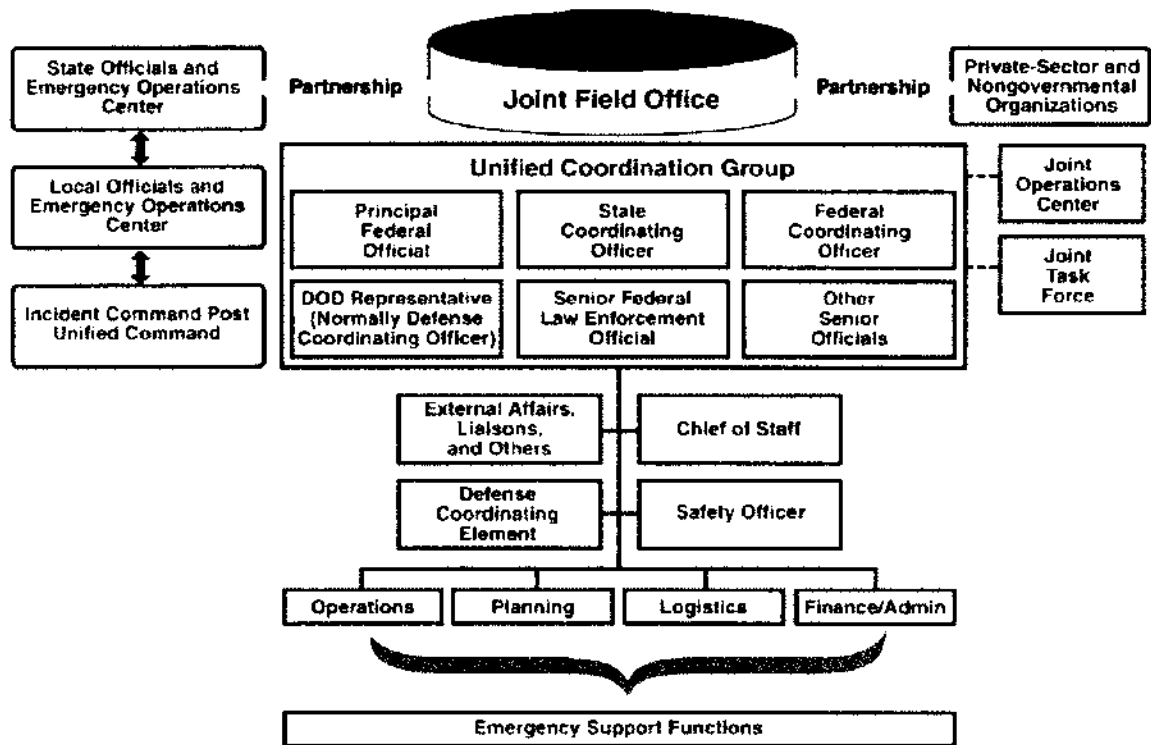


Figure 11 Joint Field Office (National Response Framework, 2008, p. 63)

2.2.5 Public Safety and Security (ESF-13)

Stability Operations (2011) introduces the elements of a stable state as human security, economic and infrastructure development, governance, and the rule of law. Within the context of this broad spectrum, Public Safety and Security, the physical protection of people and critical assets in urban areas has always been the primary focus for leading authorities and security agents during both ordinary/peacetime or crisis/wartime. The requirement summarized by Little (2004) has been assumed as an

important; “Security needs to be flexible and agile, and capable of addressing new threats as they emerge” (p. 57).

Emergency Support Functions (ESF) within the NRF are “a critical mechanism to coordinate functional capabilities and resources provided by Federal departments and agencies, along with certain private-sector and nongovernmental organizations” (*National Response Framework*, 2008, 57). Among these ESFs, the Emergency Support Function-13 (ESF-13) (Public Safety and Security) provides “a mechanism for coordination and support consisting of law enforcement, public safety, and security capabilities and resources during potential or actual incidents which require a coordinated Federal response” (Emergency Support Function-13, 2008, p. 1).

ESF-13 ensures “the conduit for utilizing and incorporating the extensive network of public safety and security coordination established for steady-state prevention efforts through a variety of interagency plans. Prevention and security plans include, but are not limited to, the following” (Emergency Support Function-13, 2008, p. 2):

- National Infrastructure Protection Plan
- Sector-Specific Plans
- The National Strategy for Maritime Transportation Security
- Area Maritime Security Plans
- Vessel and Facility Security Plans

However, the ESF-13 activities “should not be confused with the activities described in the *Terrorism Incident Law Enforcement and Investigation Annex* of the NRF or other criminal investigative law enforcement activities” (Emergency Support

Function-13, 2008, p. 2). “The law enforcement and investigative response to a terrorist threat or incident within the United States is a highly coordinated, multiagency State, local, tribal, and Federal responsibility” (Terrorism Incident, 2004, p.1). During any terrorist threat or incident, “ESF-13 coordinates and contributes support to DOJ/FBI operations, if requested” (Emergency Support Function-13, 2008, p. 2)

2.3 Hurricane Katrina

The U.S. Senate noted that the response to Hurricane Katrina showed a “failure to act on the lessons of past catastrophes, both man-made and natural, that demonstrated the need for a large, well-equipped, and coordinated law enforcement response to maintain or restore civil order after catastrophic events” (*Law Enforcement Deployment Teams*, 2007, p. 1). Having discussed ‘post-disaster security’ as one of the focal points in this dissertation, the forensic history of Hurricane Katrina has been included in the literature review considering the dramatic background information it provided for the post-disaster security and law enforcement requirement.

Hurricane Katrina was “one of the most powerful and devastating storms during the worst hurricane season in recorded history” (Oscar, 2006, p. 1). It was “the deadliest natural disaster in the United States since Hurricane San Felipe in 1928” (*The Federal Response*, 2006, p. 6). “As of early August 2006, the death toll exceeded 1800” (Graumann, Houston, Lawrimore, Levinson, Lott, McCown, Stephens and Wuertz, 2005, p.1).

Hurricane Katrina was also “the most costly natural disaster ever to strike the United States, and the deadliest since the Lake Okeechobee disaster of September, 1928”

(Graumann et al., 2005, p. 1) and it resulted in “approximately \$200 billion in property damage along the Gulf Coast area” (Wigginton, 2007, p. 6) .

In the *Select Bipartisan Committee* (2006) report, it was reported “during the first four days, no single organization or agency was in charge of providing a coordinated effort for rescue operations” (p. 230), “following the Hurricane Katrina, general unrest and violence occurred in crowded areas” (p. 244), and “the fluctuation in centralized command created many collateral problems for law enforcement, and the breakdown of authority led to an inability to efficiently request aid from State authorities” (Farber, 2006, p. 8).

2.3.1 Climatological Summary

Hurricane Katrina “was one of the strongest storms to impact the coast of the United States during the last 100 years” (Graumann et al., 2005, p.1). Figure 12 depicts the cone of uncertainty prior to Katrina’s landfall in southeast Louisiana which has been issued by National Hurricane Center. “At landfall, sustained winds were 127 mph and the minimum central pressure was the third lowest on record (920 mb)” (Graumann et al., 2005, p. 1). “It first made landfall as a Category 1 hurricane just north of Miami, Florida on August 25, 2005, then again on August 29 as a Category 4 along the Central Gulf Coast near New Orleans, Louisiana” (Oscar, 2006, p. 1). “The flooding of New Orleans resulted in the displacement of more than 250,000 people, a higher number than during the Dust Bowl years of the 1930’s” (Graumann et al., 2005, p. 1).

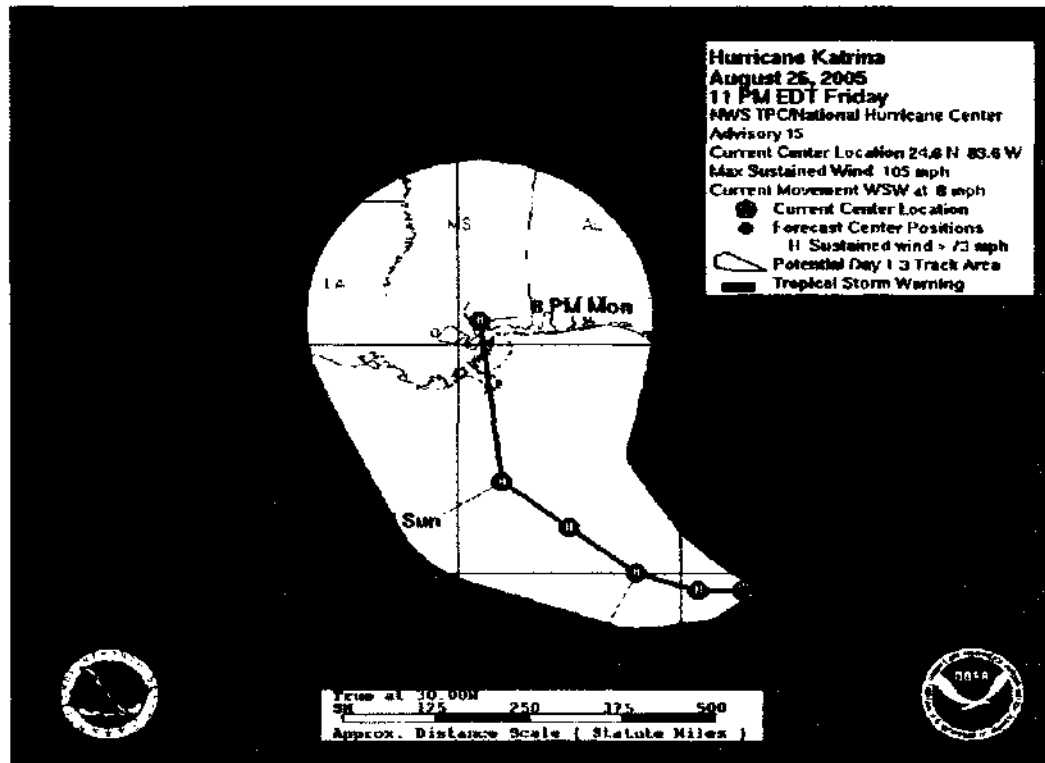


Figure 12 Hurricane Katrina: Cone of the Uncertainty (Hurricane Katrina, 2006, p.13)

2.3.2 Forensic Continuum of the Crisis

This chapter aims to delineate the causes of disorder and lawlessness in the post-disaster urban environment where the execution of security and law enforcement missions failed.

The word 'forensic' "applies to the use of scientific methods and techniques to investigate a crime and help resolve legal issues in a court of law" (Forensic, *Forensic Science*, (n.d.)). Forensic is "relating to or dealing with the application of scientific knowledge to legal problems" (Merriam-Webster, *Forensic*, 2011). "Forensic scientists are instrumental in identifying and convicting criminals, and their analysis of forensic

evidence often confirms the guilt or innocence of possible suspects in a crime” (Forensic, *Forensic Science*, (n.d.)).

Law and Order Operations (2011) defines ‘forensics’ as it is “the deliberate collection and methodical analysis of evidence to establish facts that can be used to establish connections between persons, objects, or data” (p. 3-17). In similar way, NATO CBRN (2012) discusses that “forensics is the comprehensive scientific analysis of physical, biological, behavioral, and documentary evidence in support of an investigation, and the goal of forensics is to determine whether associations exist among people, places, things, and events” (p. 4).

The following paragraphs, which excerpt information from different sources provide valuable insights for interpreting the forensic continuum of the Hurricane Katrina disaster and evidence of the public safety and law enforcement failures.

Public Safety and Security Failures

“First the levees were breached, and then law and order” (*Select Bipartisan Committee*, 2006, p. 260). “In the aftermath of Hurricane Katrina, local and state authorities were unclear of the procedures necessary to receive assistance from federal authorities; while FEMA was on site, it alone did not have the authority to bring in active duty troops” (Oscar, 2006, p. 10). “Much of the military support was also uncoordinated. The Louisiana National Guard and Department of Defense active duty forces, under Joint Task Force Katrina, were under separate commands” (*Select Bipartisan Committee*, 2006, p. 195).

Following Hurricane Katrina, in support of local police and other security agents, thousands of troops from National Guard Units, Active Military Units and other federal

units were deployed to the disaster area. “As of 7 September the National Guard forces operating in the recovery area are over 41,000 and there were more than 17,000 Active duty Soldiers, Airman and Marines hard at work in the effort” (Oscar, 2006, p.10). This great surge of forces did not make the expected impact on the scene at the initial phases of the response/recovery activities:

Due to lack of coordination and inefficient plans, although while the military clearly provided vital support, no one had the total picture of the situation on the ground, the capabilities that were on the way, the missions that had been resourced, and the missions that still needed to be completed. (Pickup, 2006, p. 3)

From the law enforcement perspective, many security failures were experienced particularly in the first 1-3 days of the response/recovery phase of the disaster. During this period, many crimes were committed: stores were looted, many people were murdered, and gangs terrorized the public in some part of the cities. Eventually, the shortfalls in security management deteriorated other emergency management response/recovery missions as it was reported by Select Bipartisan Committee (2006) report; “1,000 FEMA employees set to arrive in New Orleans on Wednesday, August 31, turned back due to security concerns” (p. 249). Wigginton (2007) described the situation dramatically:

Once Hurricane Katrina hit the disaster area; the local agents were unable to act as first responders because of the flooding. During the waning days following the storm, there was complete chaos. New Orleans was on the verge of anarchy and the police department was literally paralyzed by the storm. Especially, as the NOPD focused on rescue operations, civil disorder began to spread throughout the city. Gangs roamed the streets, robbed, looted and committed acts of arson on businesses and residences. Various news agencies reported that New Orleans area Wal-Mart stores had been looted and all the weapons and ammunition had been reported stolen. NOPD district stations were often victimized by random sniper fire. (p. 5)

The *Select Bipartisan Committee* (2006) contended “in some areas, the collapse or absence of law enforcement exacerbated the level of lawlessness and violence” (p.244). “Citizens described not just a lack of a show of force but the widespread perception that the police themselves were engaged in criminal behavior” (Farber, 2006, p.6).

However, “the Louisiana State Police provided relatively quick assistance; although the New Orleans Police Department had lost its command and control capabilities, the Louisiana State Police operated under its own broad law enforcement statutory mandate” (*Select Bipartisan Committee*, 2006, p. 246). “Approximately four days following the storm, federal troops began to arriving in New Orleans” (Wigginton, 2007, p.49), and eventually a more stable security environment was established:

Law and order were eventually restored as local law enforcement officers were removed from search and rescue, reassigned to law enforcement missions, and supplemented first by state National Guard troops, then by other state and local police through the Emergency Management Assistance Compact (EMAC¹) process. (*Select Bipartisan Committee*, 2006, p. 242)

The National Guard “was activated to help maintain law and order in the city as well as to assist with rescue efforts” (Mener, 2007, p. 45). “These forces participated in every aspect of emergency response, from medical care to law enforcement and debris removal, and were considered invaluable by Louisiana and Mississippi officials” (Committee, 2006, p. 10).

¹ The Emergency Management Assistance Compact (EMAC) offers state to state assistance during governor-declared states of emergency. Ratified by Congress in 1996, 49 states and the District of Columbia have enacted legislation to become members of EMAC. EMAC is administered by the National Emergency Management Association (NEMA) (*Select Bipartisan Committee*, 2006, p. 249). Through EMAC or other mutual aid or assistance agreements, a State can request and receive assistance from other member States. Such State-to-State assistance may include (National Response Framework, 2008, p. 40):

- Invoking and administering a Statewide Mutual Aid Agreement, as well as coordinating the allocation of resources under that agreement.
- Invoking and administering EMAC and/or other compacts and agreements, and coordinating the allocation of resources that are made available to and from other States.

Mener (2007) claimed “by the end of the relief efforts, 40,000 National Guard troops were deployed under state control and an additional 30,000 military personnel were deployed under federal control” (p. 45), while Select Bipartisan Committee (2006) underlined the contribution of the active military units:

While not immediately deployed, Department of Defense (DoD) active duty forces also played a role in restoring and maintaining law and order. Precautions were taken to prevent DoD active duty forces from direct law enforcement missions, thereby avoiding Posse Comitatus² issues. (p. 242)

In summary, while the severity of the disaster deteriorated the overall situation in terms of emergency management, the contingency plans and relevant response/recovery missions did not sufficiently meet the requirements of coordination and security during the post-disaster period. There was a lack of central coordination, and preparedness regarding the positioning of the support troops as well as determining the actions that should be executed by those troops in the disaster hit areas of the operation. Following quote highlights this assumption:

Although the process successfully deployed a large number of National Guard troops, it did not proceed efficiently, or according to any pre-existing plan or process. There was, in fact, no established process for the large-scale, nation-wide deployment of National Guard troops for civil support. In addition, the deployments of National Guard troops were not coordinated with the federal Northern Command. (Committee, 2006, p. 10)

² The federal Posse Comitatus Act of 1878 prohibits the use of the Army and the Air Force (originally part of the Army) to execute the laws of the United States except where authorized by the Constitution or Acts of Congress (Committee, 2006, p. 470). The Posse Comitatus Act is inappropriate for modern times and needs to be replaced by a completely new law. The old law is widely misunderstood and unclear. It leaves plenty of room for people to do unwise and perhaps unlawful things while trying to comply with their particular interpretation (Oscar, 2006).

2.4 Systems Thinking and Complexity

DHS has an organizational structure that presents complex system of systems (meta-system comprised of multiple complex systems, further defined on page 40) characteristics with numerous entities and too many interagency missions/functions that all require a tremendous amount of oversight, coordination and synchronization effort.

The literature review addressing the ‘Challenges of Complex Systems’ and ‘Systems Philosophy and Thinking’ is included in the next chapters since the analysis and model development processes of this dissertation were mostly inspired from these theories.

2.4.1 Challenges of Complex Systems

Weck, Roos and Magee (2011) noted “heightened awareness has been fueled by the explosion in the information available to people on nearly any topic and technology continued to progress and systems became even more complex and capable of making modern life simultaneously easier and more challenging” (p. 12). Secilmis (2012) discussed “while already having many mysterious³ and complex universal systems which are still waiting to be explored, we’ve found ourselves in dealing with the manmade systems which have even turned into challenging complex paradigms”, while Weck et al. (2011) claimed “systems that had once been clearly separate began to interact more than anyone could have imagined, scale and complexity increased inexorably and we ended up with systems of systems” (p. 12).

³ Since we realize that even at the beginning of 21st century, we don’t have a clear understanding of dark matter and dark energy which are claimed to make over 95 % of the universe (NASA-science). Furthermore, cosmologist talk about multiverses that we don’t know yet (Oren and Yilmaz, 2013, p. 158).

Secilmis (2012) further contended “organizational systems as well as the normal life routines are becoming increasingly complicated due to the involvement of more sophisticated information and communication technologies” as Bar-Yam (2004) supported Secilmis’s discussion “the amount of the information that is flowing and the rate of exchange are both aspects of the growing complexity of our existence” (p.13). “Today, boundaries between large-scale technology-based systems are becoming increasingly blurry. This increasing degree of complexity and interconnectedness poses formidable challenges for the new generation of engineers, scientists, and managers in the twenty-first century” (Weck et al., 2011, p. XII).

In this challenging environment, the individuals’ involvement is now more important for organizational success than it was in the past because the existing high information flow and rate of exchange empower the individual easy access to what he or she needs; however it is likely that “exceedingly large number of entities, dynamic interactions, continuous unforeseen emergent conditions and high degree of uncertainty in a complex system would continue to make the individuals confused to define their roles and contribute/involve in the system appropriately” (Secilmis, 2012).

Secilmis (2012) claimed “the increase in the numbers of different system elements would eventually dictate complexity to the system”, while Szabo and Teo (2013) noted complex systems characteristics “complex systems often exhibit properties that are not easily predictable by analyzing the behavior of their individual, interacting components” (p. 319). “Since all the elements in a complex system are rarely in the same shape, mode, structure or character; every specific system state would have a different pattern of relations” (Secilmis, 2012).

Calvano and John (2004) state that “a number of workers in Complexity Science, seeking to characterize complexity, have developed a list of features, of which at least some would be possessed by a complex system, which are: elements, interactions, formation/operation diversity and variability, environment, and activities” (p. 30). In a similar way, Secilmis (2012) has introduced three important characteristics of the complex systems: the number of elements/entities, the number and type of interactions, and the dynamic nature of the system.

The definitions of Complex Systems and System of Systems (Table 3) studied by Keating, Sousa-Posa and Mun (2003) provide a deeper insight on the terminology which is required for the appreciation of complexity and complex systems discussions.

Table 3 Definitions of Complex Systems and System of Systems

COMPLEX SYSTEMS	SYSTEM OF SYSTEMS
A bounded set of richly interrelated elements for which the characteristic structural and behavioral patterns that produce system performance emerge over time and through interaction between the elements and the system interaction with the environment (p. 3).	A meta--system comprised of multiple embedded and interrelated autonomous complex subsystems that can be diverse in technology, context, operation, geography, and conceptual frame. These complex subsystems must function as an integrated meta-system to produce desirable results in performance to achieve a higher-level mission subject to constraints (p. 4).

2.4.2 Systems Philosophy and Thinking

Since the systems field is divided into three main components of ‘general systems theory, systems science, and systems philosophy’ in a study of the literature (M’Pherson,

1974), the definitions of philosophy, philosophy of science, system(s), and systems philosophy should be revisited before eliciting the relationship between systems philosophy and systems thinking.

Philosophy is “the academic discipline concerned with making explicit the nature and significance of ordinary and scientific beliefs and investigating the intelligibility of concepts by means of rational argument concerning their presuppositions, implications, and interrelationships” (Philosophy, *The Free Dictionary*, (n.d.)). Philosophy is “the rational investigation of the truths and principles of being, knowledge, or conduct” (Philosophy, *Dictionary*, (n.d.)).

Philosophy of science is “concerned with the methods that scientists use in discovery, and to elaborate and confirm theories” (Machamer, 1998). Philosophy of science is “the formulation of worldviews that are consistent with, and in some sense based on, important scientific theories” (Losee, 2001). “Epistemologically, it asks what the nature and essential characteristics of scientific knowledge are, how this knowledge is obtained, how it is codified and presented, how it is subjected to scrutiny, and how it is warranted or validated” (Machamer, 1998).

With regard to system(s), Secilmis (2012) states that a basic system phenomenon should at least consist of elements/entities, interactions and borders, while Laszlo (1998) defines the system as it is a “structured set which elements interact among them and that has characteristics of the whole no present in the characteristics of its elements or their relationships” (p. 2). Further, Edson (2008) contends that “a system is a set of two or more elements that satisfies the following three conditions” (p. 6):

- The behavior of each element has an effect on the behavior of the whole.

- The behavior of the elements and their effects on the whole are interdependent.
- Elements of a system are so connected that independent subgroups of them cannot be formed.

Notwithstanding that systems philosophy and systems thinking might be used interchangeably, Laszlo (1998) tells us “systems philosophy sets forth a reorganization of ways of perceiving and thinking while systems thinking is systems philosophy as a process,” while Edson (2008) contends “systems thinking is both a world view and a process, it can be used for both the development and understanding of a system and for the approach used to solve a problem.”

Systems philosophy is “a perspective philosophy, seeking the connections between different theories, and probing the ultimate implications of the systems paradigm; it provides links to such traditional philosophical studies as epistemology and ontology” (M’Pherson, 1974, p.228). Systems philosophy is “about using systems concepts and systems methods to construct a realistic ‘philosophy’ and putting it to practical use” (About Systems Philosophy, 2012).

Laszlo (1998) discusses that systems thinking is a cognitive process which uses both analysis and synthesis to capture a comprehensive understanding of the whole. It helps to understand the whole and its parts, the relations between those, and further the relation of the whole with its context and environment. In a similar vein, Weck et al. (2011) contend:

System thinking includes holism, an ability to think about the system as a whole; focus, an ability to address the important system level issues,

emergence, and recognition that there are latent properties in systems; and trade-offs, judgment, and balance, which enable one to judge all the various considerations and make a proper choice. (p. 190)

In systems thinking, as a matter of holism, framing the system problem at the very beginning is crucial for the subsequent phases of the analysis. To frame the system problem, Secilmis (2012) proposes a vantage point and viewing angle far enough from the area of system interest in line with the level of their involvement in the system process, as illustrated in Figure 13. He contends that doing so enables analysts to appreciate the system structure, layers and functions in both scale and scope.

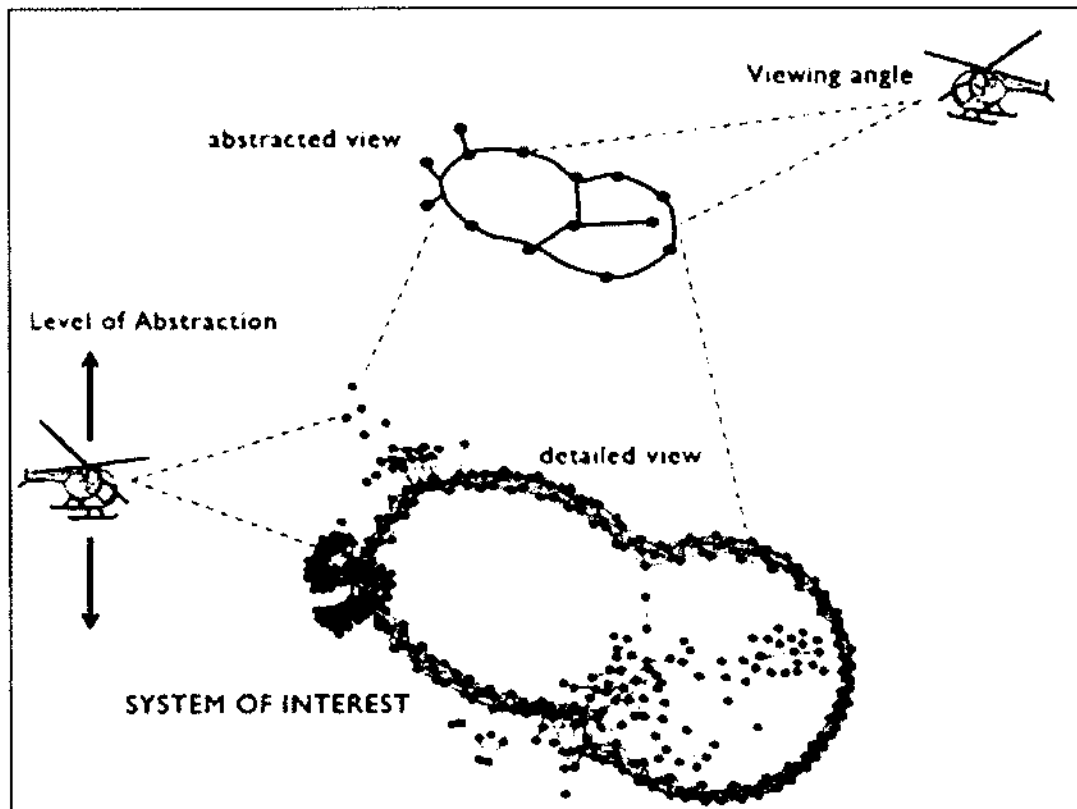


Figure 13 Systems (Re)Visioning Perspective at Various Levels of Abstraction and Viewing Angles (Weck et al., 2011, p. 47)

In conclusion, consistent with the systems philosophy, systems thinking looks for an understanding of a system considering the linkages and interactions between the elements that compose the entire system (Hake, 2009). As Edson (2008) has pointed out, systems thinking could be utilized in different areas:

In today's world of interconnectivity, interdependence and globalization, the traditional and reductionist approaches to problem solving might be inadequate; while systems thinking, which adopts the holism, provides the tools to understand and solve the tough problems through the combination of synthesis, analysis and inquiry. In this sense, systems thinking can be utilized in all areas including national security, homeland security, energy, environment, healthcare, and business. (p. 47)

2.5 Epistemology and Philosophical Perspective of Modeling

Tolk (2013) contends “a formal approach to ontology, epistemology, and teleology of Modeling and Simulation (M&S) will provide a framework to address many fundamental questions systemically and holistically” (p.12).

The appreciation of systems philosophy is required for “systems architects” to conduct complex systems analyses and develop optimal representations and models. The rationale is that philosophy of science issues (ontology and epistemology) affect the utilization and interpretation of results obtained from applications of systems methodologies (Systems Analysis, 2010). For this reason, the exploration of Epistemology and Philosophical Perspective of Modeling has been included in this chapter to support the key focus areas of this dissertation theoretically.

2.5.1 Epistemology

Epistemology is “the study of how we come to know, how we define knowledge, represent it, and communicate it with others” (Hofmann, 2013, p.82). It “focuses on the

way we define knowledge, especially how we come to know new knowledge” (Wang, Wang, Li, and Yang, 2013, p. 336). Bozkurt (2009) contends that “the Epistemological paradigm is related to how the individual tends to seek knowledge about reality; the questions put forward by epistemology include: What are the sources of knowledge? What is nature of knowledge? Is our knowledge is valid?” (p. 34).

Epistemology “deals with the question of what can be known. It is also closely associated with the psychology of cognition, with the premise that one cannot give the best advice about intellectual operations without detailed information about mental processes” (Bozkurt, 2009, p.30).

Bozkurt (2009) further discusses empiricism and rationalism as they are the main two currents of epistemology paradigm. She defines empiricism as “a theory of knowledge which emphasizes the aspects of scientific knowledge that are closely related to experience through deliberate experimental arrangements” (p. 35), while “Rationalism is the philosophical belief that asserts the truth can best be discovered by reason and factual analysis” (p. 37).

Since a quick overview of the philosophical paradigms would catalyze the appreciation of epistemology and its critical aspects from a holistic perspective, a synopsis of the philosophical paradigms has been included in the following paragraph.

Synopsis of the Philosophical Paradigms: Bozkurt (2009) contends that “Denzin and Lincoln (1994) consider Ontology, Epistemology and Axiology as the main philosophical paradigms” (p. 29), while Wang et al. (2013) posit “Ontology, Epistemology, and Teleology build philosophical foundation of a discipline” (p. 336). Further; “Ruona and Lynham (2004) include Methodology within Axiology” (Bozkurt,

2009, p. 29), whereas Bozkurt adds Teleology to the philosophical categories to explore the philosophical profile of the individual. To that end, “together these branches of philosophy are indispensable to answer the crucial question: why and when can we rely on the recommendations generated via M&S” (Hofmann, 2013, p.82). In the context of model development, a holistic interpretation of the relationship of these philosophical paradigms has been depicted in Figure 14, and supporting definitions have been included in Table 4.

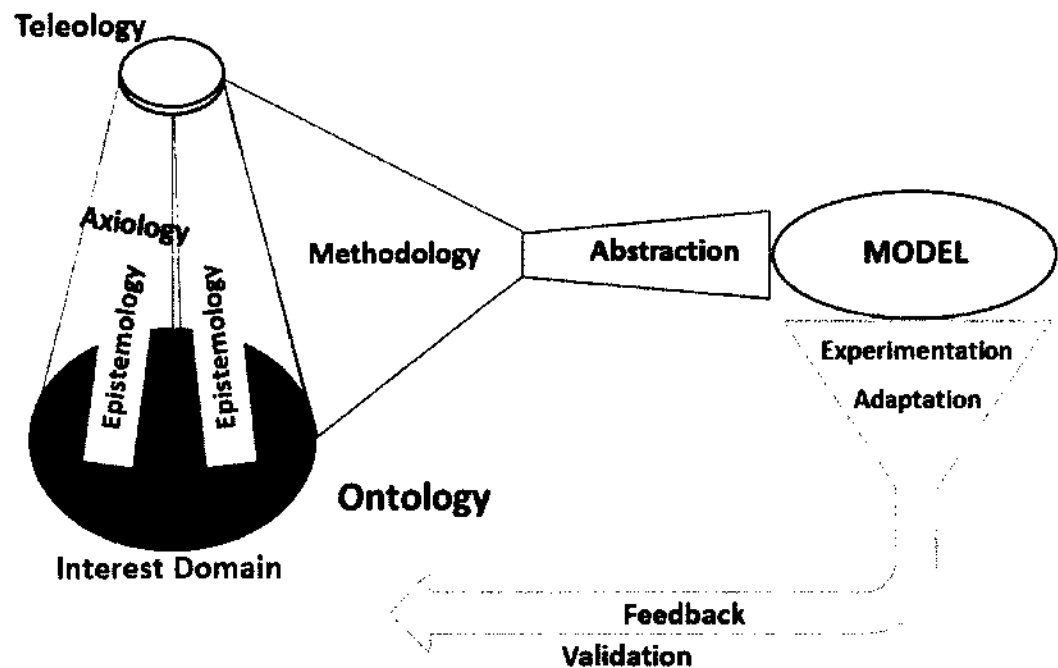


Figure 14 Relationships between Philosophical Paradigms in the Context of Model Development

Table 4 Definitions of Philosophical Paradigms

Ontology
Ontology is “the study of what exists” (Hofmann, 2013, p.60); it is “our picture of how the world looks” (Solem, 2003, p.439); it “includes everything that is accepted” (Bozkurt, Padilla and Souza-Poza, 2007).
Epistemology
Epistemology is “the study of how we come to know, how we define knowledge, represent it, and communicate it with others” (Hofmann, 2013, p.82). It “focuses on the way we define knowledge, especially how we come to know new knowledge” (Wang et al., 2013, p. 336).
Axiology
Axiology is ‘the study of the nature, types, and criteria of values and of value judgments especially in ethics’ (Merriam-Webster, Axiology, 2012). Axiology is “the philosophical study of goodness, or value, in the widest sense of these terms” (Bozkurt, 2009, p. 40).
Teleology
Teleology is “the study of purpose and purpose-driven actions that result in methods” (Wang et al., 2013, p. 349). Teleology is “an area of philosophy which explains the future in terms of the past and the present based upon the study of purpose, ends, goals and final causes “(Bozkurt, 2009, p. 39).
Methodology
Methodology is “the epistemology within an implemented and more pragmatic level, it can be assumed to be one level more specific than epistemology. Whereas epistemology is the theory of acquiring knowledge, methodology is the detailed explanation and description of ‘how’ and through which means this knowledge is obtained” (Bozkurt, 2009, p. 30). “The desired methodology will provide guidance for methods relating ontology to epistemology, consistent with axiology. Consequently, the methodology will be composed of conclusions derived from the associated principles” (Brewer, 2010, p. 81).

2.5.2 System Representation and Modeling

Modeling is “a science when we attempt to organize what has been created and discovered in the field in an attempt to create a working and valuable abstraction of that field” (Smith, 2013, p. 253). It is “always centered on a specific problem; whether the right level of abstraction was chosen can only be properly assessed with respect to the problem one wants to solve” (Pyka and Deichsel, 2013, p.151).

In decision problems as well as in analysis problems, a model is a “representation of reality, and simulation provides a very powerful and flexible opportunity for goal-directed experimentation with a model reality (Oren and Yilmaz, 2013, p. 167). Weirich (2013) contends “a model explains a natural system because of the way the model represents the natural system; accounting for its explanatory power requires specifying the representational figures that give it explanatory power” (p. 113). He further discusses “models are more ambitious in their treatment of reality than are heuristic devices” (p. 112).

Smith (2013) posits “abstraction and aggregation are two powerful tools for identifying a model’s representation of the world; abstraction creates hierarchy, while aggregation internalizes or eliminates hierarchy” (p. 249). In this sense; “the conceptual model represents, as a purposeful abstraction and simplification of a perception of reality, everything that according to the world view of the model developers is necessary to address the underlying research questions, but no more” (Tolk, 2013, p.6).

Regarding the effective utilization of models, Tolk (2013) contends “the intelligent use of modeling and simulation science requires not just an appraisal of how well a chosen method works within a given model, but strategies for choosing the

appropriate modeling techniques to attack a given problem” (p.VII), while Smith (2013) makes an emphasis on the unbounded nature of the modeling, “though modern science and business have created and adopted classification schemes, taxonomies, and operating rules that can be applied almost universally, the practice of building models and simulations remains unbounded by science” (p. 246).

The fineness or correctness of a model could be appreciated through its resolution or precision. Tolk (2013) defines the resolution of a model or simulation as “the degree of detail and precision used in the representation of real world aspects in a model or simulation; resolution means the fineness of detail that can be represented or distinguished in an image” (p. 17). In a similar vein, Smith (2013) discusses the ‘usefulness’ of the model: “the current practice of modeling allows almost any approach while its measure of correctness is determined solely by the usefulness of the resulting product” (p. 246), while Oren and Yilmaz (2013) underline the perception of reality in the context of the representation: “sometimes a representation of reality may be different than reality under several conditions such as: misperceived reality, misunderstood reality, distorted reality, deliberately distorted reality, apparent reality, and unknown reality” (p. 164).

Models are “purposeful abstractions and simplification of reality resulting in a conceptualization that is transformed into an executable simulation system” (Tolk, 2013, p.11). Pyka and Deichsel (2013) contend “simpler models are not only easier to understand, but they are more tractable as well” (p. 151), and “in practice, it seems more likely that we do not understand the processes under investigation to a high degree, which makes approximation and estimation inevitable” (p. 148), whereas Douglass and Mittal

(2013) point out the importance of exhaustive information which may lead us to the utilization of a complex model: “in order to express a rich knowledge set that includes environment, contingencies, resources, possible actions and much more; we need a framework that allows us to represent knowledge in many facets or dimensions” (p. 282).

To that link to the hypotheses of this dissertation: once the complexity of a system increases, a reliable system abstraction/representation through figurative illustrations or representation by models/methods would be required to appreciate the system design/concept/context as a whole. In that sense; as has been discussed in Chapter 5, the utilization of the figures, which illustrate top-down holistic multi-dimensional system representations/abstractions could be helpful not only for the decision making and training requirements of the system stakeholders (individuals, groups, leaders, etc.), but also for the development of reliable models which would perform critical functions to achieve the assigned goals.

However, we are still having challenges developing optimal complex system abstractions. In principle, a complex context needs to be utilized to address the knowledge in many facets when the interest domain represents complex characteristics. In other words, the complexity of the methods/models must theoretically match the complexity of the systems/system problems. Per contra, the fact that simpler models/methods are easier to understand is still valid. Models should be scoped in workable limits, abstraction and aggregation as well as approximation, when dealing with complex systems with extensive scales. The quality of the resolution (degree of detail and precision used in the representation) of a model/method inextricably links to the elaborated details processed in the model/method.

Therefore, the development of modeling & simulation and multi-dimensional holistic illustrative system abstractions/representations is an open ended process, which mostly relies on divergent thinking capacity and systems appreciation of the analysts. The postulate of Smith (2013) has been included as an epilogue for this discussion:

The unbounded nature of the current practice of modeling is supportive of an artistic approach to modeling that encourages creative freedom in imagining and building a unique new model. (p. 246)

2.6 Multi-Criteria Decision Making (MCDM)

Hester (2010) contends that complex choices are a way of life for individuals, and it is usually challenging to make a decision on complex choices that involve multiple attributes⁴. “In the presence of a large number of conflicting criteria and numerous alternatives, it becomes very difficult for decision makers to articulate trade-off information and maintain some measure of consistency in their responses” (Jin, 2005, p. 51).

Multi-Criteria Decision Making (MCDM) is a process that helps people make choices in the presence of multiple conflicting criteria (Koksalan, Wallenius and Zionts, 2011). MCDM, used interchangeably with Multi-Criteria Decision Analysis (MCDA), is a continuum during which supportive ideas or recommendations are developed to provide a clear guidance for the decision maker(s) who needs to deal with complex choices, which includes multiple attributes and different sets of criteria.

Considering the stakeholder preferences and value judgments as well as scientific modeling and risk analysis; MCDM focuses on a comprehensive, structured process for

⁴ Attribute is a quality or characteristic inherent in or ascribed to someone or something (Attribute, (n.d.)). An attribute is a concrete descriptive value, a measurable characteristic of an entity, including interentity relationships. Attributes are used as both decision variables and decision criteria (Drobne. Lisc, 2009, p. 461).

selecting the optimal alternative in any given situation (Linkov and Steevens, (n.d.)). The final goal in MCDM is to come to a compromised judgment or optimal decision to avoid conflicting evaluations.

2.6.1 Overview of Multi-Criteria Decision Making (MCDM)

MCDM “aims at providing the decision makers with a systematic way to clarify the decision problem” (Jin, 2005, p. 52). The MCDM framework relies on the decision criteria and weightings, and it allows assessment of trade-offs involved in the decision-making process (Linkov and Steevens, (n.d.)). Ye (2006) discusses that multiple criteria decision analysis involves in defining objectives; identifying criteria, and alternatives; and then measuring consequences. Malczewski (1999) contends that MCDM addresses a set of alternatives that are evaluated on the basis of conflicting and incommensurate criteria.

MCDM, as an important subfield of Operations Research/Management Science, has grown quickly (Koksalan et al., 2011). “As humans tend to base rational decisions on an assessment of multiple decision criteria, MCDM methods have become important tools in management sciences and operations research” (Drobne and Lisec, 2009, p. 460), and different schools of thought have been developed for solving MCDM problems.

Since the 1960s, MCDM has been a part of Operations Research which explicitly deals with multiple criteria in decision-making processes. The two major classes of MCDM can be introduced as Multi-Attribute Decision Analysis (MADA) and Multi-objective Decision Analysis (MODA). While MADA is concerned with choosing from small, finite, or countable number of strategies, MODA considers choosing from a large,

infinite, or uncountable number of alternatives. Both MADA and MODA problems are categorized into single-decision-maker problems and group decision problems, and these two categories could be further subdivided into three different groups; Deterministic, Probabilistic, Fuzzy Decision (Malczewski 1999).

Decision making with consideration of risk is used when determining the probabilities of future or unknowable events; there are potential risks when uncertainty is involved (Hester, 2010). “Different types of real life problems in management practice can be formulated as multi-criteria analysis problems. Such are the problems of evaluation and choice of resources, strategies, projects, offers, policies, credits, products, innovations, designs, costs, profits, portfolios, etc.” (Genova, Vassilev, Andonov, Vassileva, Konstantinova, 2004).

The measurement processes in MCDM are developed subjectively from various preferences (Saaty, 2005). MCDM provides a decision matrix framework or structure, which supports integrating the expected weights as well as evaluating and ranking the alternatives (Yoe, 2002). “This structured process would be of great benefit to decision-making for decision problems, where there is currently no structured approach for making justifiable and transparent decisions with explicit trade-offs between different factors” (Linkov and Steevens, (n.d.), p. 827).

Within MCDM, there are multiple methods utilized which have unique characteristics organizing the evaluation/assessment algorithm and data. “Each one of these methods has its advantages and shortcomings, connected mainly with the ways of receiving information by the DM relating to his/her preferences” (Genova et al., 2004). Regarding the evaluation of different MCDM methods, Hester (2010) further discusses

four criteria that could be applied for the assessment of different decision making strategies: compensatory vs. non-compensatory, effort, alternative-based vs. attribute-based strategies, and exhaustive.

In conclusion, decision making processes usually have three content elements which are alternatives, criteria and methods. From alternatives, we choose the 'best'; criteria is a tool for an exact judgment; and methods are ways to select one alternative from the whole set. During a complex decision making process, finding the best method for a problem might be challenging. However, the MCDM methodologies ease the process, as they provide different measurement algorithms, and the selection of the methodology depends on the problem definition and variables at hand, as well as the decision maker's preferences.

2.6.2 Fuzzy Sets Theory

The conceptual matrix framework of the PDSI Model, which is delineated in Chapter 4, has been mostly inspired from the Fuzzy Sets theory, one of the major approaches in the school of MCDM.

Dhar (1979) contends "the concept of fuzzy sets theory recently has been extended and applied in various fields" (p. 586). Regarding the uncertainty, imprecision and vagueness of potential decision making problems; Jin (2005) underscores the powerful characteristics of fuzzy modeling:

Many systems are not amenable to conventional modeling approaches due to the lack of precise or accurate information, due to the strongly nonlinear behavior, the high degree of uncertainty, or the time varying characteristics. Fuzzy modeling along with other related techniques has been recognized as a powerful tool that can facilitate effective reflection of uncertainties. (p. 65)

“To find an optimal alternative of a project, usually the states of the system and associated utilities are assumed to be statistically known” (Dhar, 1979, p. 585), however this is not the case for many circumstances, since utilities of variables usually are unknown statistically and uncertainty is a typical characteristic of the system state. In that sense, Dhar (1979) criticizes the statistical decision theory:

In applying statistical decision theory since the decision maker tacitly equates the system fuzziness with randomness and neglects certain criteria of merits because of unavailability of statistical data, the application of only statistical decision theory for determination of the optimal decision is of doubtful value. (p. 592)

Belmann and Zadeh (1970) posit “by decision-making in a fuzzy environment is that a decision process in which the goals and/or the constraints, but not necessarily the system under control, are fuzzy in nature” (p. iii); likewise Dhar (1979) contends “the final objectives, the system states and constraints are not sharply defined and are fuzzy in nature” (p. 585).

A fuzzy set is “a class of objects with continuum of grades of membership. The notions of inclusion, union, intersection, complement, relation, convexity, etc., are extended to such sets, and various properties of these notions in the context of fuzzy sets are established” (Zadeh, 1965, p. 338). “Fuzzy goals and fuzzy constraints can be defined precisely as fuzzy sets in the space of alternatives. A fuzzy decision, then, may be viewed as an intersection of the given goals and constraints” (Belmann and Zadeh, 1970, p. iii).

Through various fuzzy sets applications, both quantitative and linguistic criteria of merits are included in the process of assessment. Regarding qualitative fuzzy semantics, “the fuzzy assessments expressed in linguistic terms are often the most

intuitive and effective way for the decision makers to deal with the subjectiveness and vagueness inherent in the fuzzy MCDM problem” (Yeh and Deng, 1997, p. 1567).

Some significant characteristics of step-wise algorithms which have been derived from Fuzzy Sets Theory as include;

- Fuzzy Sets enable decision maker(s) to perform analysis considering all possible system states.
- Both grades of membership for each possible system state and utility weights for each alternative can be incorporated into analysis.
- Both statistical data and linguistic variables can be processed within the criteria of merit. (Decision maker can include the criteria of merit that are usually neglected in statistical decision theory.)
- The choice of an optimal alternative, as an output of the decision making process, indicates the relative merits of all alternatives.

2.6.3 Recognition Heuristic and Elimination by Aspects

In case the exhaustive methods are impractical due to time constraints, resources, etc., a heuristic approach could be utilized to accelerate the speed of the decision making process, which seeks a compromised solution. Hester (2010) contends that “decisions are biased by individual’s availability heuristic (whatever information is most available to the analyst at the time of the analysis carries the most weight)” (p. 45).

The recognition heuristic is “a simple model that can be applied for many purposes” (Gigerenzer and Goldstein, 2011, p. 114). It is “a low effort, alternative-based, non-exhaustive approach; it is very efficient but not necessarily optimal” (Hester, 2010,

p. 46). The recognition heuristic “makes inferences about criteria that are not directly accessible to the decision maker; it exploits the basic psychological capacity for recognition in order to make inferences about unknown quantities in the world” (Gigerenzer and Goldstein, 2011, p. 101).

Regarding the significant characteristics of heuristics, some summary points developed by Gigerenzer and Gaissmaier (2011) as follow (p. 474):

- “Heuristics can be more accurate than more complex strategies even though they process less information.”
- “A heuristic is not good or bad, rational or irrational; its accuracy depends on the structure of the environment.”
- “With sufficient experience, people learn to select proper heuristics from their adaptive toolbox.”
- “Decision making in organizations typically involves heuristics because the conditions for rational models rarely hold in an uncertain world.”

Elimination by aspects, as a technique, is also “a heuristic followed by decision makers during a process of sequential choice and which constitutes a good balance between the cost of a decision and its quality (Laurent, 2006, p. 1). It is a “medium effort, attribute-based, non-exhaustive approach” (Hester, 2010, p. 45). “At each stage of decision, the individuals eliminate all options not having an expected given attribute, until only one option remains” (Laurent, 2006, p. 1).

Elimination by aspects “can be utilized to eliminate some sub-optimal alternatives early in the decision process; if we order our attributes in descending order of

importance, this approach is very useful in attaining a good choice quickly” (Hester, 2010, p. 45).

CHAPTER 3

ANALYSIS OF THE INCORPORATION OF EMERGENCY MANAGEMENT, AND PUBLIC SAFETY AND SECURITY

3.1 Introduction

Within the broad domain of Homeland Security, the Emergency Management concept plays a critical role for the conceptual design of the Homeland Security missions and functions. Following the foundation of the DHS, the development of Homeland Security concept was inspired from Emergency Management, which has addressed the `response activities` in the past.

In the last decade, since the terrorist acts of 9/11, parallel with the increase in the vulnerability of urban areas, myriad efforts, including public, state or private initiatives (policy/strategy development, legislation, academic research and activities, administrative regulations, exercises, etc.) have been made to enhance the national preparedness. These efforts incorporated the essence of the Emergency Management concept differently in their relevant studies under the oversight of the Homeland Security enterprise leaded by DHS.

Initial contextual analysis (conducted through the review of relevant literature, which comprises numerous governmental and public references) reveals an epistemological problem with the existing contextual structure of Homeland Security regarding the incorporation of the Emergency Management concept.

Furthermore, an examination of the ESFs which have been framed within the NRF (a critical mandate of Homeland Security domain) - through a holistic systems

thinking with post-disaster security centric focus - reveals that the conceptual design of the ESFs - particularly the ESF-5 and ESF-13 - also suffer from similar epistemological problems. These issues require the modification of contextual system design as well as the development of additional vulnerability assessment models to enhance the Public Safety and Security planning process.

In this regard, Chapter 3 analyzes the contextual architecture of Homeland Security regarding the incorporation of the Emergency Management concept, and Public Safety and Security within NRF according to the methodology delineated in Chapter 3.2. The analysis primarily focuses on the definitions and major components/phases of the concepts. (Comprehensive analysis of the whole context is beyond the scope of this dissertation.)

3.2 Analysis Methodology

Systems analysis “does involve finding the ‘best’ way to address the problem, or in mathematical terms ‘optimization’ among alternatives” (Keating, 2008), while systems thinking “includes holism, an ability to think about the system as a whole” (Weck et al., 2011, p. 190). Systems thinking “tries to understand the whole (system) and its parts (subsystems), the relations between the parts and the whole, and the relation of the whole with its context or environment” (Laszlo, 1998, p. 9). The utilization of holistic approach through systems of systems thinking is critical since it helps to avoid a Type IV error, which is to try to solve the problem with inappropriate, incompetent or insufficient tools, methodologies, and resources (Secilmis, 2012).

In the light of the systems thinking and holistic approach theories, the contextual analysis of Homeland Security regarding the incorporation of the Emergency Management concept, and the Public Safety and Security function within the NRF has been conducted based on the Contextual Analysis Methodology (CAM)⁵ depicted in Figure 15. The CAM is accomplished in six phases. Although it suggests a sequential flow throughout the analysis process, nonlinear interactions and information exchange could take place when necessary.

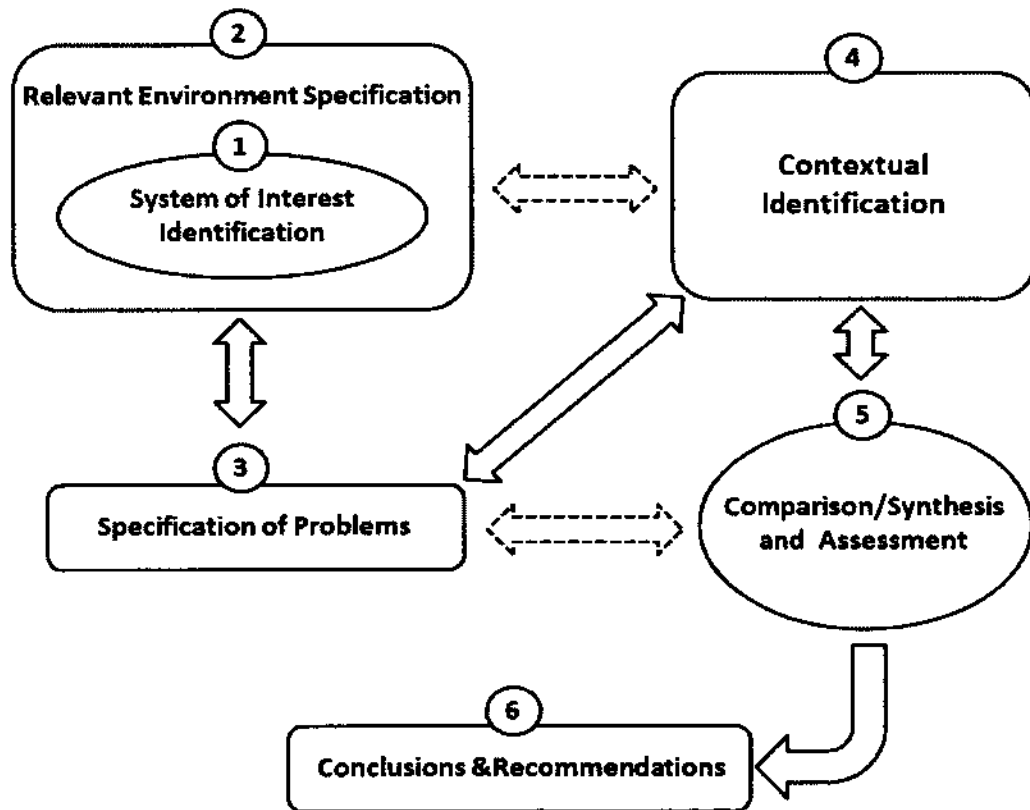


Figure 15 Contextual Analysis Methodology

⁵ Contextual Analysis Methodology (CAM) has been developed mostly inspiring from the Keating's (2000) methodology for conducting analysis of system structure (p. 189).

3.3 System of Interest Identification (Phase 1)

Keating (2000) notes that “detailed analysis requires the system of interest is clearly identified; failure to identify the system for study can result in unnecessary ambiguities in further stages of analysis” (p.186). To point out the focus of this analysis, two corollaries (Table 5) have been developed based on the discussions in Chapter 1.2 (Problem Domain), since Chapter 1.2 has already clarified the system of interest that is to be addressed during the dissertation.

Table 5 Focus of the Analysis

Corollary 1	Incorporation of the Emergency Management concept within the Homeland Security contextual system design should be re-aligned contextually to enhance the resiliency and preparedness of the overall system, since the efficiency of both organizational and functional system structures strongly relies on the coherence in the contextual structure,
Corollary 2	Post-disaster security centric planning approach should be promoted within the National Response Framework to improve the reliability of security plans.

In line with these corollaries, the purpose of the analysis is to identify the major implications of contextual inconsistencies stemming from the inaccurate incorporation of the Emergency Management concept throughout many official documents, and to

evidence the significance of the Public Safety and Security function and post-disaster security centric planning approach within NRF.

3.4 Relevant Environment Specification (Phase 2)

This phase comprises the identification of wider system characteristics in a holistic approach which are external to the system of interest. “The relevant environment for a system is the set of entities and patterns external to the system that either have an influence on the system or are influenced by the system” (Keating, 2000, p.186). To avoid Type III error⁶, which refers to “muddled thinking, or solving the wrong problems precisely” (Secilmis, 2012), this phase should be considered seriously. In this vein, the theoretically relevant environment that influences the focal discussions of the analysis has been specified in the following paragraphs.

Emergency Management, as a profession, “did not exist 35 years ago” (FEMA Pub 1, 2010, p. 15); it “started slowly being recognized after the Disaster Relief Act of 1974” (McEntire, (n.d.), p. 12). Today, Emergency Management plays a critical role for the accomplishment of other Homeland Security missions. However as Blanchard (2007) has discussed, it contextually resides in an erratic structure:

Emergency Management in the U.S. is very much conditioned and constrained by the various contexts within which it must function. It operates within the changing intergovernmental system. The “power relationship” amongst these levels of government has shifted over time when it comes to hazards, disasters, emergency management, and now homeland security. (p. 23)

⁶ Mitroff (1998) discusses five basic types of Type III Error. Each type represents a different sense but they are not independent:

- Picking the wrong stakeholders
- Narrowing one's options
- Picking the wrong language of variables
- Narrowing the boundaries/scope of a problem
- Ignoring parts/systems connections

Emergency Management belongs to a contextual domain where numerous concepts have linked to each other. While Blanchard (2007) contends that Emergency Management is not synonymous with Homeland Security, the National Incident Management System (2008) discusses that Incident Management refers to how incidents are managed across all Homeland Security activities, including prevention, protection, and response, mitigation, and recovery (although the aforementioned activities theoretically address the components Emergency Management). On the other hand, the Post-Katrina Act (2006) ascribes a broad governmental functional role to Emergency Management, which almost covers all mission areas of Homeland Security.

While the *Bridging the Gap* (2010) report defines Emergency Management as a subset of the Incident Management, the *National Incident Management System* (2008) articulates that NIMS has been built on the foundation provided by existing emergency management and incident response systems. Furthermore, the National Emergency Management Agency (NEMA) follows totally a different approach defining Emergency Management and Disaster Management as synonymous concepts: “the discipline of dealing with and avoiding risks, particularly those that have deleterious or catastrophic consequences for communities, regions, or entire countries” (*What is Emergency Management*, (n.d.)).

Regarding post-disaster security centric planning, the relevant environment that virtually surrounds post-disaster security also stays within the boundaries of Homeland Security. The Public Safety and Security function, which addresses the security requirements to be fulfilled during an emergency, has been designed within NRF as it is one of the conceptual pillars of Homeland Security.

Security “enhances freedom of action by reducing friendly vulnerability to hostile acts, influence, or surprise” (Joint Operations, 2011, A-3). “The ultimate goal of security operations is to protect the force from surprise and reduce the unknowns in any situation. Security operations encompass five tasks; screen, guard, cover, area security, and local security” (Offense and Defense, 2012, p. 5-3).

“The security sector consists of both uniformed forces—police and military—and civilian agencies and organizations operating at various levels within the operational environment. Elements of the security sector are interdependent; the activities of one element significantly affect other elements” (Figure 16) (Stability Operations, 2008, p. 6-13).

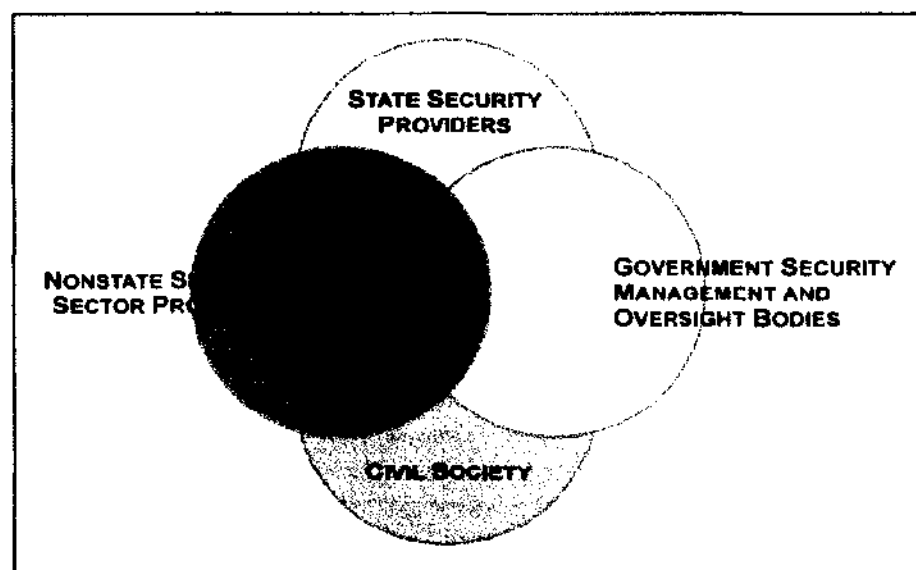


Figure 16 Elements of the Security Sector (Stability Operations, 2008)

From the holistic perspective of Homeland Security, there are two major target audiences in the existing security paradigm: people and assets. As its name implies, the ESF 13 (Public Safety and Security) has been designed within the NRF to ensure security

and protection for both audiences. The Public Safety and Security support function provides “the conduit for utilizing and incorporating the extensive network of public safety and security coordination established for steady-state prevention efforts through a variety of interagency plans” (Emergency Support Function 13, 2008, p. 2).

3.5 Specification of Problems (Phase 3)

The problems which address the discrepancies in the contextual layer of the ‘System of Interest’ are identified during this phase in accordance with implications derived from the ‘Relevant Environment Specification’ phase. However, substantiation of the problems as valid findings still requires evaluations and assessments that are to be performed in the 5th Phase (Synthesis and Assessment). This phase is considered as critical since its outcomes would navigate the rest of the analysis process. Therefore, “enough time should be allocated for the identification of system problem in the beginning of analysis” (Secilmis, 2012).

With the System of Interest and Relevant Environment of the problem domain identified and the focus of the analysis summarized with corollaries stated in Chapter 3.3, the synopsis of the analysis problems to underline the background motives of the analysis is as follow:

- Incorporation of Emergency Management concept within the extensive contextual structure of Homeland Security shows epistemological problems with numerous discrepancies.
- Conceptual design of the ESFs within the NRF has similar problems, and existing urban area Public Safety and Security planning processes

have not been supported by the methodologies which address post-disaster security requirements.

In this phase, as a part of the technique adopted by this methodology (CAM), the analysis regarding the incorporation of Emergency Management has been expanded with citations from different references providing specific background information explicitly.

The citations have been clustered into two groups in Appendix A:

- General and Coordination Issues
- Poor Policy Formulation (Epistemological Problems) and Lack of Training

3.6 Contextual Identification (Phase 4)

Keating (2000) contends “every structure must operate within a context, and in effect; context provides both constraint and facilitation to the operational structure” (p. 188). In that sense, the contextual and organizational structures of a system have an inextricable link to each other and this link directly affects the viability functions of the system. A coherent context allows a well-designed, reliable organizational system structure that eventually yields properly running system functions.

During the analysis, a rational mixture of holistic and reductive approaches should be employed to explore the context of the whole system as well as to identify the problems precisely (Secilmis, 2012). To that end, Phase 4 is dedicated to identification of the substantial data reviewing through the references that constitute the contextual structure of the problem domain (utilizing the data triangulation process: gather-analyze-

refine. See Chapter 4.8 for further information). The captured data would support the assessments which are to be made during the 5th phase (Synthesis and Assessment).

3.6.1 Emergency Management within the Homeland Security Contextual Structure

The evolution of Emergency Management in the context of Homeland Security has moved along with the development of the Homeland Security concept. Having already discussed previously, the incorporation of the Emergency Management concept within the different layers of the Homeland Security system design lacks contextual coherence with numerous discrepancies. During the evolutionary process, the notion and principles of Emergency Management have been adapted differently in numerous documents without epistemological consistency. This course has catalyzed the production of different terms and definitions, which are mostly used interchangeably.

Particularly, when capstone documents like NIMS, NRF, QHSR, DHS Strategic Plan, etc. are reviewed comparatively, the take-away is too fuzzy either to appreciate the exact role of Emergency Management in the DHS Integrated Strategic Framework⁷ or to make a clear distinction between the contents of the definitions of Emergency Management and other concepts - Homeland Security, Incident Management, Disaster Management, Crisis Management, National Preparedness. In a similar vein, the discussion of McEntire (2004) underlines this confusion:

Another way to foster the theory is to seek an alternative name for the field of emergency management. There are many possibilities being discussed including disaster management, risk management, sustainable hazards management or disaster vulnerability management. While it is doubtful

⁷ DHS Integrated Strategic Framework has been illustrated in DHS Strategic Plan (2012, p. A-3) without including any explanatory information which would help the interpretation of this figure. It is contended that this framework represent an ill-designed system architecture since the logic behind its design plan is blurry and does not match with facts of the historical development process of Homeland Security which have delineated in the relevant documents.

that the term emergency management will disappear because of its increased recognition in recent years, scholars should at least make explicit the drawbacks of continuing to rely on this name for the discipline. (p. 9)

In the following paragraphs, the concepts of Homeland Security, Incident Management, Disaster Management, Crises Management, National Preparedness and Emergency Management are explored (to elaborate similarities and distinctions to be considered in the following phase - Synthesis and Assessment). This is completed through literature review with regard to definitions and major components/phases, since the Homeland Security theoretical constellations, which constitute the contextual structure, have been clustered around these overarching concepts.

Homeland Security⁸

Homeland Security is “a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur” (National Strategy for Homeland Security, 2007, p.3). Homeland security “describes the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border control, and immigration” (Quadrennial Report, 2010, p. viii).

Incident Management⁹

Incident Management is “the broad spectrum of activities and organizations providing effective and efficient operations, coordination, and support applied at all

⁸ For further information about Homeland Security concept see Chapter 2.2.1.

⁹ For further information about NIMS see Chapter 2.2.3.

levels of government” (*National Incident Management System*, 2008, p. 140). Incident management “includes measures and activities performed at the national level and includes crisis and consequence management activities” (Homeland Security, 2005, IV-7).

Origination of NIMS dates back to 2003. On February 28, 2003, Homeland Security Presidential Directive 5 (HSPD-5) - Management of Domestic Incidents, directed the Secretary of Homeland Security to develop and administer a national incident management system (*Fundamentals of Emergency Management*, 2011).

The NIMS framework “sets forth the comprehensive national approach” (*National Incident Management System*, 2008, p. 5). “Originally published on March 1, 2004, the NIMS document was revised in 2008 to reflect contributions from stakeholders and lessons learned during recent incidents” (*National Incident Management System*, 2008, p. 4).

Civil Support Operations (2010) defines the NIMS as it “establishes the national approach for incident management across local, state, and federal levels (All types of emergencies and disasters generally are known as incidents)” (p. 2-1), while *National Incident Management System* (2008) makes a distinction between Emergency

Management and Incident Response:

Emergency management and incident response refer to the broad spectrum of activities and organizations providing effective and efficient operations, coordination, and support. Incident management, by distinction, includes directing specific incident operations; acquiring, coordinating, and delivering resources to incident sites; and sharing information about the incident with the public. (p.45)

Disaster Management

Disaster is “a crisis situation causing wide spread damage which far exceeds our ability to recover” (Thirunavukarasu, (n.d.)). Disasters “often strike with limited or no warning, and by definition they result in large-scale death, destruction, and mass hysteria; they often have long-lasting and large-scale economic, political, and psychological effects” (Mener, 2007, p. 3). McEntire and Marshall (2003) contend:

Disasters are qualitatively distinct from accidents and emergencies. First responders are required for small incidents, while their efforts are supplemented and superceded by those of emergency managers in larger disasters. Therefore, first responders are not emergency managers, although they are certainly important participants in emergency management. Emergency managers, on the other hand, are really disaster managers. (p. 122)

Regarding the management of disasters, Thirunavukarasu (n.d.) defines 5 phases in a disaster management cycle - Disaster phase, Response phase, Recovery/ Rehabilitation phase, Risk Reduction/ Mitigation phase and Preparedness phase. Disaster Management (Emergency Management) is “the discipline of dealing with and avoiding risks, particularly those that have deleterious or catastrophic consequences for communities, regions, or entire countries” (What is Emergency Management, (n.d)).

Crisis Management

Johansson (2010) discusses Crisis Management in the context of Emergency Management: “Crisis Management is normally divided into four main phases; mitigation (also referred to as prevention), preparedness, response and recovery” (p. 13); while Joint Publication 3-26 focuses on Crisis Management underlining the significance of Law Enforcement: “Crisis Management is predominantly a law enforcement response and in

such cases involves measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism under federal law”

(Homeland Security, 2005, IV-8).

The relationship between Crisis Management and Consequence Management¹⁰ has been depicted in Figure 17. The pinnacle of the pyramid represents the starting point of the response activity. While the control of the initial phases is dealt with through Crisis Management, the control of the final phases is overtaken by the Consequence Management, and Law Enforcement is the most critical mission at the very beginning of the response activity.

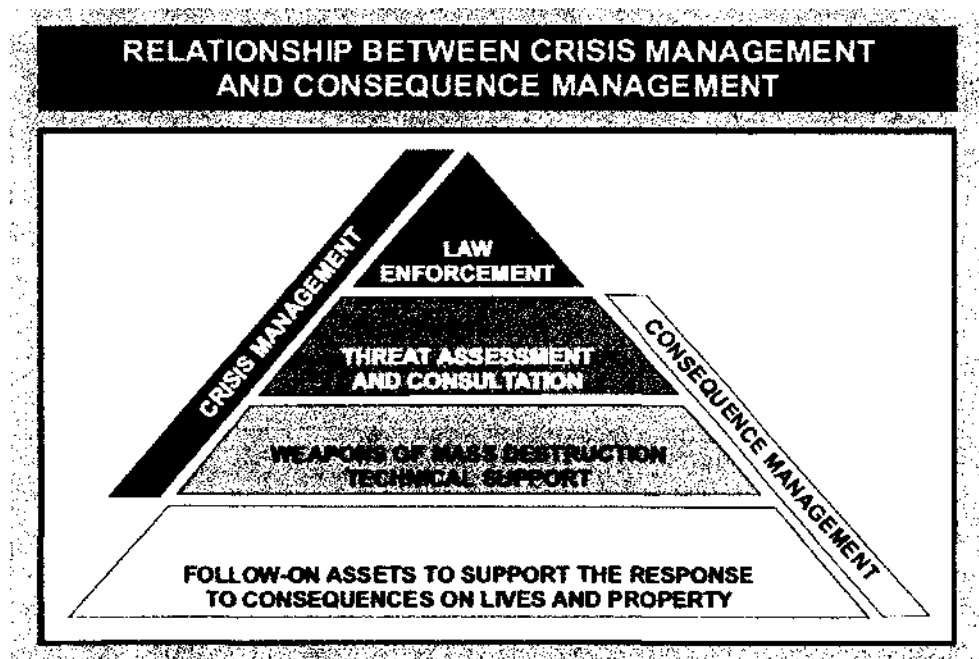


Figure 17 Relationship between Crisis Management and Consequence Management
(Homeland Security, 2005, IV-8)

¹⁰ Consequence Management includes the actions required to manage and mitigate problems resulting from disasters and catastrophes. DHS/FFMA has the primary responsibility for coordination of federal Consequence Management assistance to state and local governments (Homeland Security, 2005, IV-8, 9).

National Preparedness

Preparedness “is the range of deliberate critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents” (National Infrastructure Protection Plan, 2006, p. 104). “Within the National Incident Management System, preparedness focuses on the following elements: planning; procedures and protocols; training and exercises; personnel qualification and certification; and equipment certification” (National Incident Management System, 2008, p. 145).

Contextually, ‘Preparedness’ is usually defined as one of the four historical mission areas of Emergency Management; however, as Blanchard (2007) has discussed, sometimes it has been linked to ‘Emergency Preparedness’:

The Disaster Relief Act of 1974 described the conditions under which the President could request assistance for emergencies and disasters. In the 1978, National Governors Association (NGA) issued Emergency Preparedness Project Final Report, which defined four phases for Emergency Preparedness - Mitigation, Preparedness, Response and Recovery. (p. 18)

In 2003, HSPD-8 defined the term “preparedness” as it “refers to the existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from major events” (National Preparedness, 2003). The Presidential Policy Directive (PPD-8) dated 2011, provided a ‘National Preparedness’ definition which matches with the context of Emergency Management as well as the Homeland Security domain as an overarching context:

National Preparedness refers to the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent,

protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. (National Preparedness, 2011, p. 5)

Emergency Management

An emergency is “a situation featuring one or several abnormal events in the behavior of a system, if the system in question cannot be brought back to normal operation by normal routine procedures only” (Gheorghe, Vamanu, 1996, p. 7).

Emergency is “any incident, whether natural or manmade, that requires responsive action to protect life or property” (Fundamentals of Emergency Management, 2011, p. 2-13).

“Emergencies take many forms; they can involve any combination of consequences stemming from technological and man-made hazards, natural disasters, internal disturbances, energy and material shortages, and attack” (Comprehensive Emergency Management, 1979, p. 12).

Baird (2010) contends “the widespread use of ‘mitigation, preparation, response, and recovery’ to help describe ‘Comprehensive Emergency Management’¹¹ is the result of work by the National Governors’ Association (NGA) in the late 1970s” (p. 2). The original NGA description states: “following the establishment of FEMA, the activities and objectives of federal, state, and local emergency management activities in the United States have been based on a ‘comprehensive emergency management model’ divided into four phases: mitigation, preparedness, response, and recovery” (Hidek, 2010, p. 210), and “the federal government acknowledged that emergency management included mitigation,

¹¹ The ‘comprehensive’ aspect of Comprehensive Emergency Management (CEM) includes all four phases of disaster or emergency activity: mitigation, preparedness, response, and recovery, and it applies to all risks: attack, man-made, and natural, in a federal-state-local partnership (Comprehensive Emergency Management, 1979, p. 11).

preparedness, response and recovery activities and Emergency management was slowly being recognized as a profession” (McEntire, (n.d.), p. 12).

In 2006, the Post-Katrina Emergency Management Reform Act (PKEMRA) provided the following Emergency Management definition which has been discussed during this analysis as an important catalyst of the epistemological problems:

Emergency Management is the governmental function that coordinates and integrates all activities necessary to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other man-made disasters. (p. 1394)

In *Fundamentals of Emergency Management* (2011), a FEMA document, Emergency Management has been defined as “the managerial function charged with creating the framework within which communities reduce vulnerability to hazards and cope with disasters. Emergency management key components include; Prevention/Protection, Preparedness, Mitigation, Response and Recovery” (p. 4.2), while NEMA has provided the following Emergency Management definition which is considered synonymous with the Disaster Management:

Emergency management (disaster management) is the discipline of dealing with and avoiding risks, particularly those that have deleterious or catastrophic consequences for communities, regions, or entire countries. Focus on mitigation, preparedness, response, and recovery. Effective emergency management relies on integration of emergency plans at all levels of government and non-government. Activities at each level (individual, group, community) affect other levels. (What is Emergency Management, (n.d))

Emergency Management has also been defined within the NRF as an ESF:

Emergency Management (ESF-5), which is one of the Emergency Support Functions within the National Response Framework, is responsible for supporting overall activities of the Federal Government for domestic incident

management. It is organized in accordance with the National Incident Management System (NIMS). (Emergency Support Function 13, 2008, p. 1)

Furthermore, in *Fundamentals of Emergency Management* (2011), a categorization for Emergency Management activities has been included: “there are two ways to categorize emergency management activities; Emergency management core functions and Emergency management program functions. Emergency management core functions are performed during emergencies while Emergency management program functions continue on a day-to-day basis” (Fundamentals of Emergency Management, 2011, p. 10-6) (Table 6).

Table 6 Emergency Management Core and Day-to-Day Program Functions (Fundamentals of Emergency Management, 2011)

Core Functions	Day-to-Day Program Functions
<ul style="list-style-type: none"> • Direction and control • Information Collection and Dissemination • Communications • Warning • Emergency public information • Evacuation (or in-place sheltering) • Mass care • Health and medical • Resource management 	<ul style="list-style-type: none"> • Laws and Authorities • Risk Analysis • Hazard Mitigation • Resource Management • Planning • Direction, Control, and Coordination • Communication and Population Warning • Operations and Procedures • Logistics and Facilities • Training • Exercises, Evaluations, and Corrective Actions • Public Education and Information • Finance and Administration

Lastly, Emergency Management has also been considered as an integrated effort, and a subset of incident management as delineated in the following excerpts:

Emergency Management is the risk-based coordinated and collaborative integration of all relevant stakeholders into the four phases of emergency management (mitigation, preparedness, response and recovery) related to natural, technological, and intentional hazards. Its framework is both top-down as well as bottom-up – meaning that the theory and practice of emergency management has been significantly shaped by contributions from all levels of government. (Blanchard, 2007. P. 10)

Emergency Management, as subset of incident management, is the coordination and integration of all activities necessary to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other manmade disasters. (Bridging the Gap, 2010, p. 106)

3.6.2 Public Safety and Security

`Public Safety and Security`, which includes law enforcement, public order, and physical protection of critical infrastructures and key assets in urban areas, has always been the primary focus for leading authorities and security agents during both ordinary/peacetime or crisis/wartime system states.

In a crisis in a highly populated urban environment (after high scale natural or man-made disasters), the security agents, on behalf of the law enforcement authority, are responsible for preventing panic and chaos, establishing security, maintaining law and order, and facilitating successful execution of other response/recovery missions. The police and military usually assume the primary response role to meet the aforementioned urban security requirements. Other state, public or private local agents are involved in response missions, when necessary.

Wigginton (2007) contends “traditionally, the mission of police is to protect life, prevent crime and maintain order” (p. 14); likewise, the military is supposed to have similar missions/responsibilities to support the police force by request. Buddelmeyer (2007) underlines the significant support of the military during Hurricane Katrina: “the federal military and National Guard response to Hurricane Katrina was both necessary and exceptional; Katrina demonstrated that no other organization maintains the manpower, resources, and capabilities necessary to execute large-scale disaster relief like the military” (p. 25).

In *Stability Operations* (Joint Publication) (2011), the elements of a stable state are introduced as “human security; economic and infrastructure development; governance and the rule of law” (p. I-2). Within the framework of Stability Operations, the end state conditions include the following (Stability operations, 2008, p. 1-16):

- A safe and secure environment
- Established rule of law
- Social well-being
- Stable governance
- A sustainable economy

In a similar way, regarding the rule of law, the ‘Law and Order Operations’ (2011) introduces three categories in terms of Law and Order measures:

Law and Order measures can be generally aligned within three categories; law enforcement, physical security, and crime prevention. They are most effective when conducted in a synchronized and integrated manner, producing a layered approach to security and Law Enforcement. The intent of Law Enforcement, physical security, and crime prevention measures are to prevent, detect, and respond to crime and criminal activity. (p. 3-7)

Within the boundaries of the stability paradigm, it could be postulated that Law Enforcement, Security and Public Order missions should be considered seriously during assessments performed to identify Public Safety and Security requirements, since all these missions have an inextricable link to each other as the security agents usually perform them in an integrated/interconnected fashion.

Secilmis2 (2012) discusses the significant role that Law Enforcement has in the continuum of post disaster recovery efforts in the wider context of Homeland Security. He contends that the lack of necessary Law Enforcement implementation could aggravate the crisis environment to chaos or anarchy; therefore, in the state of a post disaster environment, decision makers should confirm that they have necessary assets and reliable law enforcement plans to establish physical security and public order in the disaster area to assure that other disaster response/recovery efforts can be conducted smoothly.

In a similar way, Bowman (2000) underlines the significance of the Law Enforcement: "Law enforcement promotes the rule of law. The significance of this cannot be overestimated. Promoting the rule of law plays a key role in assuring them that they will eventually achieve stability" (p. 30).

Having resonated with the anterior discussions, it is assumed that any other response or recovery missions cannot be accomplished in a post-disaster environment where the Public Safety and Security mission fails. Considering that it may provide a wider insight for the discussions in the 5th phase of this analysis (Synthesis and Assessment), the criticality of the Public Safety and Security has been highlighted using the following metaphors depicted in Figure 18:

- **Metaphor 1**

Symbol: Circulatory System of Human Body.

Intriguing Question: How critical is the circulatory system for the viability of other human body systems?

- **Metaphor 2**

Symbol: Urban Area Road Network.

Intriguing Question: What is the significance of a road network for the continuation of daily critical routines in an urban area?

- **Metaphor 3**

Symbol: Skyscraper.

Intriguing Question: Is it technically possible to construct the upper stories of a skyscraper without building the first floor or foundation?

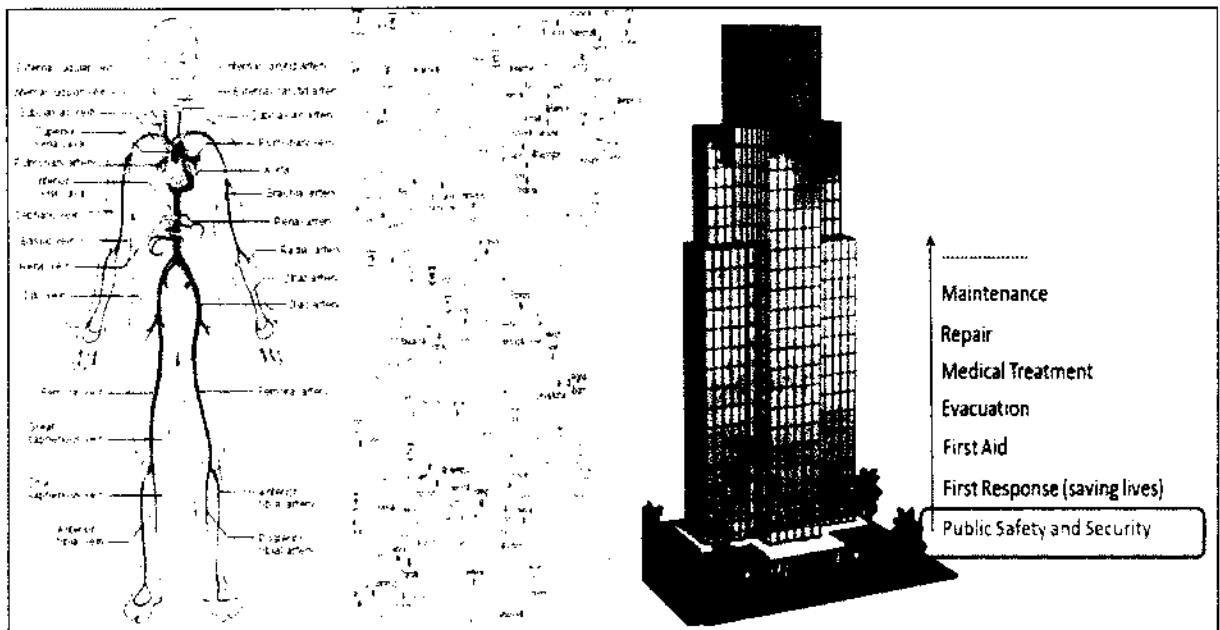


Figure 18 Public Safety and Security Metaphors (Circulatory System, Road Network, and Skyscraper Construction)

The following corollary could be postulated to signify these metaphors:

“Considering the execution of other follow-up response/recovery missions within the NRF, the Public Safety and Security mission, which directly links to Emergency Management and Homeland Security, is as critical as the circulatory system in the human body, as a road network in an urban area, and as building the foundation in a skyscraper construction.”

Public Safety and Security (Emergency Support Function-13)

In the U.S., Public Safety and Security as a response mission has been designed within the context of NRF, which stays in the domain of Homeland Security.

As discussed in Chapter 2.2.4; the NRF is “a guide to how the Nation conducts all-hazards response” (*National Response Framework*, 2008, p. 1). It establishes “a comprehensive, national, all-hazards approach to domestic incident response” (FEMA Pub 1, 2010, p. 12). It “builds upon the NIMS which provides a consistent template for managing incidents” (p. 1), and it is “comprised of the core document, the ESFs, Support, and Incident Annexes, and the Partner Guides” (*National Infrastructure Protection Plan*, 2009, p. 3). *National Response Framework* (2008) outlines the function of ESFs:

The ESFs serve as the primary operational-level mechanism to provide assistance in functional areas such as transportation, communications, public works and engineering, firefighting, mass care, housing, human services, public health and medical services, search and rescue, agriculture and natural resources, and energy. (p. 57)

Amongst these ESFs, ESF-13 (Public Safety and Security) provides “the conduit for utilizing and incorporating the extensive network of public safety and security

coordination established for steady-state prevention efforts through a variety of interagency plans” (Emergency Support Function 13, 2008, p. 2), and it further provides:

A mechanism for coordinating and providing Federal-to-Federal support; Federal support to State, tribal, and local authorities; and/or support to other ESFs, consisting of law enforcement, public safety, and security capabilities and resources during potential or actual incidents requiring a coordinated Federal response. (p.1)

3.7 Synthesis and Assessment (Phase 5)

This phase is dedicated to examination and interpretation of the data obtained through the previous phases as well as other sources from literature review. The outcomes of this phase may include the causes of contextual deficiencies and discrepancies, and further inputs for the determination of the potential solutions.

3.7.1 Incorporation of Emergency Management Concept

The Homeland Security enterprise represents an ultra-complex system of systems that assumes a tough responsibility to ensure the security of U.S. citizens within the borders of the homeland. The findings of the previous chapters have been synthesized and aggregated in this phase in a chronological order to assess the problem holistically in the different layers of the Homeland Security spectrum.

Starting with the Synthesis and Assessment phase, a brief summary of the analysis problem is highlighted in Table 7. As discussed in previous chapters, there are significant setbacks in the contextual evolution of the Homeland Security enterprise, regarding the incorporation of Emergency Management concept. These are mostly due to the lack of common understanding of Emergency Management definition and its components.

Table 7 A Brief Summary of the Analysis Problem

ANALYSIS PROBLEM
<p>The incorporation of the Emergency Management concept in the different layers of the comprehensive Homeland Security system design indicates epistemological inconsistency.</p>

“What is Emergency Management itself?” has been one of the challenging questions in this research. Since the principal focus of this analysis has been on the content of official capstone documents, the analysis inferences and conclusions would mostly be based on the data included in those documents. Having this caveat, there is very limited information in the official documents regarding the definition of the Emergency Management concept. This affirms the conclusion of Blanchard (2007): “there is not an established Emergency Management Doctrine” (p. 3).

Although there are diverse definitions and explanations in the public references, some auxiliary official documents which use the term Emergency Management interchangeably with Disaster Management (as in NEMA’s definition), Crisis Management, Risk Management and Incident Management; the capstone official documents, such as *Federal Emergency Management Agency Publication 1* (2010), *Fundamentals of Emergency Management* (Independent Study 230.b. FEMA) (2011) and *National Response Framework* (2008) comprise the same definition which refers to *Post Katrina Emergency Management Reform Act* (PKEMRA) (2006) (see Page 75 for the PKEMRA definition).

Regarding the Emergency Management concept, the other type of information articulated in the official documents is the historical phases, components or missions of Emergency Management. While the content of the Emergency Management definition is mostly consistent in the principal official documents, which refer only to PKEMRA's definition (although PKEMRA's Emergency Management definition is theoretically conflicting with the definitional content of Homeland Security as it is elaborated in the next paragraphs), the phases or components of Emergency Management have been discussed diversely in numerous documents, with different sort of elements. Table 8 provides examples of the confusion about phases/components.

Table 8 Evolutional Adaption of the Emergency Management Phases/Components

<p>Comprehensive Emergency Management (CEM) includes all four phases of disaster or emergency activity (CEM, 1979)</p>	<ul style="list-style-type: none"> • Mitigation • Preparedness • Response • Recovery
<p>The purpose of the NRP is to establish a comprehensive, national, all-hazards approach to domestic incident management across a spectrum of activities including (NRP, 2004)</p>	<ul style="list-style-type: none"> • Prevention • Preparedness • Response • Recovery
<p>Incident management refers to how incidents are managed across all Homeland Security activities, including (National Incident Management System, 2008, p.5)</p>	<ul style="list-style-type: none"> • Prevention • Protection • Response • Mitigation • Recovery
<p>Key tasks related to the three phases of effective response are (National Response Framework, 2008, 27)</p>	<ul style="list-style-type: none"> • Prepare • Respond • Recover
<p>According to PKEMRA, FEMA leads and supports the Nation in a risk-based, comprehensive emergency management system of (FEMA Pub 1, 2010, p. 55)</p>	<ul style="list-style-type: none"> • Preparedness • Protection • Response • Recovery • Mitigation
<p>For the past 7 years, homeland security has rested on four key activities oriented principally against the threat of terrorism (Quadrennial Report, 2010, p.14)</p>	<ul style="list-style-type: none"> • Prevention • Protection • Response • Recovery
<p>Key components of Emergency Management (Fundamentals of Emergency Management, 2011, p. 4-2)</p>	<ul style="list-style-type: none"> • Prevention/Protection • Preparedness • Mitigation • Response • Recovery
<p>The national preparedness system shall include a series of integrated national planning frameworks, covering (National Preparedness, 2011, p. 3)</p>	<ul style="list-style-type: none"> • Prevention • Protection • Mitigation • Response • Recovery

In order to identify the grass roots causes of the epistemological problem, the evolution of the Emergency Management and Homeland Security concepts should be scrutinized in chronological order.

The starting point of the inquiry theoretically leads to the `Response` mission, which dates back to 1800s. *National Response Framework* (2008) elaborates the discussion:

Response doctrine is rooted in America's Federal system and the Constitution's division of responsibilities between Federal and State governments. Because this doctrine reflects the history of emergency management and the distilled wisdom of responders and leaders at all levels, it gives elemental form to the Framework. (p. 8)

Fundamentals of Emergency Management (2011) stated "the role of the Federal Government in disaster response has evolved throughout the past 200 years" (p.2-1). "As disasters have occurred in the United States, policies relating to emergency management have also been developed" (McEntire, (n.d.), p.11). Mener (2007) underlines the role of federal government in disaster response:

Throughout the 19th century and the early 20th century, disaster response was handled by the federal government on a case-by-case basis without any clearly defined system. The vast majority of incidents were handled by state and local authorities independent of federal involvement. When federal disaster management was necessary, the military was the primary coordinator and source of manpower. (p. 7)

Lindsay (2010) contends "the approach to disaster relief changed dramatically from 1950 to 1979, when it transitioned from a largely uncoordinated and decentralized system of relief to the current model, which is dominated by the federal government" (p. 21). "After the promulgation of the Disaster Relief Acts of 1950, the process of administering disaster relief was further shaped by the Disaster Relief Acts of 1966,

1974” (Lindsay, 2010, p.23); and in 1979, “President Jimmy Carter created the Federal Emergency Management Agency (FEMA) by executive order and Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 100-707), was passed in 1988. It was an amended version of the Disaster Relief Act of 1974” (McEntire, (n.d.), p. 12).

McEntire (n.d.) noted “in conjunction with Stafford Act, FEMA also established the Federal Response Plan in 1992 as a way to better coordinate the government’s reaction to disasters; it included the involvement of 28 federal agencies as well as the American Red Cross” (p. 12).

After the 2000s, the two significant milestone events, September 11th and Hurricane Katrina, seriously influenced the evolution of both Emergency Management and Homeland Security. Figure 19 depicts these milestone events and key elements of the evolutionary process of Homeland Security to provide a holistic view.

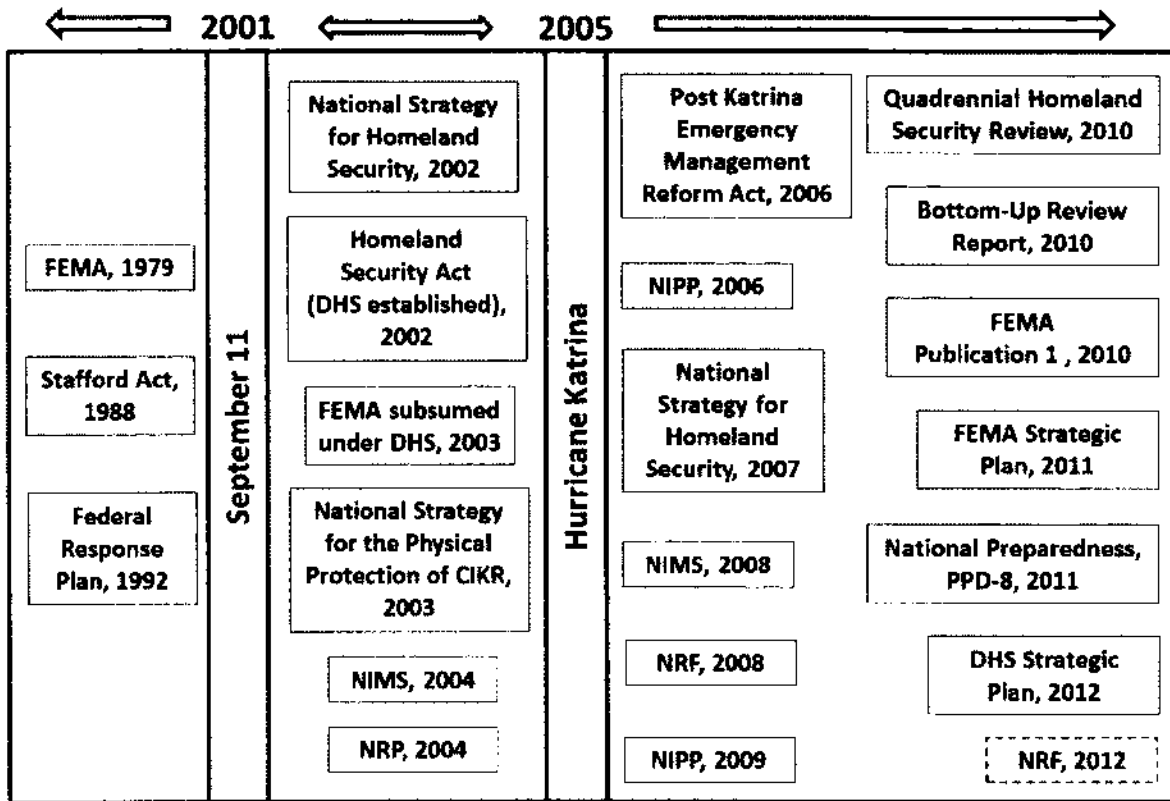


Figure 19 Key Elements of Homeland Security Evolution Process¹²

Pre-2001 Period

For the pre-2001 period, it is assumed that there was a common agreement for the definition and phases of Emergency Management, which referred to the guide of National Governors’ Association. In the ‘A Governor’s Guide’ which dated 1979, Comprehensive Emergency Management (CEM) was defined addressing the state’s responsibility and capability for managing all types of emergencies and disasters by coordinating the actions

¹² Homeland Security Presidential Directives (HSPD) could also be included in this context. NRF (2012) box with the dotted line represents the working draft document.

of numerous agencies. The “comprehensive” aspect of CEM included all four phases¹³ of disaster or emergency activity - mitigation, preparedness, response and recovery.

Period between 2001 and 2005

After the September 11 terrorist acts, DHS was established in 2002, and the National Strategy for Homeland Security (2002) identified three strategic objectives of Homeland Security, in order of priority and six critical mission areas:

The Strategic Objectives of Homeland Security:

- To prevent terrorist attacks within the United States;
- To reduce America’s vulnerability to terrorism;
- To minimize the damage and recover from attacks those do occur.

Homeland Security Critical Mission Areas:

- Intelligence and warning,
- Border and transportation security,
- Domestic counterterrorism,
- Protecting critical infrastructure and key assets,
- Defending against catastrophic terrorism,
- Emergency preparedness and response.

From a holistic perspective, while no direct reference has been attributed to the Emergency Management concept in the *National Strategy for Homeland Security* (2002),

¹³ “Following the establishment of FEMA, the activities and objectives of federal, state, and local emergency management activities in the United States have been based on a ‘comprehensive emergency management model’ divided into four phases – MPRR” (Hidek, 2010, p. 210). “The widespread use of “mitigation, preparation, response, and recovery” to help describe ‘Comprehensive Emergency Management’ is the result of work by the National Governors’ Association (NGA) in the late 1970s” (Baird, 2010, p. 2).

the three strategic objectives and six Homeland Security critical mission areas are based on the principals of four phases of Comprehensive Emergency Management (CEM) defined by the National Governors' Association. However, the focus of the strategy has been on terrorism as it is traced in its Homeland Security definition: "Homeland Security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur" (National Strategy for Homeland Security, 2002, p. 2).

During this period, Homeland Security and Emergency Management have been defined as an 'incident management discipline' by the *National Response Plan* (2004):

The NRP incorporates best practices and procedures from various incident management disciplines - homeland security, emergency management, law enforcement, firefighting, hazardous materials response, public works, public health, emergency medical services, and responder and recovery worker health and safety - and integrates them into a unified coordinating structure. (p. 2)

Post-2005 Period

After Hurricane Katrina, which was one of the nation's most destructive natural disasters, the evolution of the Homeland Security and Emergency Management concepts sailed towards a fuzzier context, creating some more epistemological problems. In 2006, the PKEMRA¹⁴ provided a contentious Emergency Management definition. The PKEMRA's definition aimed to mark the boundaries of Emergency Management in principle. However, since its content articulated an overarching concept addressing a broad mission spectrum, the new terminology theoretically could conflict with the

¹⁴ Nelson, Bodurian and McEvoy (2010) has contended "this legislation restored some of the agency's autonomy by reclassifying FEMA as a "distinct entity" within DHS, like the U.S. Coast Guard and Secret Service, and by prohibiting the transfer of FEMA resources to other DHS components" (p. 1).

domain of the Homeland Security, which was supposed to have the higher structural context.

Following PKEMRA, one year later, the *National Strategy for Homeland Security* (2007) kept up the same focus on terrorism as the *Strategy* of 2002 but also suggested a common framework by which the American nation should focus on the four goals to guide, organize, and unify the Homeland Security efforts (p.1):

- Prevent and disrupt terrorist attacks;
- Protect the American people, our critical infrastructure, and key resources;
- Respond to and recover from incidents that do occur; and
- Continue to strengthen the foundation to ensure our long-term success.

The *Strategy* of 2007 made no direct reference to the Emergency Management concept, as did the *Strategy* of 2002. However, the four goals in the *Strategy* of 2007 were built in the light of four traditional phases of Emergency Management.

The *National Infrastructure Protection Plans* (NIPP) of 2006 and 2009 included almost no detail about the Emergency Management concept, with one exception; NIPP (2006) referred to the *National Response Plan* of 2004 which had defined Homeland Security and Emergency Management as an 'incident management discipline.'

This was not the case for the NIMS and NRF, which were issued in 2008. These documents brought more epistemological inconsistency to the existing problem domain, although both adopted the same Emergency Management definition of PKEMRA (2006). Furthermore, NIMS (2008) provided another confusing interpretation, adapting the four traditional Emergency Management phases as the 'Homeland Security activities':

NIMS uses a systematic approach to integrate the best existing processes and methods into a unified national framework for incident management. Incident management refers to how incidents are managed across all homeland security activities, including prevention, protection, and response, mitigation, and recovery. (National Incident Management System, 2008, p. 5)

The new taxonomy of Homeland Security activities in the NIMS (2008) literally excluded the `preparedness` phase of traditional Emergency Management, but adding `prevention` and `protection.` Moreover, the brand new `three phases of effective response` taxonomy of the NRF (2008), which was the contemporary of the NIMS (2008), blurred the context a little more: “Key tasks related to the three phases of effective response are prepare, respond, and recover” (National Response Framework, 2008, 27).

In addition, the NIMS (2008) highlighted the need for focusing on improving Emergency Management, incident response capabilities, and coordination processes across the country due to the September 11 terrorist attacks and the 2004 and 2005 hurricane seasons; but the NRF (2008) incorporated Emergency Management as if it was only a part of ESFs within the NRF, although the definition of Emergency Management in the same document (NRF) linked to PKEMRA definition which was requesting more than that.

In the following years, the *Quadrennial Homeland Security Review* (QHSR) (2010) provided an extensive definition of Homeland Security which expanded its boundaries in comparison with the one defined in the National Strategy for Homeland Security of 2002 and 2007, putting a provident distance between its primary responsibilities and Emergency Management: “...In other areas, such as critical

infrastructure protection or emergency management, the Department’s role is largely one of leadership and stewardship on behalf of those who have the capabilities to get the job done” (p.iii).

QHSR (2010) also stated “for the past 7 years, homeland security has rested on four key activities—prevention, protection, response, and recovery—oriented principally against the threat of terrorism” (p. 14), and delineated the new homeland security missions:

1. Preventing terrorism and enhancing security;
2. Securing and managing our borders;
3. Enforcing and administering our immigration laws;
4. Safeguarding and securing cyberspace; and
5. Ensuring resilience to disasters.

Although the four key activities and the design of the missions in QHSR are similar to the foundational roots of Emergency Management, it directs the Emergency Management focus only to the 5th mission (Ensuring resilience to disasters) underlining the resiliency requirement to disasters:

The strategic aims and objectives for this mission are grounded in the four traditional elements of emergency management: hazard mitigation, enhanced preparedness, effective emergency response, and rapid recovery. Together, these elements create the resilience to disasters so necessary to the functioning and prosperity of this Nation. (p.31)

While QHSR directed the Emergency Management focus only to the 5th mission and particularly referred to four traditional elements of Emergency Management: hazard mitigation, enhanced preparedness, effective emergency response, and rapid recovery, the

capstone document of FEMA, Publication 1 (2010), contextually linked to the broader PKEMRA Emergency Management definition and five core missions of preparedness, protection, response, recovery, and mitigation: “According to PKEMRA, FEMA leads and supports the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation” (FEMA Pub 1, 2010, p. 55).

Fundamentals of Emergency Management (2011), which is the FEMA’s Independent Study 230.b., suggests five key Emergency Management components¹⁵ that include ‘prevention’, similar to what FEMA Publication 1 (2010) described before. Meanwhile, the *FEMA Strategic Plan* (2011) heads towards the shores of QHSR, which has a different perspective than *Fundamentals of Emergency Management* (2011), and *FEMA Publication 1* (2010).

In March 2011, the *Presidential Policy Directive* (PPD-8) ‘National Preparedness’ was issued with a revolutionary agenda and scope:

The directive has aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters. (National Preparedness, 2011, p. 1)

Although PPD-8 (2011) included early inferences and similar epistemologically inconsistent perspective regarding the incorporation of the Emergency Management concept within the architecture of the Homeland Security enterprise, it delivered significant Presidential Guidance, which has links to primary focus of this dissertation analysis:

¹⁵ Emergency management key components include: Prevention/Protection Preparedness Mitigation Response Recovery (Fundamentals of Emergency Management, 2011, p. 4-2).

This directive shall be implemented consistent with relevant authorities, including the Post-Katrina Emergency Management Reform Act of 2006 and its assignment of responsibilities with respect to the Administrator of the Federal Emergency Management Agency. (p. 5)

The term "national preparedness" refers to the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. (p. 5)

The national preparedness system shall include a series of integrated national planning frameworks, covering prevention, protection, mitigation, response, and recovery, and the frameworks shall be coordinated under a unified system with a common terminology and approach, built around basic plans that support the all-hazards approach to preparedness and functional or incident annexes to describe any unique requirements for particular threats or scenarios, as needed. (p. 3)

In February 2012, DHS issued its strategic plan which covered the fiscal years 2012-2016. The *DHS Strategic Plan (2012)* had been built on the design of the QHSR (2010), although the PPD-8 (National Preparedness) was promulgated in March 2011 with a different mindset. The *DHS Strategic Plan* also included a 'DHS Integrated Strategic Framework' (p. A-3) without any explanatory information. Although the framework provided a figurative holistic system representation, it was too fuzzy to clarify the role of Emergency Management and other functions/missions within Homeland Security in accordance with what the previous documents delineated before.

Finally, towards the end of this research, the working draft of 2012 NRF was still being staffed for approval. In one of the significant changes in this draft, the name of the ESF-5, which was 'Emergency Management' in 2008 NRF, was changed to 'Information and Planning' without any rationale to clarify how this framework incorporates the Emergency Management concept. Also, additional tables of 'core critical capabilities'

and 'critical tasks' have been added to draft, which could add more confusion. The following quote provides an insight about the design perspective of this framework:

The NRF is one element of the National Preparedness System mandated by PPD-8. The NRF describes how the Nation prepares to deliver the core capabilities established in the National Preparedness Goal for the Response mission area. The other mission areas defined by PPD-8 have corresponding frameworks that explain how the core capabilities established for those mission areas are delivered. (NRF - Working Draft, 2012, p. 46)

In conclusion, regarding the incorporation of the Emergency Management concept within the Homeland Security contextual structure, the following deductions could be posited:

- Considering the whole context, it could be inferred that the September 11 (2001) terrorist attacks and Hurricane Katrina (2005) disaster are the milestone events which framed the evolutionary process of Homeland Security, as well as Emergency Management.
- Before 2001, there is an overall consensus on the system of interest context, which links to the guide of National Governors' Association (1979).
- Between 2001 and 2005, although there is no specific reference to the Emergency Management concept in the official capstone documents, the conceptual design of the Homeland Security (particularly the objectives and critical mission areas), which were established after 2002, were founded on the principles of Emergency Management.
- After 2005, the PKEMRA's Emergency Management definition (2006) added to the epistemological hurdle within the overall contextual architecture. Although the PKEMRA's definition has aimed only to mark the

boundaries of Emergency Management in principle, its theoretical influence zone covered the domain of the Homeland Security, which is supposed to have the higher structural context.

- While the major theoretical conflict between Homeland Security and Emergency Management at the highest level distracted the whole system design, the divergent interpretation of the Emergency Management concept adopted within numerous Homeland Security key documents (like NIPP, NRF, NIMS, QHSR, FEMA Strategic Plan, PDD-8, etc.) has created an entangled ball of string.
- Although the *National Preparedness (PPD-8) (2011)* aimed to create an architecture based on a coordinated and unified system with a common terminology and approach, its content (when examined holistically in terms of definitions and components/phases of key concepts) is epistemologically inconsistent and fuzzy; and the recent working draft of *National Response Framework (2012)* is poised to be a major contributor to the existing epistemological complicity.

3.7.2 Public Safety and Security

The challenging aspects of the urban environment and emergent characteristics of diverse threats/hazards have been elaborated in Chapter 2.1 as they are the major components of the modern security paradigm. Today, we are more likely to live in an environment that is:

- Associated with densely populated urban areas, and more complexities representing different social, political and economic tensions.
- Dominated by emergent threats, which impose a broad spectrum of challenges that have ambiguous traits.

In a crisis system state, just after a catastrophic disaster like an earthquake or hurricane, what is called post disaster environment, the overall situation immediately gets more complicated with the involvement of numerous diverse interactions between the system elements. Deductive logic tells us that the characteristics of the security requirement will be more challenging because it would not be easy to deal with the post-disaster urban environment where the following characteristics dominate:

- Lack of power and other supplies
- Lack of communication
- Disorder
- Emergency
- Potential Threats
- Complexity
- Uncertainty
- Poor coordination

In the post-disaster urban environment, the Public Safety and Security function, including Law Enforcement, assumes a vital role for the facilitation of other follow-up disaster response/recovery activities in the wider scope of the Emergency Management

(Secilmis2, 2012). All disaster response/recovery activities, such as first response (saving lives), first aid and medical treatment, law enforcement, public order and security, evacuation, maintenance, repair, etc. should be executed coherently in a relatively secure and stable system state using a synchronized planning methodology. However, there is always high probability for having the states of crises ranging from the least to most, like 'chaos' or 'anarchy.'

In this demanding conjuncture, Homeland Security describes “the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border control, and immigration” (Quadrennial Report, 2010, p.viii). In the overarching domain of Homeland Security, the Public Safety and Security (ESF-13) which has been built within the context of NRF provides “a mechanism for coordinating and providing support; consisting of law enforcement, public safety, and security capabilities and resources during potential or actual incidents requiring a coordinated Federal response” (Emergency Support Function #13, 2008, p. 1).

Public Safety and Security (ESF-13) provides “the conduit for utilizing and incorporating the extensive network of public safety and security coordination established for steady-state prevention efforts through a variety of interagency plans. Prevention and security plans include, but are not limited to, the following” (Emergency Support Function #13, 2008, p. 2):

- National Infrastructure Protection Plan
- Sector-Specific Plans
- The National Strategy for Maritime Transportation Security

- Area Maritime Security Plans
- Vessel and Facility Security Plans

Finally, as underlined in the metaphors, the Public Safety and Security mission is highly critical. Lack of security on the scene could aggravate the crisis environment, letting it degrade to chaos or anarchy; in other words, other response or recovery missions cannot be accomplished in a post-disaster environment where the Public Safety and Security mission fails. In this sense, the lessons learned from Hurricane Katrina, which have been elaborated in Chapter 2.3, provide valuable insights to explore the discussion on the extent of Public Safety and Security, and underpin how any lack of security and law enforcement missions could severely impact the post-disaster response/recovery activities.

3.8 Conclusions¹⁶ (Phase 6)

There is a long history of outstanding achievements and great experiences in the U.S. regarding Homeland Security. As the Quadrennial Report (2010) states: “Homeland security draws on the rich history, proud traditions, and lessons learned from these historical functions to fulfill new responsibilities that require the engagement of the entire homeland security enterprise and multiple Federal departments and agencies” (p. 14). The established rules and experiences gained during the ‘disaster response’ endeavors have been evolved throughout the past 200 years. Due to the evolution of threats and hazards, the disaster relief efforts were finally institutionalized in the Federal level with the establishment of FEMA in 1979. It was during this period that “the federal

¹⁶ The recommendations pertinent to this analysis have been excluded from this chapter to be included in Chapter 5.

government acknowledged that Emergency Management included mitigation, preparedness, response and recovery activities and Emergency Management was slowly being recognized as a profession” (McEntire, (n.d.), p. 12).

Although it faced many challenges during its first years from 1979-2000s, “FEMA developed the Integrated Emergency Management System, an all-hazards approach based on preparedness, response, recovery, and mitigation, which provided direction, control, and warning systems common to the full range of emergencies from small, isolated events to the ultimate emergency – war” (FEMA Pub 1, 2010, p. 15), and a number of major reforms were initiated to streamline disaster relief and recovery operations.

From the 2000s up until now, the U.S. experienced two major milestone events that played a critical role on the evolution of U.S. Emergency Management concept. The first event was the September 11 terrorist attack which led the foundation of a brand new organization, DHS that would be responsible for security against terrorist acts. In 2003, FEMA was subsumed by DHS, while DHS kept its strategic focus on the threats emerging from the terrorist acts. The second event was Hurricane Katrina in 2005. After this devastating disaster, the 2006 PKEMRA was issued, including an Emergency Management definition and follow-up adjustments, which provided a broad spectrum for the maneuver of Emergency Management related concepts and activities. During this time, the Homeland Security mission was leaded by DHS in an overarching role that was supposed to integrate and coordinate all efforts and activities.

In this sense, nobody can underestimate the vigorous initiatives, and devoted efforts of the U.S. to sustain a high level of resiliency and preparedness against all type of

threats. However, from a holistic perspective, the Homeland Security contextual system design has serious discrepancies in terms of the incorporation of the Emergency Management definition and basic components/phases, as delineated in Chapter 3.7.1. Further, these discrepancies have the potential to hinder the expected overall coordination and coherence of the whole system architecture, which has numerous entities, missions and functions.

As Blanchard (2007) contends: “There is not an established Emergency Management Doctrine” (p. 3), which has been synthesized and well-defined particularly for the period after 2001 up until now. Moreover, during the evolution of Homeland Security, the adaption/interpretation of the definition and historical phases/components of the Emergency Management by different concepts in a different way has turned the overall contextual architecture into an enigma¹⁷ which indicates epistemologically ill-designed features.

In addition to the epistemological problems delineated in the analysis, the Homeland Security contextual system structure also suffers from the lack of holistic and reliable graphic/figurative system representations in a top-down approach, which is critical for the situational awareness¹⁸ of system stakeholders. Although there is a single example of holistic representation - DHS Integrated Strategic Framework - in the DHS Strategic Plan (2012, p. A-3), it is not clear enough to appreciate the incorporation of

¹⁷ Regarding the causes of some part of contextual problems, Hidek's (2010) excerpt highlights the potential impacts of disconnected, uncoordinated studies “...layers of statutes have been built upon existing guidelines without modifying previous statutes or reassessing the assumptions upon which they rest” (p. 253).

Situational awareness is a cognitive state that reflects the current, real-time understanding of an environment and its relation to pertinent goals (Gap Assessment Report, 2010, p. 3-12).

¹⁸ Situational awareness is a cognitive state that reflects the current, real-time understanding of an environment and its relation to pertinent goals (Gap Assessment Report, 2010, p. 3-12).

Emergency Management concept within the system framework in line with the discipline that consistently resonates with the historical evolution of Homeland Security as it has been articulated in the former references. Furthermore, there is no explanatory information associated with this annex, and it is contended that the missions, functions, priorities, etc. illustrated in this figure (in the context of Homeland Security) have been intermingled in a fuzzy logic.

Considering the whole problem domain, it has also been concluded that there are two major driving factors which have caused the existing context to be fuzzier and epistemologically more inconsistent:

- Evolving state of security environment which is being driven by challenging urban area characteristics and emergent nature of threats/hazards.
- The bulky scope of the Homeland Security enterprise.

The integration of impacts comprises a complex cluster of interactions between a vast number of interconnected, interdependent and independent elements, which should be the entities, functions, missions, goals, contexts, structures, etc. The potential for 'overwhelming complexity' emerges as the most significant challenge for the context development and management processes, which should be dealt with seriously.

Regarding the post-disaster security centric focus, security and law enforcement plays a critical role for the facilitation of other follow-up disaster response/recovery activities in the post-disaster urban environment. In the U.S. Homeland Security system architecture, the Public Safety and Security mission has been designed as an 'Emergency Support Function' within the NRF. However, the design mindset of this function in the

NRF is incompetent, and the instructions and guidelines provided in the existing Public Safety and Security (ESF-13) annex do not include necessary details, particularly in terms of interaction with the other ESFs, which would support the accomplishment of security missions in severe conditions like catastrophic post-disaster periods.

Although the criticality and vulnerability assessment of critical assets in an urban area (including critical infrastructures, facilities, state/public/private properties, etc.) has a significant impact on the post-disaster security planning process, there is no model in practice that provides an urban area critical asset prioritization methodology that specifically addresses the post-disaster urban security unique characteristics.

CHAPTER 4

POST-DISASTER SECURITY INDEX (PDSI) MODEL

4.1 Introduction

The Public Safety and Security function within the NRF plays a significant role for the execution other response/recovery missions under the overarching architecture of the Homeland Security enterprise. The NRF associated with NIMS and NIPP sets the policies/procedures and concepts of operations for the Public Safety and Security function, including the security of critical infrastructure and key resources. However, post-disaster security requirements are lacking and open to the incorporation of new mindsets and innovative approaches.

A significant part of the existing knowledge about urban area security (mostly the security related perspectives of the military doctrines) stays within the concept of Urban Area Operations. However, there is limited information (tactical level direction and guidance, criteria sets, techniques, methodology, etc.) in the military literature about how security agents should improve security plans to cope with the challenges, such as crisis in the post-disaster environment. In brief, decision making and prioritization requirements for force tailoring, unit positioning, identification of appropriate security operations techniques, etc. for a tactical unit that would be responsible for maintaining the security of an urban area in a post-disaster environment has not been elaborated categorically in the literature.

4.2 Requirement for Better Planning and Coordination

From the Homeland Security perspective, there are two major target audiences in the existing security paradigm: people and assets. Within the NRF, the ESF-13 (Public Safety and Security) was designed to ensure the security and protection of both audiences. In a post-disaster urban environment, the Police are the first echelon/tier responsible authority (to be supported by military and civilian security agents as necessary) for the coordination and execution of the Public Safety and Security mission. The NIPP (2009) is a critical initiative, which aims to provide the “unifying structure for the integration” (p. 1) of efforts to protect the critical infrastructures and key resources.

It is assumed that the requirement for security, law enforcement and public order in terms of the Public Safety and Security exponentially increases in the post-disaster urban environment, and excessive numbers of troop deployment are likely, as was the case during Hurricane Katrina in 2005. To accomplish the Public Safety and Security mission in a post-disaster urban environment, a successful security planning process should be completed in advance. During this planning process, the security assessments (vulnerability assessments and prioritization) for critical assets in a jurisdiction become important, since they would be required during any decision making process on the selection of optimal courses of actions for the security operations requirements, such as force tailoring, unit positioning, identification of appropriate security operations techniques, etc.

The assessment data provided through this process is also critical for both internal and external coordination requirements, as coordination activities play a crucial role in synchronous operations. In that vein, the Public Safety and Security operations will

require similar coordination activities in the post-disaster environment. To underline the significance of this coordination requirement between Homeland Security stakeholders, the dramatic difference between the military capability requirements in typical and catastrophic incidents is depicted in Figure 20. The figure implies that support troops deployed from adjacent regions or other locations in great numbers should be oriented by the local troops and pertinent authorities, and this means that an effective and comprehensive coordination effort will be required to achieve success during the security operations.

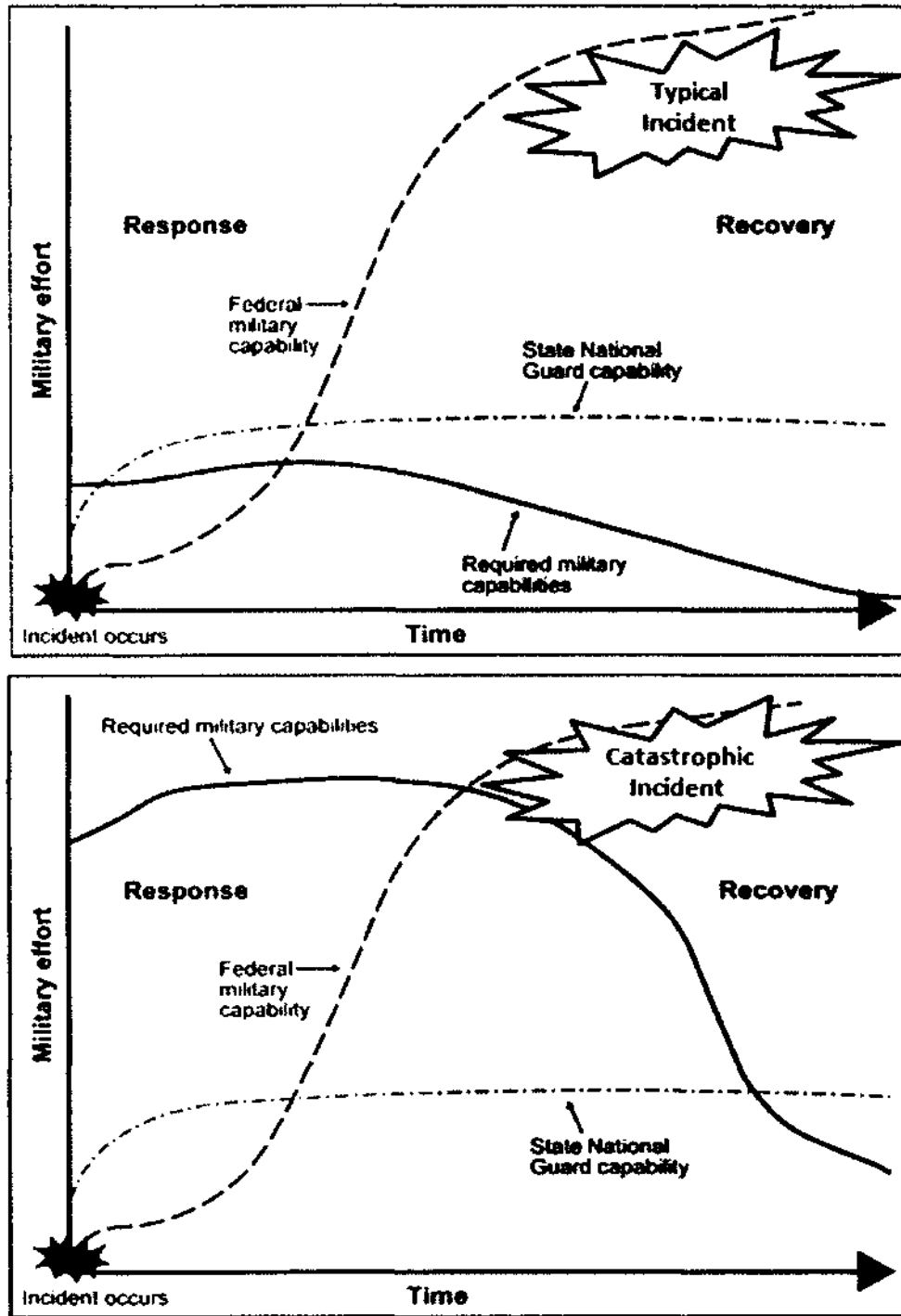


Figure 20 Required Military Capability in Typical and Catastrophic Incidents (Civil Support Operations, 2010)

Additionally, the National Guard response to Hurricane Katrina in terms of troop numbers in Figure 21 provides a spectacular illustration of how massive a response support troop deployment can be in a disaster area.

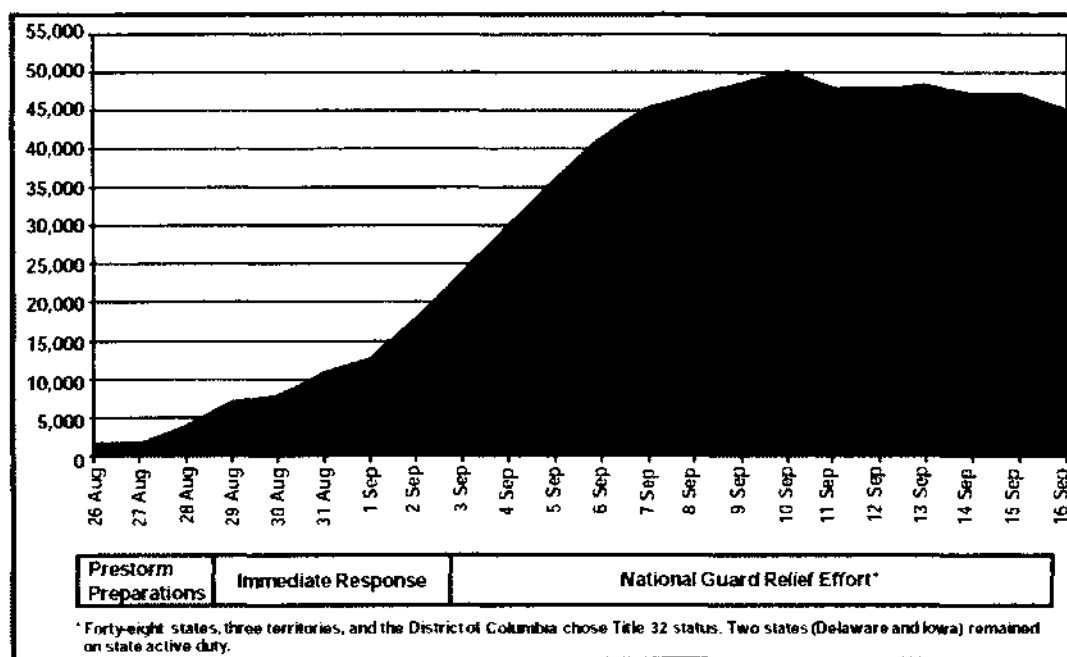


Figure 21 National Guard Response to Hurricane Katrina¹⁹ (Wombwell, 2009, p. 70)

After Hurricane Katrina, due to the severe impact of the storm and the lack of effective preparedness (mostly lack of pre-coordination of common supporting methodologies and advance exchange of necessary information), the execution of the Public Safety and Security missions failed early and further deteriorated the execution of other response and recovery missions in a domino effect. The following quotes highlight these facts:

¹⁹ When Hurricane Katrina hit, almost 6,000 National Guardsmen were on state active duty in Louisiana. Three days later, the number of Guardsmen in Louisiana doubled to more than 12,000 (Wombwell, 2009, p. 70).

Although the process successfully deployed a large number of National Guard troops, it did not proceed efficiently, or according to any pre-existing plan or process. There was, in fact, no established process for the large-scale, nation-wide deployment of National Guard troops for civil support. (Committee, 2006, p. 10)

While the military clearly provided vital support, no one had the total picture of the situation on the ground, the capabilities that were on the way, the missions that had been resourced, and the missions that still needed to be completed. (Pickup, 2006, p.3)

One thousand FEMA employees set to arrive in New Orleans on Wednesday, August 31, but turned back due to security concerns. (Select Bipartisan Committee, 2006, p. 249)

The security landscape of the post-disaster urban environment is exemplified by Hurricane Katrina in this dissertation, since it provided a plentiful number of lessons learned. However, as the discussion expands with different cases, the post-disaster security requirements still have much room for improvement. In addition, existing Public Safety and Security planning methodologies should be supported by different tools/models to provide more precise solutions for the security and coordination requirements.

New vulnerability assessment and prioritization models, which would process multiple criteria and different systems state variables for the critical assets, and produce generalizable indices for decision making requirements, should be developed to support the post-disaster security planning processes that theoretically should address the worst-case scenarios of the fuzzy post-disaster environment. This type of model would fully support the tactical level security agents in decision making and planning processes regarding force tailoring, unit positioning, identification of appropriate security operations techniques, etc. in the context of post-disaster security operations.

4.3 Existing Security Planning Practices

Before exploring the existing security planning considerations, the tactical aspects of the current security operations concept should be captured. To that end, Security Operations have been outlined at Appendix B. The protection of the population and critical assets is the top priority in post-disaster urban area security operations. There are different techniques available to security agents, as discussed at Appendix B. Four of these techniques – Patrol, Guard, ‘Intelligence, Surveillance, and Reconnaissance’ (ISR) and Response/Reaction Force - have primary roles in security operations. The concept of security operations is practically based on the execution of these techniques by troops assigned to area of responsibility. To elucidate the existing practice of security operations planning and execution, the following questions could be articulated:

- What are the methodologies being used to develop post-disaster security plans for urban areas?
- What kind of criteria is being utilized in these methodologies?
- Specifically, how are the force tailoring²⁰ and unit positioning²¹ decisions being made to allocate the optimal numbers of troops for the execution of security operations techniques (Patrol, Guard, ‘Intelligence, Surveillance, and Reconnaissance’ (ISR) and Response/Reaction Force, etc.)?

²⁰ Force tailoring refers to the process of determining and deploying the right mix of capabilities to support the force or mission. During Urban Operations, the sustainment commander can tailor the support element required to accomplish a specific mission or task, thereby mitigating the risk associated with deploying a larger, more robust capability package forward into the urban area (Urban operations, 2006, p.10-7) .

²¹ Unit positioning/Deployment refers to the positioning of forces into a formation for battle (DoD Dictionary of Military and Associated Terms, 2010, p. 105). Factors affecting base and unit positioning include the implications of the current threat assessment, the suitability and survivability of available facilities, and the subordinate unit mission requirements. Component commanders and their staffs should use these factors and their own risk assessments to determine whether units should be dispersed or grouped together for mutual support (Joint Security Operations in Theater, 2010, p. III-18).

Based on the information provided through literature review and interviews with the subject matter experts, the common approach to develop a security plan for an urban area hinges on the identification of critical assets within the area of responsibility, and follow-up criticality and vulnerability/threat assessments. Through various criticality and vulnerability/threat assessment methodologies, the decision makers can provide some security requirement parameters for each critical asset, and eventually a decision making process supported by different prioritization approaches could be executed for the organization and deployment of the available troops in term of `force tailoring` and `unit positioning`. Finally, with the identification of security operations techniques to be executed by the deployed troops in area of operation, the overall planning process is roughly completed.

As it has been stated in Police Intelligence Operations (2010), “there are numerous tools available to assess the criticality and vulnerability of a particular asset, and each of these tools has unique inherent strengths and weaknesses” (p. 5-17). However, there is no methodology or technique in place yet to provide a comprehensive approach that incorporates the complex characteristics of the post-disaster urban environment and diverse threat spectrum into its process design.

The argument can be traced through the NIPP as well as other tools available for the Police and Military. The Emergency Services Sector-Specific Plan (SSP)²² that is a part of the NIPP provides a sophisticated assessment and prioritization tool to address critical infrastructure protection. “The cornerstone of the NIPP is its risk analysis and

²² The Emergency Services Sector-Specific Plan (ES SSP) is an annex to the National Infrastructure Protection Plan (NIPP) and addresses efforts to improve protection of the ESS in an all-hazards environment (p. i). The ES SSP, in conjunction with the NIPP, provides the unifying Federal structure for the integration of Emergency Services Sector (ESS) critical infrastructure and key resources (CIKR) protection efforts into a single national program (Emergency Services Sector-Specific Plan, 2010, p. v).

management framework (Figure 22) that establishes the processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector risk” (National Infrastructure Protection Plan, 2009, p. 2).

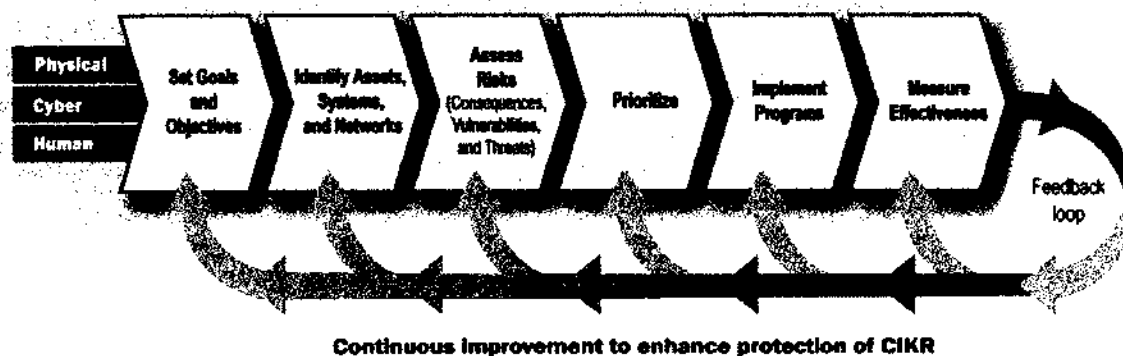


Figure 22 NIPP Risk Management Framework (National Infrastructure Protection Plan, 2009)

In this framework, the base element for the vulnerability component is the Enhanced Critical Infrastructure Protection (ECIP)²³ security survey, which resides in the Infrastructure Survey Tool (IST)²⁴ and utilizes the approved DHS Infrastructure Protection vulnerability methodology (Emergency Services Sector-Specific Plan, 2010). However, although the NIPP Risk Analysis and Management Framework and the other tools used in the ECIP program may provide outstanding capabilities for resource allocation decision processes, the employment of these tools to support the tactical level security planning processes is unlikely, since they do not adequately address the post-

²³ The Enhanced Critical Infrastructure Protection (ECIP) program is designed to assess risks to fixed facilities to compare - with risks to like facilities (Emergency Services Sector-Specific Plan, 2010, p. ii).

²⁴ The Infrastructure Survey Tool (IST) provides asset or facility based information from a wide range of CIKR facilities, such as commercial buildings, electrical substations, and dams (p. 5). It has more than 1500 variables covering 6 major components and 42 subcomponents (Fisher, Buehring, Bassett, Dickinson, Haffenden, Klett, and Lawlor, 2009, p. 9).

disaster aspects of the security paradigm from a perspective of security concept of operations as discussed in Appendix B.

In police security operations, the primary focus is on the practice of 'patrolling', which has a broad spectrum consisting of different types. The methodology for the development of patrol plans is usually shaped with inputs provided through numerous computer-based software applications that allow a wide range of applicable data to be overlaid, including demographic data, industrial hazard areas, sensitive assets, key traffic routes and congestion points, existing patrol and police station operational boundaries. They also allow security agents to overlay crime and incident data on a digital map of the Area of Operations (AO) as it is elaborated in Law and Order Operations (2011).

While existing planning approaches for patrol planning supported by aforementioned computer-based software applications enable security agents to enhance the security measures to some extent, they would not be sufficient to support the development of comprehensive security plans that integrate the execution of other necessary security operation techniques besides patrolling. Also, since existing methods mostly rely on historical crime data²⁵ without incorporating the ambient tensions and variables specific to each critical asset, the outcomes of plans developed through these methods would likely not be resilient enough to tackle the complexities of post-disaster urban environment.

²⁵ This data comes from historical records of criminal and other police and security-related activity, demographic data for the jurisdiction in question, seasonal and other cyclical events or activities, and areas of specific command emphasis (Law and Order Operations, 2011, p. 2-22).

In the context of the military security concept of operations; while patrol planning²⁶ has similar established practices like the police security operations, the security paradigm is usually managed through the principles of Military Decision Making Process (MDMP)²⁷ as it is a common approach applied for all military actions which requires the commander's decision at the appropriate level. However, there is also limited discussion in the military literature²⁸ regarding the identification of force tailoring and unit positioning requirements of the troops to be deployed in the post-disaster urban area. For these particular requirements, military references usually advice general approaches and techniques without providing specified direction and guidance, criteria sets, etc. as outlined in Appendix C. To deliver precise outputs, these approaches and techniques require elaboration thorough the decision making processes which relies on the decision makers' vision and personal capability.

In addition to primary approaches/methodologies employed within the context of the military decision making process (like METT-TC, OAKOC, IPB)²⁹ [see Appendix C

²⁶ Patrol areas and patrol distribution are methods used by Law Enforcement agencies to divide a jurisdictional area into manageable and organized subordinate areas for Law Enforcement personnel to conduct operations. Patrol distribution must consider, at a minimum, the following factors (Law and Order Operations, 2011, p. 2-22);

- Crime and complaint histories for the AO.
- Geography and characteristics of the AO, including;
 - Population and critical resource densities across the AO.
 - Obstacles and number of ingress or egress routes.
- Minimum response requirements.
- Manpower and mission requirements, including personnel available and mission loads.

²⁷ The military decision making process (MDMP) is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order . The military decision making process integrates the activities of the commander, staff, subordinate headquarters, and unified action partners to understand the situation and mission; develop and compare courses of action; decide on a course of action that best accomplishes the mission; and produce an operation plan or order for execution (The Operations Process, 2012, p. 2-11). Theoretically, decision making process (and the mission analysis within the decision making process algorithm) begins with the receipt of the mission and it is usually followed by the risk/threat/hazard assessment.

²⁸ The scope of the military literature research is limited to U.S. military literature.

²⁹ **METT-TC:** Mission, Enemy, Terrain and Weather, Troops and Support Available, Time Available, Civil Considerations.

OAKOC: Observation and Fields of Fire, Avenues of Approach, Key Terrain, Obstacles, and Cover and Concealment.

IPB: Intelligence Preparation of the Battlefield.

for further information excerpted from Urban Operations (2006)], the MSHARPP³⁰ and CARVER³¹ assessment techniques provide relatively advanced toolsets for the security planners as they are elaborated in Antiterrorism (2011). However, since both focus on terrorist threats, and their concept frameworks have not been designed to address the complex characteristics of the post-disaster urban areas, the use of those tools would not meet the post-disaster security planning requirements.

4.4 Conceptual Background of the PDSI Model

The concept design of the PDSI Model is derived from a combination of the epistemological perspective of modeling, Multi-Criteria Decision Making (MCDM), systems thinking and relevant aspects of the military literature including MDMP.

The essence of the PDSI Model relies on the realistic assumptions of post-disaster security, and mostly addresses the planning requirements for the deployment of the security agents (including both the local/state police and military forces and external support agents from adjacent regions or other locations as necessary) who are responsible for securing any urban area, and maintaining law and order after a catastrophic natural or man-made disaster.

Prescriptive research aims to provide a remedial solution as implied in its name.

Wollman (n.d.) further delineates what the prescriptive research is:

Prescriptive research comes up with an assertion, a solution, and a proposal for how to address a known problem space. The implication of most research questions in prescriptive research is what we should do now: how a policy should be changed or improved; how an organization can achieve specific outcomes or meet requirements; a set of recommendations or solutions or ideas that involve change and action.

³⁰ **MSHARPP**: Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity.

³¹ **CARVER**: Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognisability.

The PDSI Model has been developed through a prescriptive research methodology. Its foundational motives are based on the following three conclusions, which were derived from the literature review and analysis results delineated in previous chapters. The conclusions are:

Conclusion 1: Increasing complexity of urban environment and emergent characteristics of diverse threats (all types of natural and man-made threats) impose serious challenges to the post-disaster urban security.

Conclusion 2: Since the Public Safety and Security function plays a critical role for the execution of other follow-up disaster response/recovery missions in the context of the NRF, the security agents should ensure that they have reliable Public Safety and Security plans in place.

Conclusion 3: To maximize the efficiency, the Public Safety and Security plans should be developed utilizing appropriate tools and methodologies that can address post-disaster urban environment characteristics theoretically reflecting worst-case scenario features, such as lack of power and other supplies, lack of communication, disorder, emergency, potential threats, complexity, uncertainty, poor coordination, etc.

4.5 Significance of the PDSI Model

Regarding the existing practice of urban security operations planning, the criticality and vulnerability assessment of critical assets has a significant impact on the

planning of security operations techniques which are to be executed on the ground as necessary. Presently, a number of different tools are available for the security agents as discussed in the previous chapters. These tools are used to provide data for asset prioritization for different purposes as some of them support the decision making processes on resource allocation. However; from the tactical level security planning perspective, there is no model of an urban area critical asset prioritization methodology that employs both a multiple criteria decision making approach (like fuzzy sets for multiple system states), and criteria sets that specifically address unique post-disaster urban security characteristics.

To that end, the implementation of the PDSI Model would be valuable for urban area security planners, enhancing the quality of their post-disaster security plans, which also have critical implications for the continuation of other disaster response/recovery missions. With the conceptual background delineated in Chapter 4.4, the significance of the PDSI Model is outlined in the following three topics:

1. Since the security implications and vulnerabilities vary according to different system states, the model design has been built in a matrix form. So different grades of membership and indexes, which represent outcomes of different system states can be aggregated in a fuzzy sets approach.
2. Since the post-disaster environment has unique characteristics, the Criteria of Merit to be processed through the model have been developed based on realistic assumptions that address these unique features. In addition to comprehensive review and synthesis of the relevant literature, the decision tree analysis in Chapter 4.8 supports the validation of the criteria set.

3. The PDSI Model empowers a methodology that ensures generalizable indices with the incorporation of generalizability grades of membership for each Criteria of Merit, and each Possible System State. Therefore, the potential outcomes would be helpful at different levels in the planning processes in the wider context of the Homeland Security enterprise, as delineated in Chapter 5.

4.6 PDSI Model Algorithm

4.6.1 Introduction

The expected outcome of the PDSI Model is basically to provide an efficient vulnerability assessment tool for security planners who deal with post-disaster urban area security in the tactical level. In addition, the model's implementation would also likely to have operational and strategic level implications. The concept design and step-wise algorithm of the PDSI Model have been delineated in this dissertation. However, a software program supported by Geographic Information Systems (GIS) is still required for the practical use of the model in future. The PDSI Model includes five sequential components (Figure 23):

1. Identify Boundaries
2. Identify Critical Assets
3. Measure Basic Criticality Value (BCV)
4. Measure Post-Disaster Security Fuzzy Index (PDSFI)
5. Measure Post-Disaster Security Index (PDSI)

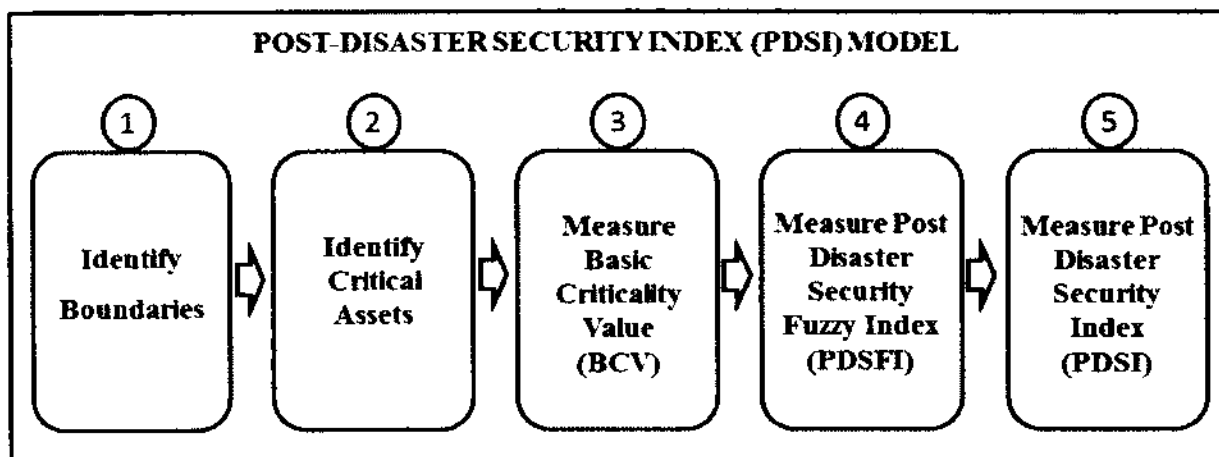


Figure 23 Components of the Post-Disaster Security Index Model

Before starting to explore each phase, note the basic assumptions outlined below for further appreciation of the implementation process:

- The model concept addresses the post-disaster urban area environment which has unique characteristics that are depicted, but not limited to those in Figure 24.



Figure 24 Unique Characteristics of Post-Disaster Urban Environment

- There are four major security operations techniques: Patrol, Guard, 'Intelligence, Surveillance, and Reconnaissance' (ISR), Response/Reaction Force.
- The security agents who are responsible for securing any area of responsibility (sectors/sub-sectors) in a jurisdiction utilize the outputs of this model to improve post-disaster security plans in terms of force tailoring and unit positioning as well as identifying the required security operations techniques to be executed on the scene.
- The model could be utilized for any urban area of responsibility (sub-sector, sector, district, city, state, etc.) as appropriate, and the outputs could be integrated/aggregated and interpreted in a bottom-up and top-down approach through various methods.

4.6.2 Identify Boundaries (Phase 1)

In the first phase of the PDSI Model, the areas of responsibility are identified in line with any existing administrative boundaries: e.g.; police districts³², patrol division sectors, etc. Different techniques could be utilized for this requirement, however a unified approach should be adopted for the whole interest area (as illustrated at Figure 25) to ensure the consistency and generalizable integration/aggregation inferences be derived for specific purposes.

³² After Hurricane Katrina, Emergency Support Function (ESF)-13 (the Public Safety and Security) requests were processed through the Law Enforcement Coordination Center (LECC) at Louisiana State Police (LSP) headquarters in Baton Rouge (Select Bipartisan Committee, 2006, p. 257). The LECC divided the federal law enforcement entities by New Orleans police districts. Each federal law enforcement agency was responsible for coordinating with the precinct captain of the district (Select Bipartisan Committee, 2006, p. 259).

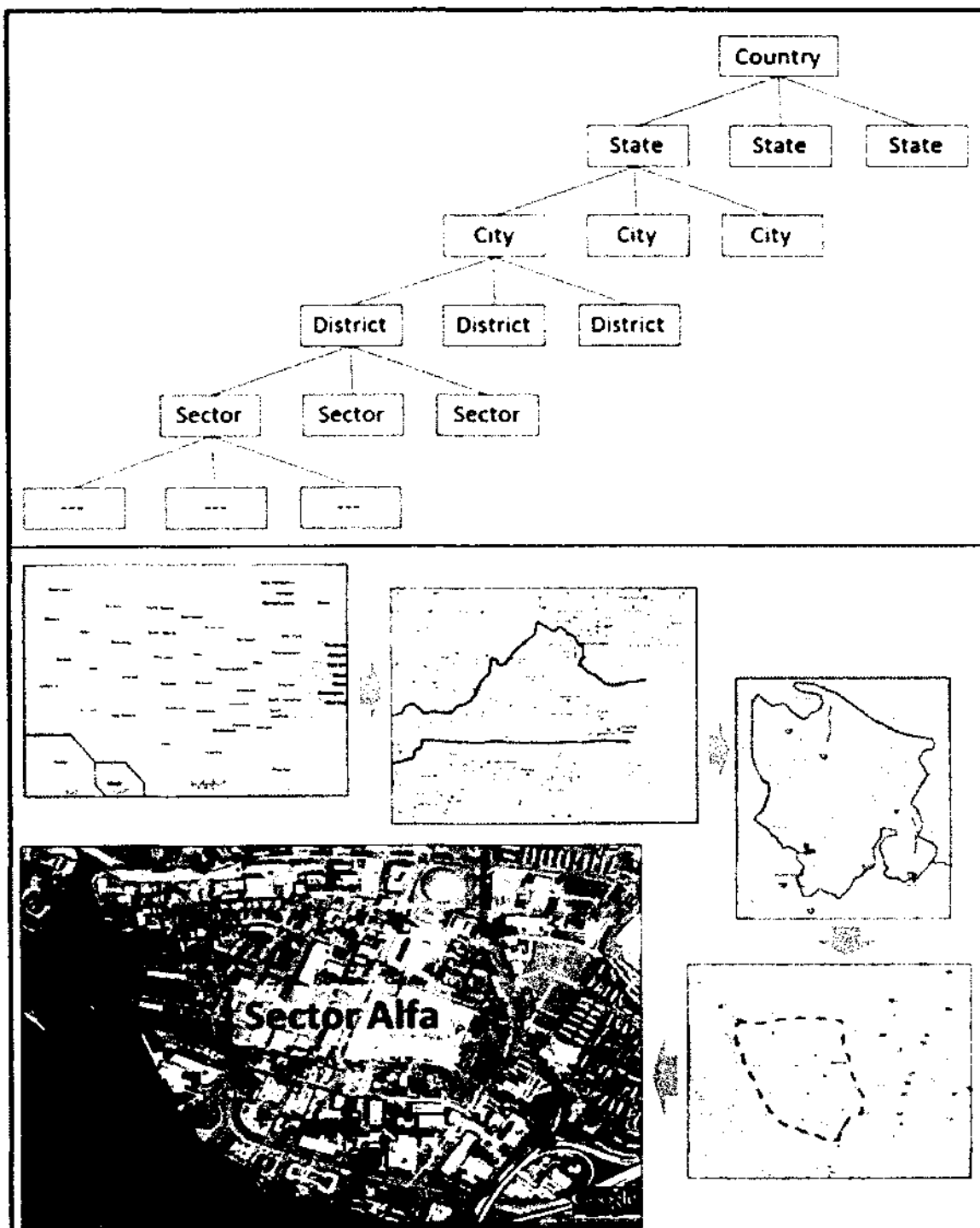


Figure 25 Identification of Boundaries (Subdivision of the Interest Areas of Responsibility)

4.6.3 Identification of Critical Assets (Phase 2)

Having clarified the boundaries, the critical assets (which include critical infrastructures, facilities, state/public/private properties, etc.) in each sector are identified with rough estimates, and enumerated (see an example at Figure 26). If it were technically possible, all the assets in the sector could be assumed as critical and enumerated accordingly. However, since it would be unfeasible to work with all assets in an urban area throughout the assessment process, the former instruction should be followed.

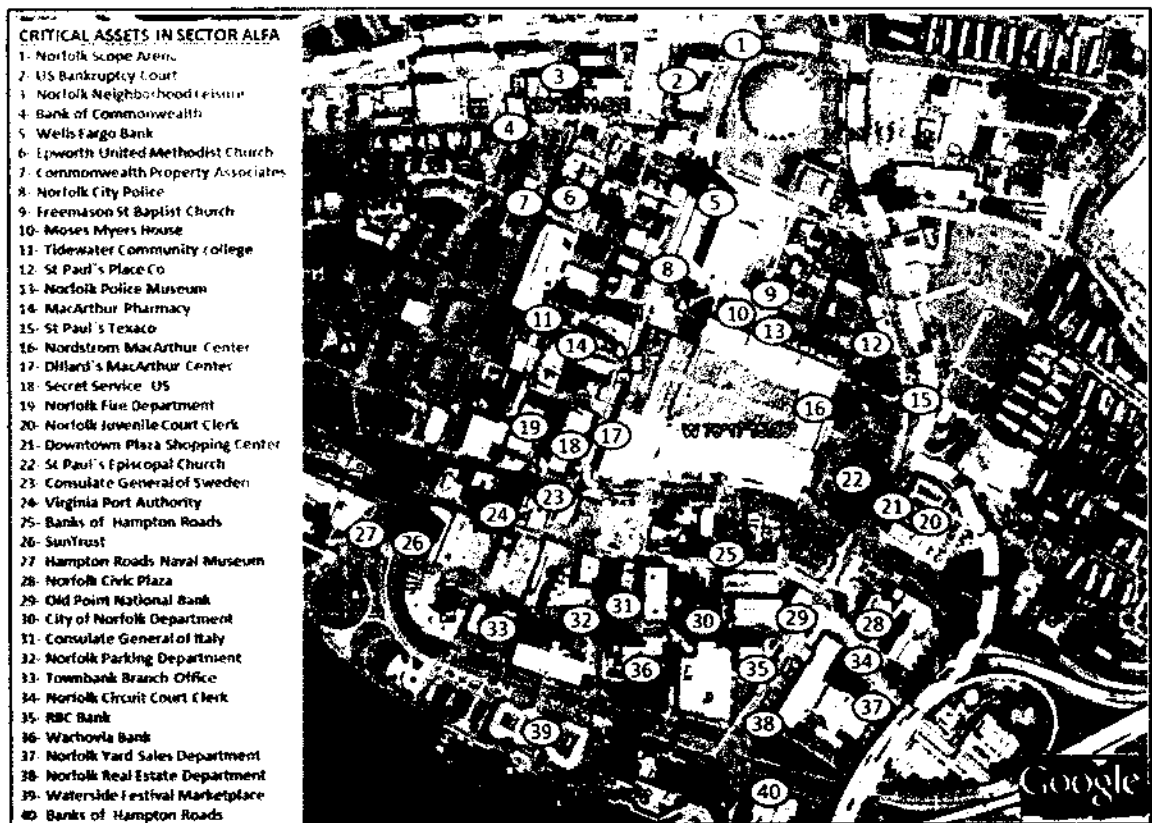


Figure 26 Identification and Enumeration of Critical Assets

Although the initial criticality identification could be made through either intuitive methods like Recognition Heuristic and Elimination by Aspects as discussed in Chapter 2.6.3 or any other methods to be performed by the subject matter experts, official guidance provided by local, state or federal authorities associated with the set of certain criteria and classifications defined within the appropriate margins would support optimal decisions and produce generalizable outputs.

As a guide for planning purposes, a list of the potential types of critical assets in an urban area is included in Table 9, which has been adapted from the list of the Critical Infrastructure and Key Resource Sectors (CIKR) (Table 1).

Table 9 Potential Types of Critical Assets

Power Plants
Governmental Buildings
Major Industrial Facilities
Banks/ATMs
Gas Stations
Major Retail
Shopping Malls
Hospitals
Schools
Places of Worship
Airports
Major Transportation Terminals
Highly Populated Buildings
Recreation Centers
Road Intersections (Traffic Control)
Possible Shelters-Post Disaster
Points of Distribution (POD)-Post disaster
Prisons

4.6.4 Measurement of Basic Criticality Index (BCI) (Phase 3)

Various asset criticality assessment methods can be used to produce a criticality index to be processed in the PDSI Model. However, the possible outcomes of these methods would address contextually different aspects as each of their conceptual designs has been built to achieve a different goal. Nevertheless, the criticality index provided through the Basic Criticality Index (BCI) Assessment Matrix (Table 4-4), which has been developed in line with the context of the PDSI Model, would adequately reflect the post-disaster urban environment characteristics considering the viability functions of the key sectors/services.

The function of the BCI is to normalize the Post-Disaster Security Fuzzy Index (PDSFI), which is to be produced in the next phase. The BCI, for each critical asset, is obtained through the equation included in the relevant key sector/service row at Table 10. It provides a score between 0 and 1 that reflects the relative functional weight of criticality of the assigned asset in terms of its level of involvement in the relevant sector/service group³³. However, the BCI does not reflect the post-disaster security requirements of the assigned assets. Rather, it addresses the criticality of assets in the system state of the post-disaster urban environment where the key sectors/services play a significant role for the continuation of daily life activities. The ultimate role of the BCI is to normalize the PDSFI to culminate in PDSI at the last phase. See Appendix D for the detailed instructions for the measurement of the BCI.

³³ Urban Area Key Sectors/Services list has been generated in line with essence of 18 Critical Infrastructure and Key Resource Sectors (CIKR) that have been developed within the context of National Infrastructure Protection Plan (NIPP).

Table 10 Basic Criticality Index (BCI) Equations

No	Urban Area Key Sectors/Services	BCI(i)
1	Governance, Homeland Security, Law/Public Order, Emergency Service	$BCI1=S1 \times (SRW1 \cup EW1)$
2	Housing/Accommodation	$BCI2=S2 \times (EW2 \cup OW2)$
3	Power/Energy Service (Power plants, nuclear reactors, dams, fuel supply stations, etc.)	$BCI3=S3 \times (SRW3 \cup EW3)$
4	Healthcare and Public Health	$BCI4=S4 \times (SRW4 \cup EW4)$
5	Telecommunication (including Information Technology)	$BCI5=S5 \times (SRW5 \cup EW5)$
6	Transportation/Postal and Shipping Service (including airports, major transportation terminals)	$BCI6=S6 \times (SRW6 \cup EW6)$
7	Food/Water and Other Goods Service (Shopping malls, major retail, etc.)	$BCI7=S7 \times (EW7 \cup SW7)$
8	Banking and Finance (including banks/ATMs, etc.)	$BCI8=S8 \times (SRW8 \cup EW8)$
9	Critical Manufacturing (including major industrial facilities)	$BCI9=S9 \times (EW9 \cup IW9)$
10	Training and Education Activities (including schools)	$BCI10=S10 \times (EW10 \cup STW10)$
11	Worship Activities (Places of worship, etc.)	$BCI11=S11 \times (EW11 \cup SCW11)$
<p>Variables: Si: Scaling Constant; SRW: Service Relativity Weight; EW: Employment Weight; OW: Occupancy Weight; SW: Size Weight; IW: Investment Weight; STW: Student Capacity Weight; SCW: Seating Capacity Weight</p> <p>The combination rule for the equations: $A \cup B = (A+B) - (A \times B)$</p>		

4.6.5 Measurement of Post-Disaster Security Fuzzy Index (PDSFI) (Phase 4)

The Post-Disaster Security Fuzzy Index (PDSFI) component provides a matrix assessment structure that constitutes the backbone of the PDSI Model. The theoretical concept of this matrix structure simply relies on the incorporation of three sub-components, which are illustrated in Figure 27.

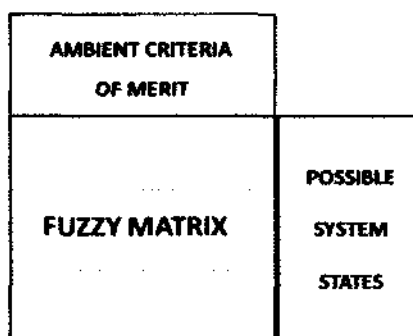


Figure 27 Three Main Components of PDSFI Matrix

The ultimate goal in this phase is to produce a PDSFI for each critical asset through the process formulated within the Fuzzy Matrix component (elaborated in Table 12) considering the parameters to be derived from the incorporation of the Ambient Criteria of Merit and Possible System States listed in Table 11.

Table 11 Ambient Criteria of Merit and Possible System States

AMBIENT CRITERIA OF MERIT	POSSIBLE SYSTEM STATES
<ul style="list-style-type: none"> • Physical Security (C1) • Number of Inhabitants/ Visitors (C2) • Size/ Area (C3) • Traffic Access/Mobility (C4) 	<ul style="list-style-type: none"> • Offences against Property (like looting, larceny/theft, burglary, arson, motor vehicle theft, etc.) (S1) • Offences against Persons (like murder, sexual assault, robbery, etc.) (S2) • Terrorist Attacks/ Warfare Threats (aggregated assaults, sabotages, etc.) (S3)

Technically, we can generate numerous criteria for vulnerability assessments that would conclude with security requirement prioritizations. However, since different system states dictate different security requirements, the criteria set for any system state should be developed in line with the essence of the system state characteristics. To that end, the Ambient Criteria of Merit (Table 10) identified in this study would sufficiently address the post-disaster security requirement characteristics. The validation of the criteria set has been supported by the decision tree analysis included in Appendix H.

From the causality perspective, the vulnerability of each asset may vary according to the characteristics of the system state. As an example, in a system state where there is lack of food, the assets which provide any kind of food services would be more susceptible to the potential offences while the others do not attract the offenders who have been motivated by the lack of food. To incorporate the assets' different vulnerability weights (according to the different system state characteristics) in the PDSI Model measurement process, three Possible System States (Table 11) have been defined in line with the major crime categories adopted within the common justice literature. ('Terrorist Attack/Warfare Threats' is the only exception of this rule, which has been added as a third system state since it has been considered critical.)

Furthermore, to ensure the outputs of this model provide generalizable indices that address a broad implementation spectrum, the 'Generalizability Grades of Membership' index definitions have been developed per each Criterion and System State, considering they would represent the generalizable local/ambient parameters regarding each Criterion and System State, but not the critical asset.

Table 12 depicts the integrated PDSFI Matrix. Three steps associated with the matrix variables are outlined below:

1. Measurement of Input Variables
2. Measurement of Fuzzy Matrix Variables
3. Aggregation

Table 12 Post-Disaster Security Fuzzy Index (PDSFI) Matrix

Ambient Criteria of Merit				Vulnerability Indexes				Possible System States			
Scaling Constant (sc)	(sc1)	C1: Physical Security	V(C1)	V(C2)	V(C3)	V(C4)	S1: Offences against Property S2: Offences against Persons S3: Terrorist Attacks/ Warfare Threats				
	(sc2)		Generalizability Grades of Membership								
	(sc3)	C2: Number of Inhabitants/Visitors	G(C1)	G(C2)	G(C3)	G(C4)					
	(sc4)	C3: Size/Area									
C4: Traffic Access/Mobility											
Fuzzy Matrix			PDSFI(S1)	(G1, V1)	(G2, V2)	(G3, V3)	(G4, V4)	G(S1)	Generalizability Grades of Membership	M(S1)	Vulnerability Index Modifiers
			PDSFI(S2)	(G5, V5)	(G6, V6)	(G7, V7)	(G8, V8)	G(S2)		M(S2)	
			PDSFI(S3)	(G9, V9)	(G10, V10)	(G11, V11)	(G12, V12)	G(S3)		M(S3)	

1. **Measurement of Input Variables:**

The list of PDSFI Matrix input variables and their sub-components are listed below. Further information for the measurement of each variable and sub-components is included in Appendix E.

a. **Scaling Constants:**

- **sc1:** Scaling Constant for the Criterion of Physical Security

- **sc2:** Scaling Constant for the Criterion of Number of Inhabitants/Visitors
- **sc3:** Scaling Constant for the Criterion of Size/Area
- **sc4:** Scaling Constant for the Criterion of Traffic Access/Mobility

b. Vulnerability Indexes of the Critical Asset per each Criterion:

- **V(C1):** Vulnerability Index of the Critical Asset for Physical Security
 - Perimeter Security Index
 - Building Envelope Wall Type Index
 - Building Envelope Fenestration Index
- **V(C2):** Vulnerability Index of the Critical Asset for Number of Inhabitants/Visitors
- **V(C3):** Vulnerability Index of the Critical Asset for Size/Area
- **V(C4):** Vulnerability Index of the Critical Asset for Traffic Access/Mobility
 - Periphery Road Width Index
 - Adjacent Primary Roads Proximity Index
 - Bridge Dependency Index
 - Transportation Terminals Proximity Index

c. Vulnerability Index Modifiers of the Critical Asset per each Possible

System State:

- **M(S1):** Vulnerability Index Modifier of the Critical Asset for Offences against Property
- **M(S2):** Vulnerability Index Modifier of the Critical Asset for Offences against Persons
- **M(S3):** Vulnerability Index Modifier of the Critical Asset for Terrorist Attacks/Warfare Threats

d. Generalizability Grades of Membership per each Criterion:

- **G(C1):** Generalizability Grades of Membership for Physical Security
 - Seismicity Vulnerability Index
 - Hurricane Vulnerability Index
 - Flood Vulnerability Index
- **G(C2):** Generalizability Grades of Membership for Number of Inhabitants/Visitors
- **G(C3):** Generalizability Grades of Membership for Size/Area
- **G(C4):** Generalizability Grades of Membership for Traffic Access/Mobility
 - Road Length Index
 - Transportation Lines Index
 - Bridges Index

e. Generalizability Grades of Membership per each Possible System

State:

- **G(S1):** Generalizability Grades of Membership for Offences against Property
- **G(S2):** Generalizability Grades of Membership for Offences against Persons
- **G(S3):** Generalizability Grades of Membership for Terrorist Attacks/Warfare Threats

2. Measurement of Fuzzy Matrix Variables:

The equations for the measurement of fuzzy matrix variables (Table 13) have been included in Table 14. The combination rule for Generalizability Grades of Membership Variables is:

$$A \cup B = (A+B) - (A*B) \quad (1)$$

Table 13 Fuzzy Matrix Variables

Fuzzy Matrix	PDSFI(S1)	(G1, V1)	(G2, V2)	(G3, V3)	(G4, V4)
	PDSFI(S2)	(G5, V5)	(G6, V6)	(G7, V7)	(G8, V8)
	PDSFI(S3)	(G9, V9)	(G10, V10)	(G11, V11)	(G12, V12)

Table 14 Equations for the Measurement of Fuzzy Matrix Variables

Generalizability Grades of Membership Variables	Vulnerability Index Variables
$G1 = G(C1) \cup G(S1)$	$V1 = sc1 * V(C1) * M(S1)$
$G2 = G(C2) \cup G(S1)$	$V2 = sc2 * V(C2) * M(S1)$
$G3 = G(C3) \cup G(S1)$	$V3 = sc3 * V(C3) * M(S1)$
$G4 = G(C4) \cup G(S1)$	$V4 = sc4 * V(C4) * M(S1)$
$G5 = G(C1) \cup G(S2)$	$V5 = sc1 * V(C1) * M(S2)$
$G6 = G(C2) \cup G(S2)$	$V6 = sc2 * V(C2) * M(S2)$
$G7 = G(C3) \cup G(S2)$	$V7 = sc3 * V(C3) * M(S2)$
$G8 = G(C4) \cup G(S2)$	$V8 = sc4 * V(C4) * M(S2)$
$G9 = G(C1) \cup G(S3)$	$V9 = sc1 * V(C1) * M(S3)$
$G10 = G(C2) \cup G(S3)$	$V10 = sc2 * V(C2) * M(S3)$
$G11 = G(C3) \cup G(S3)$	$V11 = sc3 * V(C3) * M(S3)$
$G12 = G(C4) \cup G(S3)$	$V12 = sc4 * V(C4) * M(S3)$

3. Aggregation:

Following the measurement of fuzzy matrix variables, final aggregation is performed through Equation 2 below. When necessary, matrix variables could also be aggregated per each system state through Equations 3, 4, 5 to be processed for different assessment purposes (e.g.; for a specific area of responsibility, vulnerability weights of the critical assets could be scrutinized only considering the 'Offences against Property' system state).

$$\text{PDSFI} = \left[\sum_{i=1}^{12} G_i \times V_i \right] / 12 \quad (2)$$

$$\text{PDSFI}(S1) = \left[\sum_{i=1}^4 G_i \times V_i \right] / 4 \quad (3)$$

$$\text{PDSFI}(S2) = \left[\sum_{i=5}^8 G_i \times V_i \right] / 4 \quad (4)$$

$$\text{PDSFI}(S3) = \left[\sum_{i=9}^{12} G_i \times V_i \right] / 4 \quad (5)$$

4.6.6 Measurement of Post-Disaster Security Index (PDSI) (Phase 5)

The Post-Disaster Security Index (PDSI), which is the final output of the PDSI Model, is measured processing the Basic Criticality Value (BCV) and Post-Disaster Security Fuzzy Index (PDSFI) (which have already been measured in the previous phases) through Equation 6. The PDSI provides a score between 0 and 10.000 that represent the post-disaster security requirement of each critical asset assigned in the area of responsibility³⁴.

$$\text{PDSI} = (\text{BCV} * \text{PDSFI}) * 1000 \quad (6)$$

4.7 Sample Measurement

4.7.1 Scenario

The Operations Bureau in the City of Delta Police Department has been tasked to develop a Post-Disaster Security Plan for the city. To proceed the planning process, they need to identify the criticality and vulnerability weights of the critical assets within the city to decide on the best option between force tailoring (organization) and unit positioning (deployment) alternatives for the execution of security operations techniques (which could be Patrol, Guard, 'Intelligence, Surveillance, and Reconnaissance' (ISR), Response/Reaction Force).

The Operations Bureau planning team decided to use the PDSI Model to make the vulnerability assessments and derive necessary data for the prioritization and decision making. They followed the five sequential phases delineated in Appendix F.

³⁴ The equation is multiplied by a coefficient of 1000 to obtain an integer which provides a score highest in precision, minimally rounded to the left.

4.7.2 Measurement Results

The PDSI for each critical asset is listed in Table 15, which has been obtained through the PDSI Model algorithm at Chapter 4.6.

Table 15 PDSI of the Critical Assets

Critical Asset	BCV	PDSFI	PDSI
Blue Shopping Center (BSC)	0.548	2.334	1279
Delta City Hospital (DCH)	0.792	1.121	887
City of Delta Department (CDD)	0.950	0.699	664

Performance Sensitivity results of the indexes (V_a (raw), V_a , PDSFI, PDSI) are listed in Table 16.

Table 16 Performance Sensitivity

Index Types	Critical Asset		
	BSC	DCH	CDD
V_a(raw)*	6.09	5.66	4.59
Normalized V_a(raw)	1	0.929	0.754
V_a^{**}	3.723	1.825	1.206
Normalized V_a	1	0.49	0.324
PDSFI	2.334	1.121	0.699
Normalized PDSFI	1	0.48	0.299
PDSI	1279	887	664
Normalized PDSI	1	0.694	0.519

* V_a (raw): Average of the raw Vulnerability Indexes

$$V_a(\text{raw}) = \left[\sum_{i=1}^4 V(C_i) \right] / 4$$

** V_a : Average of the Fuzzy Vulnerability Indexes

$$V_a = \left[\sum_{i=1}^{12} V_i \right] / 12$$

*** Normalized weights are obtained through the division of each weight by the maximum.

4.8 Reliability and Validity of the Constructs

The conceptual design of the PDSI Model is based on the combined knowledge of the epistemological perspective of modeling, MCDM, systems thinking and relevant aspects of the military literature, including the MDMP. The model has been developed through a prescriptive research methodology.

Korb, Geard and Dorin (2013) discuss how expert opinions have a significant role in the validation of the models, while the Bayes' Theorem suggests the incorporation of both the statistical tests and expert opinions during the research. In line with the discussion of Korb et al., the validation of the PDSI Model as a whole and the set of criteria incorporated in the model relies heavily on the subjective assessments of subject matter experts, since the statistical testing of this model requires high scale comprehensive experimentation through extended studies and extensive participation of diverse security stakeholders. Nonetheless, for the validation of the PDSI Model including its development process; Face Validity, Content Validity and Internal Validity methods have been applied during the dissertation.

For the subjective analysis of a model and its characteristics, Oren and Yilmaz (2013) state that "a model is not considered to be absolutely correct or incorrect, but rather subjective analysis of qualitative characteristics is considered essential for its acceptability and credibility" (p. 162) in the pragmatist and holistic schools, while Korb, Geard and Dorin (2013) claim "a great deal of practical effort in developing models goes into making sense of expert opinions about a modeling domain" (p. 255).

Regarding the Face Validity; Health and Jackson (2013) contends "while there are similar approaches when compared to traditional scientific techniques of validation such

as statistical testing, Face Validation (i.e., asking experts to determine whether the model behavior seems reasonable) almost completely relies on subjective human judgment” (p. 100). In a similar way, Korb, Geard and Dorin (2013) underline the significance of face validity “while face validity is a weak kind of test of a model, it is nevertheless central to most modeling endeavors” (p. 262). In this sense, the Face Validity of the PDSI Model has been obtained through interviews with subject matter experts³⁵ who have more than 10 years of experience in their respective domains. The validation questionnaire utilized during the interviews is included in Appendix G.

Pertaining to Content Validity, Korb, Geard and Dorin (2013) state: “Content Validity considers whether the most important factors and relationships between variables noted in the literature are present in the model; expert opinion will be the primary guide here, but focused reviews of the literature will also be useful” (p. 262). Triangulation, which could be utilized as a Content Validity approach, is “broadly defined as synthesis and integration of data from multiple sources through collection, examination, comparison, and interpretation” (Overview of Triangulation Methodology, (n.d.), p. 7). It is “typically a strategy for improving the validity and reliability of research or evaluation of findings” (Golafshani, 2003, p. 603). The triangulation methodology, which has been adapted from the cycle illustrated in Figure 28, was applied during the development of the PDSI Model (particularly during the development of the variables of the Ambient Criteria of Merit and measurement matrixes) to synthesize and distill the information provided through the relevant literature.

³⁵ The author of this dissertation also qualifies the requirements as the subject matter expert on this domain.

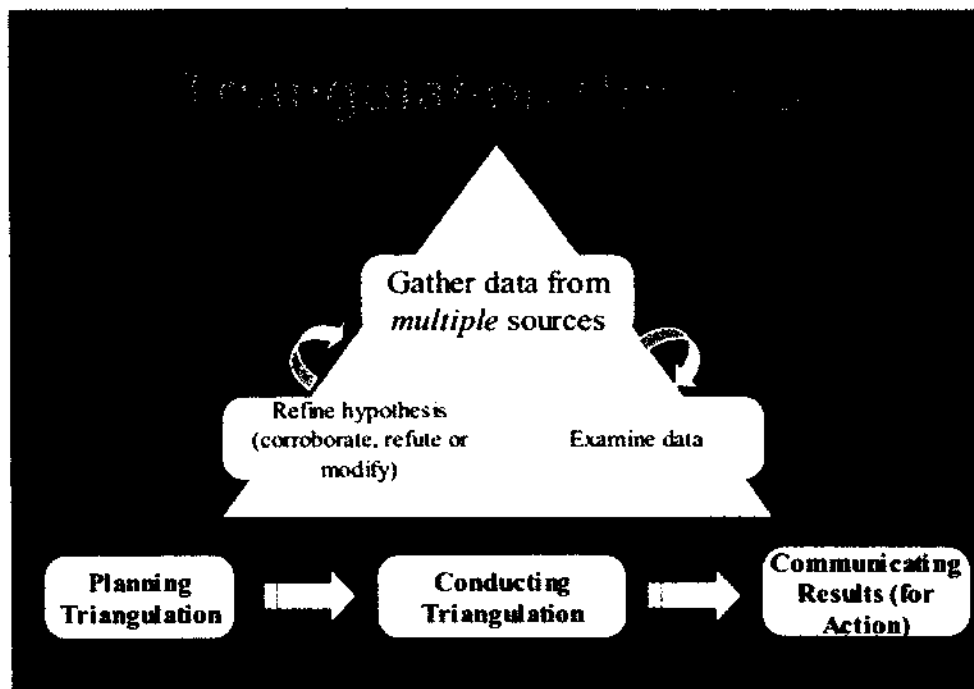


Figure 28 Visual Representation of the Triangulation Process (Overview of Triangulation Methodology, (n.d.), p. 15)

Finally, regarding Internal Validity, Korb, Geard and Dorin (2013) highlight how this method focuses on the assessment of the model variables:

Internal Validity examines whether variation in the model's variables is reasonable. This could specifically consider co-variation between sets of variables, to determine whether changes in some variable either cause or are co-dependent with changes in others, in ways which are judged sensible by experts; this is generally called sensitivity analysis. (p. 262)

Considering the variables of the PDSI Model in this context, the overall situation usually gets more complicated with numerous diverse interactions between great numbers of elements existing within the system boundaries in a crisis system state like a post-disaster environment. In such a case, it is critical that the models supporting the Public Safety and Security planning process address the post-disaster urban environment

characteristics, since they theoretically reflect the features of the worst-case scenario, like lack of power and other supplies, lack of communication, disorder, emergency, potential threats, complexity, uncertainty, poor coordination, etc. The Ambient Criteria of Merit incorporated in the PDSFI matrix were developed with the aim of capturing the aforementioned post-disaster security requirements. The Ambient Criteria of Merit play a significant role in the measurement/assessment process of the PDSI Model; each criterion in this set has multiple sub-variables that address the different aspects of the security paradigm in the context of post-disaster environment. In addition, the Internal Validity of the Ambient Criteria of Merit have been validated through the Decision Tree Analysis, which has been developed based on a specific scenario (see Appendix H: Basic Reality Face-Off Decision Tree).

4.9 Conclusion

The vulnerability assessment (associated with the criticality assessment aspects) of the critical assets significantly impacts post-disaster security planning for urban areas considering the different types of threats. Since the prioritization of security requirements for the critical assets, which is a critical driver for decision making, relies heavily on the assets' vulnerability assessments. However, there is no model or methodology (employing fuzzy multi-criteria decision making, and incorporating different system states and multiple sets of criteria derived from the essence of the security concept of operations) in place to provide the aforementioned vulnerability assessment capability.

As elaborated in the Sample Measurement in Chapter 4.7, the relative weights of the normalized vulnerability indexes³⁶ attributed for each critical asset vary, as do the number of variables processed during the measurement of each index as depicted in Figure 29. Through quantitative experimentation or statistical testing, it is challenging to choose the best quality, more precise index from among these. The validation and reliability testing for each index and its measurement process requires subjective analyses and the assessments of subject matter experts.

However, considering the serious differences between the normalized weights, the trade-offs at the end of the assessment process will have an inextricable link to the precision or resolution of the utilized index. Furthermore, since the assessment or prioritization process deals with a macro level system of interest with cumulative elements, it is most likely that the assessment results would exponentially change based on the type of utilized index, which theoretically provide different levels of precision or resolution.

Considering the justifications outlined for the PDSI Model's reliability and validity, it is assumed that it would provide valuable parameters for urban area security planners to enhance the reliability of their post-disaster security plans in the context of NRF. The potential outcomes of the PDSI Model have been elaborated in Chapter 5.2.

³⁶ Each index represents different approaches and includes different variables in the measurement process.

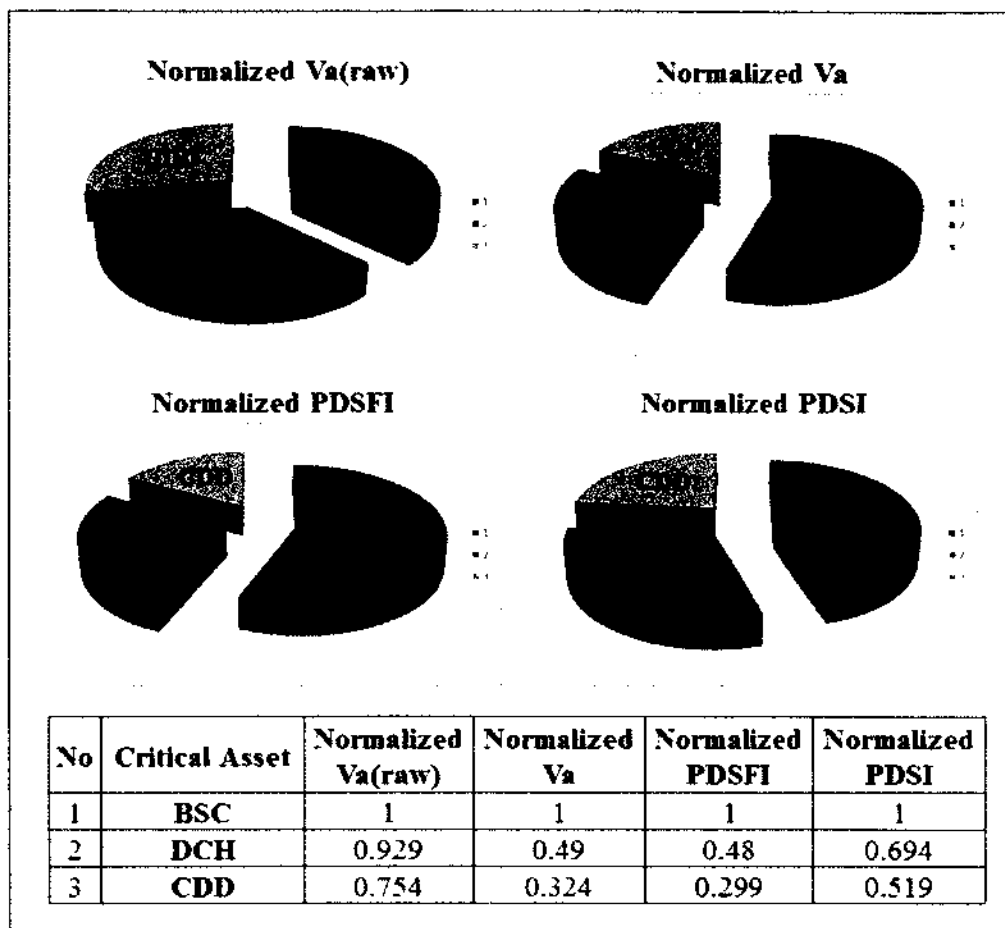


Figure 29 Relative Performance Sensitivity of Normalized Indexes³⁷

³⁷ The normalized indexes have been imported from the Sample Measurement in Chapter 4.7.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

To achieve resilience, we must more fully incorporate a comprehensive understanding of risk to establish priorities and inform decision making. Resilience will also require a shift from a reliance on top-down emergency management to a process that engages all stakeholders. (Quadrennial Report, 2010, p. 31)

In this dissertation, the incorporation of the Emergency Management concept within the U.S. Homeland Security contextual structure (theoretical content) has been scrutinized holistically, including the conceptual design of the NRF that is one of the critical mandates of the Homeland Security domain. Furthermore, in the context of the NRF, particularly the significance of the ESF-5 (Emergency Management) and ESF-13 (Public Safety and Security) has been underlined, and the PDSI Model has been developed with the aim of supporting the existing post-disaster security planning process, which is a critical part of the Public Safety and Security (Figure 30).

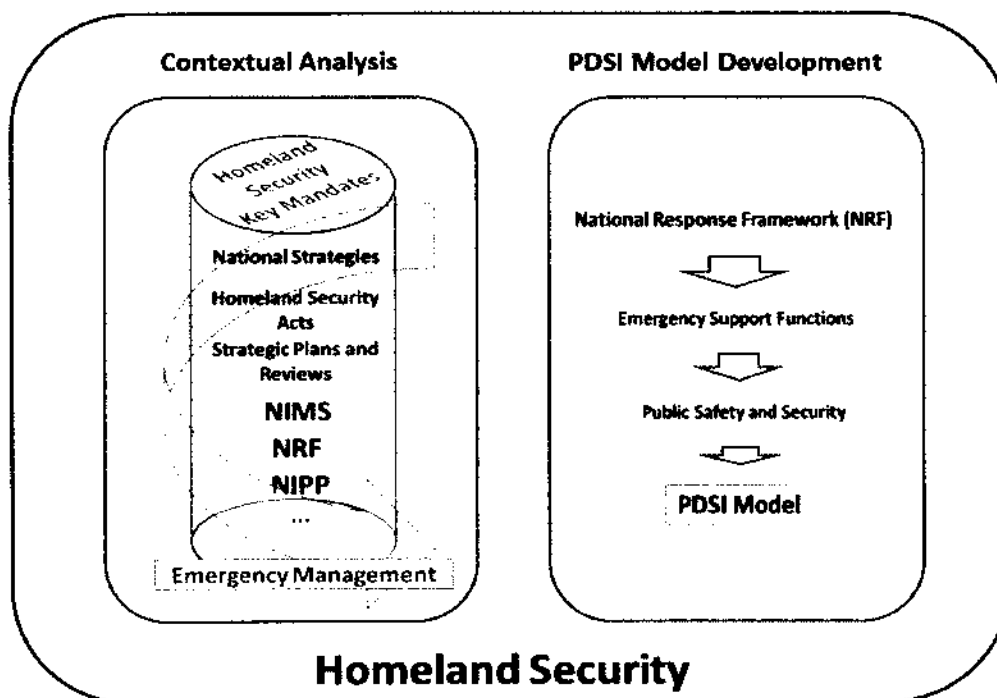


Figure 30 Synopsis of the Dissertation

5.1 Conclusions

5.1.1 Homeland Security Contextual Structure

Homeland Security led by DHS in the U.S. represents an ultra-complex organizational enterprise with great numbers of stakeholders, numerous missions, and functions that entail extraordinary oversight and synchronization. This enterprise is critical and has unique characteristics, since it aims to provide people with the security that is a first priority core human need.

After the 2000s, Homeland Security was founded on the conceptual framework of Emergency Management which is theoretically the successor of 'disaster response' efforts that date back to 19th century. From the 19th century until the establishment of FEMA in 1979, the disaster response was handled by decentralized initiatives. In 1979, FEMA assumed an overarching role on the response missions and institutionalized and centralized these initiatives up to 2002. However, during this time, rather than developing a comprehensive Emergency Management concept/doctrine, which would elaborate the expected contextual structure including the concept boundaries of the system, only the definition and phases/components of Emergency Management were circulated.

After the September 11 terrorist attacks, DHS was established and charged with critical responsibilities. During that time, the *National Strategy for Homeland Security* and the *Homeland Security Act of 2002* defined the Homeland Security key missions and priorities based on the theoretical context of Emergency Management without any direct reference to Emergency Management. In 2003, FEMA was subsumed by DHS, and the contextual conflicts started to be surfaced. After Hurricane Katrina in 2005, the *Post Katrina Emergency Management Reform Act* of 2006 aggravated the epistemological

problems, since it attributed an overarching mission spectrum to Emergency Management that overlapped with the theoretical domain of DHS.

In the following years, the contextual deviation and confusion regarding the incorporation of the Emergency Management concept in the Homeland Security context continued through the *National Strategy for Homeland Security* (2007), QHSR (2010) and other key mandates as discussed in Chapter 3. Considering particularly the recent strategic documents of *Presidential Policy Directive-8* (2011), *DHS Strategic Plan* (2012) and draft *NRF* (2012), the following problems still exist, and unless necessary actions are taken, they would negate the development of Homeland Security, which basically aims to enhance the preparedness and resiliency of American Nation:

- “There is not an established Emergency Management Doctrine” (Blanchard, 2007, p. 3), and the conceptual relationship between Emergency Management and Homeland Security has not been clearly defined.
- Regarding meaning and content, there are different connotations attributed for Emergency Management in the various key Homeland Security mandates.
- The conceptual design of the ESFs within the NRF suffers from the lack of comprehensive Emergency Management doctrine and common terminology.
- In the pertinent official literature, there is also a lack of holistic, multi-dimensional, top-down figurative system representation. Although it is crucial to let complex system stakeholders oversee the system process and development, it is too fuzzy to appreciate the existing system framework holistically as well as to understand the system boundaries, and the relationships between key elements (entities, stakeholders, missions, functions, etc.).

- Upon the evolution of the threat spectrum and other challenges, new conceptual designs have been generated during the development of Homeland Security with the justification of evolutionary requirements. However, the new regulations have inherited the aforementioned epistemological problems in a domino effect.

The epistemological inconsistency and lack of holistic system representation within the Homeland Security contextual structure is likely to produce more confusion. that could end up with a fuzzy and lumpish system with poor policy context, blurred system representations/abstractions, poorly educated personnel devoid of necessary situational awareness, ill-designed organizational structures, and improperly running operational functions. On the other hand, contextual coherence allows a well-designed system structure to facilitate system viability functions properly. Therefore, the challenge stemming from the contextual inconsistency should be scrutinized seriously and further amendments should be implemented to the existing Homeland Security contextual structure to transform and adapt the Emergency Management concept appropriately. In this sense, the assertion of Gheorghe and Vamanu (1996) provides a meaningful guidance for those who would take part in further contextual analyses: “Validating, applying, and maintaining - including refining – existing Emergency Planning Preparedness and Management (EPPM) knowledge and systems is as important as generating new knowledge” (p. 15).

5.1.2 Post-Disaster Security

The primary focus of authorities has always been the Public Safety and Security, including law enforcement, public order, and physical protection of critical infrastructures and key assets during both ordinary/peacetime and crisis/wartime system states. Particularly after a high scale natural or man-made disaster in an urban area, the security agents are supposed to prevent public order from turning into panic and chaos by establishing security, maintaining law and order, and letting other response/recovery missions be executed successfully.

All disaster response/recovery activities (saving lives, first aid and medical treatment, law enforcement by sustaining public order and security, evacuation, maintenance, repair, etc.) are necessarily supposed to be executed coherently in a relatively more secure and stable system state using a synchronized planning methodology. Security and law enforcement play a critical role in the facilitation of other follow-up disaster response/recovery activities.

In the U.S. Homeland Security system architecture, the Public Safety and Security mission has been designed as an *Emergency Support Function* within the NRF. However, the design mindset of this function in the NRF is incompetent, and the instructions and guidelines provided in the existing Public Safety and Security (ESF-13) annex do not comprise necessary details, particularly in terms of interaction with the other ESFs, which would support the accomplishment of security missions in severe conditions like catastrophic post-disaster periods.

Although the criticality and vulnerability assessment of critical assets (which include critical infrastructures, facilities, state/public/private properties, etc.) in an urban

area has a significant impact on the post-disaster security planning process, there is no model in practice which provides an urban area critical asset prioritization methodology with both a fuzzy multiple criteria decision making approach incorporating different system states, and multiple sets of criteria that specifically address the post-disaster urban security unique characteristics.

5.2 Recommendations

Since the epistemological inconsistency and lack of necessary holistic system representation within the Homeland Security contextual structure is likely to produce more confusion, poorly educated staff, ill-designed organizational structures, and most importantly, improperly running operational functions, the contextual structure should be scrutinized seriously as a whole and further amendments applied to ensure the Emergency Management concept be transformed and adapted appropriately within the context of Homeland Security.

Rather than evolutionary, the system should be overseen through a transformational perspective by controlled, coordinated and unified efforts and common terminologies as it has been directed by the *Presidential Policy Directive-8* (National Preparedness, 2011), and systems thinking, which is supported by the holistic vision should be utilized by the system stakeholders who have the stewardship responsibility.

Preliminarily, a complete organizational system analysis could be performed for further specification and clarification of the problem domain, and identification of the possible solutions from an `independent vantage point` perspective, since the system`s contextual structure dominated by the discussed problems is highly complex and

extensive in scale, and linked to system`s organizational and functional structures. A proposed roadmap for a `Complete Complex Organizational System Analysis` is included in APPENDIX I.

After the proposed analysis is complete, the contextual system architecture should be redesigned by including common terminologies and proper taxonomies. A `Simplify- Unify-Integrate` rule could be adopted to consolidate the loose and fuzzy contextual clusters in the system. In that sense, without trying to paraphrase the differences between them, two critical mandates – NIMS and NRF – should be integrated to produce a single simple capstone document.

On the other hand, the potential dilemma “while complex systems require complex solutions³⁸, simple approaches³⁹ are preferred to deal with complexity” should be handled with the optimal decisions. While there is no golden rule for the optimal design of the system context (Figure 31), a successful system re-design could be accomplished with the utilization of a unique methodology which is exclusive to the system, and the employment of qualified subject matter experts who have the holistic thinking capability as well as the necessary system content knowledge that is epistemologically consistent with the historical development process of the system.

³⁸ “In order to express a rich knowledge set that includes environment, contingencies, resources, possible actions and much more, we need a framework that allows us to represent knowledge in many facets or dimensions.” (Douglass and Mittal, 2013, p. 282)

³⁹ Simplicity is central to reducing complexity in planning and it fosters a shared understanding of the situation, the problem, and the solution (Stability Operations, 2008, p. 4-1).

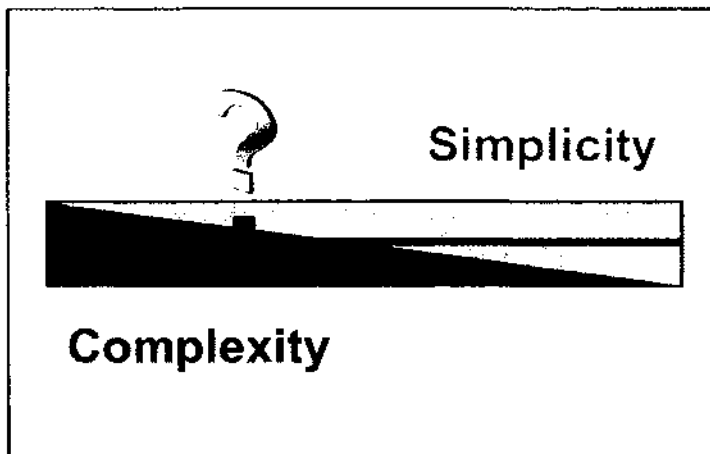


Figure 31 Optimal Design of the System Context

With regard to the conceptual design of the Emergency Support Functions, the Joint Field Office (JFO), Incident Command (IC) and ESFs are the key elements in response and recovery operations within the integrated framework of NRF and NIMS. Theoretically, ESFs bridge the JFO to the IC to facilitate the four major functional areas: operations, planning, logistics, and finance/administration, as depicted in Figure 32. In this framework, to eliminate the negative implications of the epistemological problems discussed, the role of the Emergency Management (ESF-5) should be re-designed conceptually and graphically in the existing context to ensure it oversees the whole framework as an overarching coordination function rather than a support function as the others, which are facilitated between the functional areas to link the support cycles [as it is delineated in the next paragraphs; also the role of ESF-13 (Public Safety and Security) should also be modified to let it function with a central, backdrop role in the NRF].

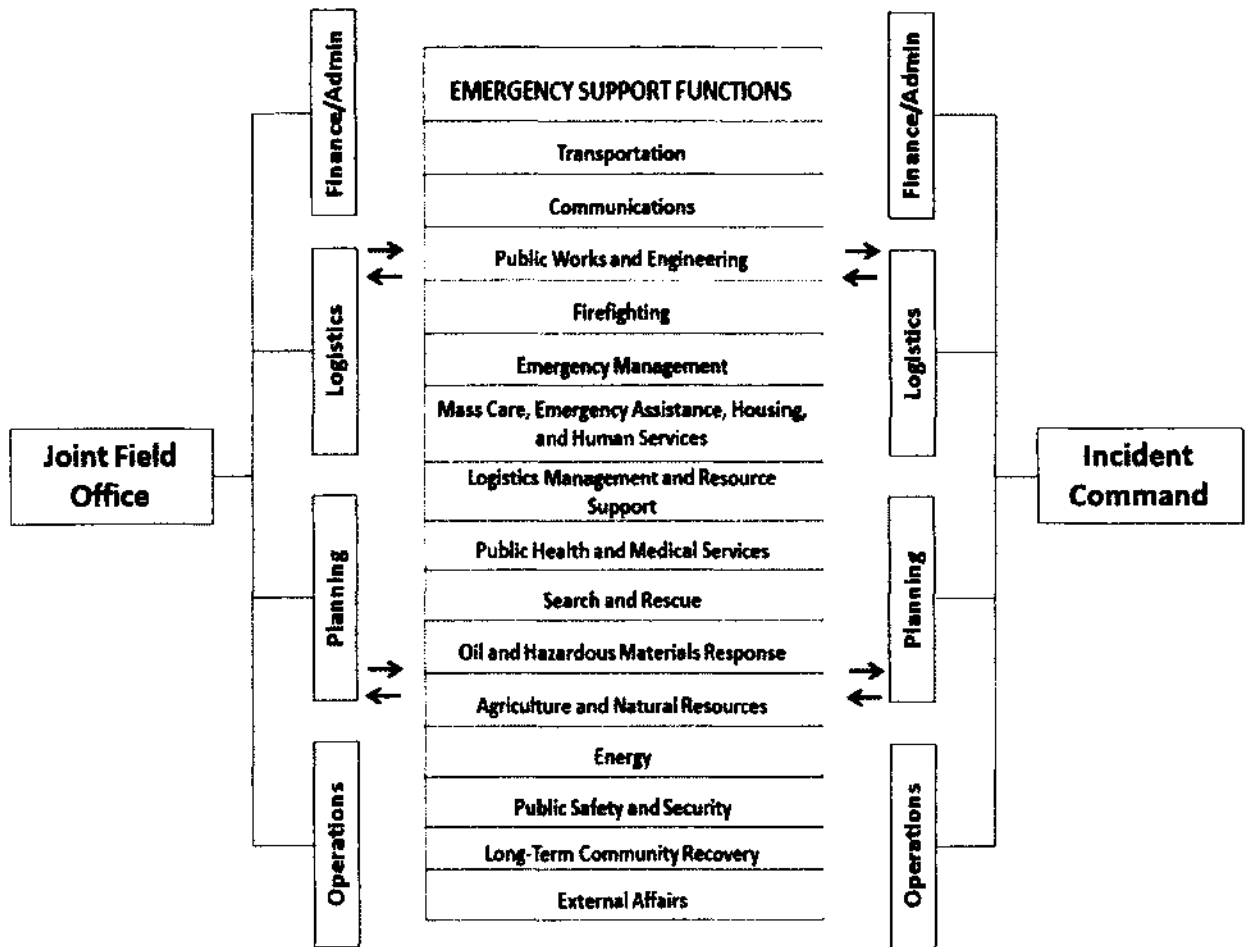


Figure 32 Facilitation of Functional Areas

While the contextual and structural architecture of the system is re-designed properly and diverse functional mechanisms are let operate efficiently, the necessary figurative multi-dimensional holistic system representations which would provide a clear insight for the individuals and other stakeholders should also be included in the relevant capstone documents. The concept of the multi-dimensional holistic system representation is depicted in Figure 33. The sample complex system represented in the figure includes different layers, components and sub-components accompanied by a great number of functions/entities that have networked in a fuzzy structure which has different clusters

and relation patterns. The representations to be produced in a similar way would provide a useful guide for the system stakeholders to make top-down and bottom-up inquiries through the system architecture as well as drill down exploration in any cluster (even in any critical nexus in any cluster) within any layer.

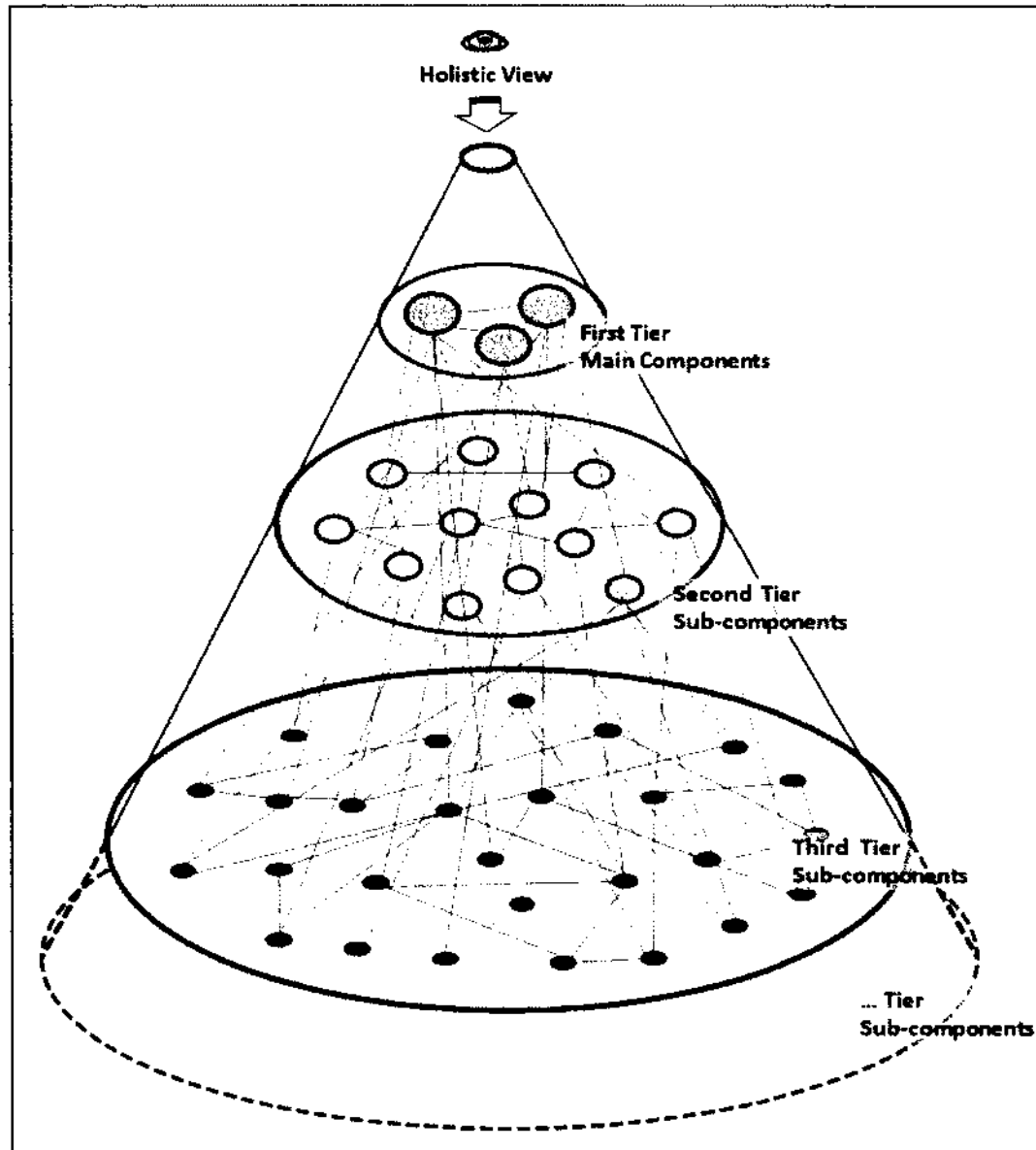


Figure 33 Multi -Dimensional Holistic System Representation

Gheorghe and Vamanu (1996) discuss that “Emergency Planning, Preparedness and Management (EPPM) knowledge should be made available at the level of widest conceivable use” (p. 15). In that sense, coherently well-designed contextual structures with multi-dimensional holistic figures would catalyze the circulation of necessary knowledge enhancing the situational awareness of the system stakeholders. The education and training initiatives should also leverage this approach to ensure the complex mega-systems are manned with qualified individuals and teams who have a deep insight on the system design and framework.

Public Safety and Security

The Public Safety and Security function plays a critical role within the NRF, since any serious failure in this function could cause the collapse of the whole framework, especially during a post-disaster period. Thus, the decision makers should ensure they have necessary assets and reliable Public Safety and Security plans to establish security and public order in the disaster area so other disaster response/recovery missions are conducted coherently. A high level of resiliency could be derived from the military perspective of effective planning: If the security plan is developed based on the possible implications of the worst-case scenario, then it would work at its best during the implementation phase whatever the conditions could be.

In line with the essence of this assumption, the Public Safety and Security plans should be developed with a post-disaster security centric focus that addresses the implications of the worst-case scenario characteristics, and utilizes some principal drivers

like 'holistic approach, systems thinking, proactive planning, applicable criteria and reliable data, simplicity, etc.' (Figure 34).

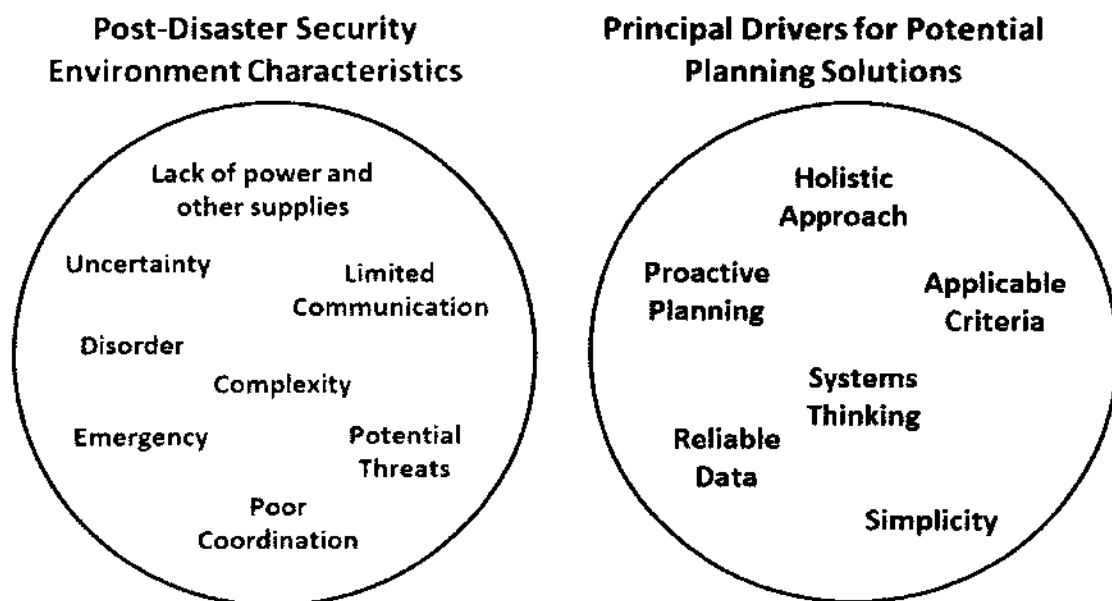


Figure 34 Post-Disaster Security Environment Characteristics and Principal Drivers for Potential Planning Solutions

Since the Public Safety and Security is highly critical for the facilitation of other follow-up disaster response and recovery missions, the Public Safety and Security plans (ESF-13) should be improved through the utilization of models which can process multiple criteria and different system state variables to address the fuzzy characteristics of the post-disaster urban security. In addition, the role of the ESF-13 should be modified in the NRF to let it function with a central, backdrop role. Having these done, it would be possible to provide more granularity in the content of the Public Safety and Security plans, ensuring they provide relevant stakeholders and other support functions with the supportive decision making and prioritization parameters [e.g.; secure lines of

transportation, potential locations/coordinates of aid delivery points, shelters, deployable operations centers, security zones (safe havens that would be secured with the highest degree security measures during the crisis), etc. could be identified utilizing the outcomes of the PDSI Model].

The PDSI Model introduced in Chapter 4, which has been developed with a post-disaster centric focus, should be utilized to develop resilient security plans to support other disaster response/recovery activities in emergency. Since the model offers to produce generalizable indices for the vulnerability assessment and prioritization of the critical assets in any urban environment, it would provide valuable insights for all level security planners to tackle with the complexities during any crisis.

Furthermore, with this model implemented, the emergency response framework would be reinforced, since its conceptual design has been developed to address the characteristics of worst case scenarios derived from the post-disaster urban environment. To enhance the resiliency and preparedness of the response framework, a 'Baseline Security Plan,' which is to be developed through the utilization of possible PDSI Model outcomes could be accompanied with the other plans outlined in NRF Emergency Support Function -13 (2008)⁴⁰. Previously discussed supportive decision making and prioritization parameters could easily be transferred to other ESFs as necessary.

⁴⁰ Public Safety and Security (ESF-13) provides the conduit for utilizing and incorporating the extensive network of public safety and security coordination established for steady-state prevention efforts through a variety of interagency plans. Prevention and security plans include, but are not limited to, the following (Emergency Support Function 13, 2008, p. 2):

- National Infrastructure Protection Plan
- Sector-Specific Plans
- The National Strategy for Maritime Transportation Security
- Area Maritime Security Plans
- Vessel and Facility Security Plans

The potential outcomes of the PDSI Model follow:

- Utilization of realistic and precise (to the largest extent possible) assessment parameters⁴¹ (an example is depicted in Figure 35) in the security planning process in terms of:
 - Force tailoring (organization).
 - Unit positioning (deployment), identification of boundaries for each troop/unit.
 - Identification of the security operations techniques: Patrolling, Guard, ISR, Response/Reaction Force, etc. (e.g. identification of critical patrol clusters, identification of target prioritization requirements for ISR assets).

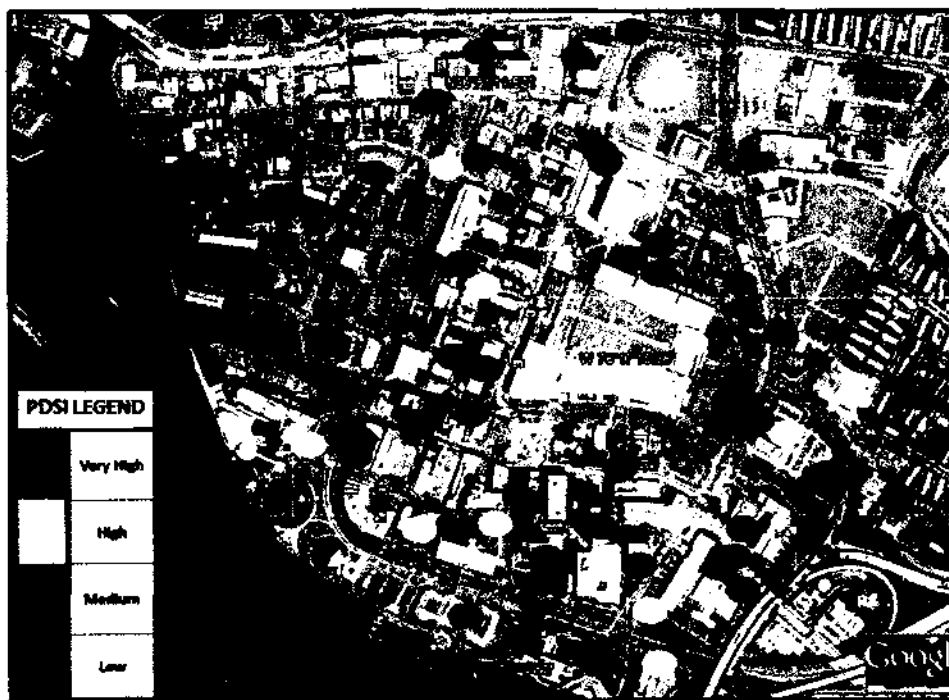


Figure 35 Depiction of PDSIs in Color Code

⁴¹ To be accompanied by Geographic Information Systems (GIS).

- Better coordination and interoperability opportunities for the local and external support troops in all levels via detailed map overlays produced with the support of PDSI data sets.
- Easy identification of the local and external support requirements from different resources (City Police, State Police, National Guard, Active Military, other State Agents or Federal Organizations). The PDSI Model provides generalizable indices that help identify the approximate security requirements.
- Provision of valuable inputs to be used in exercises that should be realistic in scenario and consequences as requested by the *National Security Strategy* (2010).
- Support to strategic decision making. The implementation of the model in the city, state or country level would also provide critical insight for the strategic planning and decision making processes in terms of optimizing the mix of military Active Component (AC) and Reserve Component (RC) elements⁴² as well as Police and other security agents, and the strategic peacetime emplacement (geographic footprint) requirements of these elements. This level of planning has an inextricable link to the Homeland Security missions and most of these elements are assigned for disaster response/recovery support operations as required.

⁴² The optimization of the mix of military Active Component (AC) and Reserve Component (RC) elements has been requested by Strategic Guidance (2012) to make them best suited to what has been stated in the strategy.

REFERENCES

- Antiterrorism*. (2011). Field Manual 3-37.2. Headquarters, Department of the Army.
- A Governor's Guide to Emergency Management*. (2002). Volume Two: Homeland Security. NGA Center for Best Practices.
- Academic room: GIS*. (n.d.). Retrieved from <http://www.academicroom.com/physical-sciences/earth-sciences/geography/geographic-information-systems>
- About Systems Philosophy*. (n.d.). Centre for Systems Philosophy. Retrieved from <http://www.systemsphilosophy.org/introduction-to-systems-philosophy.htm>
- Attribute*. (n.d.). The Free Dictionary. Retrived from <http://www.thefreedictionary.com/attribute>
- Norfolk Police Department. (2010). *Annual Report*. Virginia.
- Buddelmeyer, K. L. (2007). *Military first response: Lessons learned from Hurricane Katrina*. Research report. Alabama: Maxwell Air Force Base.
- Bowman, S. (2000). *An overview from law enforcement's perspective*. In C.W Pumphrey (Ed.), *Transnational threats: blending law enforcement and military strategies* (pp. 19-39). U.S. Army War College.
- Bush, G.W. (2001). *Homeland Security Presidential Directive-1: Organization and Operation of the Homeland Security Council*. Washington, DC: The White House.
- Bar-Yam, Y. (2004). *Making things work: solving complex problems in a complex world*. U.S.: NECSI, Knowledge Press.

- Baird, M. E. (2010). *The "phases" of emergency management*. Background Paper prepared for the Intermodal Freight Transportation Institute (IFTI), University of Memphis.
- Bozkurt, I. (2009). *Developing a philosophical profile of the individual for complex problem-solving through agent-based modeling*. Dissertation. Norfolk: Old Dominion University.
- Bozkurt, I., Padilla, J.J. & Sousa-Poza, A. (2007). Philosophical profile of the individual. *Proceedings of the 19th IEEE International Engineering Management Conference*. Austin, TX.
- Barbee, D. (2007). Disaster response and recovery: strategies and tactics for resilience. *UNCP/JHSEM*: Vol. 4, No. 1, Article 11.
- Blanchard, B. W. (2007). *Background "think piece" for the emergency management roundtable meeting: "what is emergency management?" and "what are the principles of emergency management?"*. Emmitsburg, Maryland: Emergency Management Institute, FEMA, Department of Homeland Security.
- Bridging the Gap. (2010). *Developing a tool to support local civilian and military disaster preparedness*. RAND Center for Military Health Policy Research.
- Calvano, C. N. and John, P. (2004). Systems engineering in an age of complexity. *Systems Engineering*, Vol. 7, No. 1, 2004. Wiley Periodicals, Inc., USA.
- Civil Support*. (2007). Joint Publication 3-28. Joint Chiefs of Staff.
- Counterterrorism*. (2009). Joint Publication 3-26. Joint Chiefs of Staff.
- Counterinsurgency Operations*. (2009). Joint Publication 3-24. Joint Chiefs of Staff.

- Civil Support Operations*. (2010). Field Manual 3-28. Headquarters, Department of the Army.
- Committee on Homeland Security and Governmental Affairs. (2006). *Hurricane Katrina: A nation still unprepared*. Washington: United States Senate.
- Comprehensive emergency management. a governor's guide*. (1979). Washington, D.C.: National Governors' Association Center for Policy Research.
- Crowne, S. S. (2011). *Research and statistics: generalizability and how it relates to validity. pediatrics in review*. Retrieved from <http://pedsinreview.aappublications.org/content/31/8/335.full>
- Combined arms operations in urban terrain*. (2011). Army Tactics, Techniques, and Procedures (ATTP) 3-06.11. Headquarters, Department of the Army.
- Desch, M. C. (2001). *Soldiers in cities: military operations on urban terrain (Chapter 1: Why MOUT Now?)*. Strategic Studies Institute, U.S. Army War College. Retrieved from <http://www.strategicstudiesinstitute.army.mil/pdf/files/pub294.pdf>
- Delk, J. D. (2001). *Soldiers in cities: military operations on urban terrain (Chapter 6: The Los Angeles Riots Of 1992)*. Strategic Studies Institute, U.S. Army War College. Retrieved from <http://www.strategicstudiesinstitute.army.mil/pdf/files/pub294.pdf>
- Dhar, S.B. (1979). Power system long-range decision analysis under fuzzy environment. *IEEE Transactions on Power Apparatus and Systems*, 98(2), 585-596.
- Diallo, S. Y., Padilla, J.J., Bozkurt, I. and Tolk, A. (2013). *Modeling and simulation as a theory building paradigm*. In A. Tolk (Ed.), *Ontology, epistemology, and*

teleology for modeling and simulation (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer.

Douglass, S.A. and Mittal, S. (2013). *A framework for modeling and simulation of the artificial*. In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer.

Denzin, N. K. & Lincoln Y. S. (Eds.). (1994). *Handbook of qualitative research*. Thousand Oaks, CA: Sage.

DHS strategic plan. (2012). Fiscal Years 2012-2016. Department of Homeland Security.

Drobne, S. and Lisec, A. (2009). Multi-attribute decision analysis in GIS: weighted linear combination and ordered weighted averaging. *Informatica*, 33, 459–474.

DoD Dictionary of military and associated terms. (2010). Joint Publication 1-02. Joint Chiefs of Staff.

Emergency support function-13. (2008). Public Safety and Security Annex. Department of Homeland Security.

Emergency services sector-specific plan. (2010). *An annex to the national infrastructure protection plan*. Department of Homeland Security.

Emergency Management. (2011). Definition, vision, mission, principles. principles of emergency management working group presentation. Retrieved from www.iaem.com/.../PrinciplesofEmergencyManagementAug2011.ppt

Edson, R. (2008). *Systems thinking*. Version 1.1. ASysT Institute. Retrieved from http://www.anser.org/docs/systems_thinking_applied.pdf

Farber, D. (2006). *"This isn't representative of our department"*. *Lessons from Hurricane Katrina for police disaster response planning*. Retrieved from <http://www.law.berkeley.edu/library/disasters/Anderson.pdf>

Forensic, Forensic Science. (n.d.). Retrieved from <http://www.forensicscience.net/career-description>

Federal emergency management agency (FEMA) brochure. (2008). FEMA B-653 / July 2008. Department of Homeland Security.

Fundamentals of emergency management. (2011). Independent Study 230.b. FEMA, Department of Homeland Security.

FEMA strategic plan. (2011). Fiscal Years 2011-2014. Department of Homeland Security.

FEMA Pub 1. (2010). The Federal Emergency Management Agency Publication 1. Department of Homeland Security, Washington, DC.

Folger, P. (2009). *Geospatial information and geographic information systems (GIS): Current issues and future challenges*. *Congressional Research Service (CRS) report for Congress*. Retrieved from <http://www.fas.org/sgp/crs/misc/R40625.pdf>

Fisher, R.E., Buehring, W.A., Bassett, G.W., Dickinson, D.C., Haffenden, R.A., Klett, M.S. and Lawlor, M.A. (2009). *Constructing vulnerability and protective measures indices for the enhanced critical infrastructure protection program*. ANL/DIS-09-4. Argonne, Illinois: Argonne National Laboratory.

Genova, K.; Vassilev, V.; Andonov, F.; Vassileva, M.; Konstantinova, S. (2004). A Multicriteria Analysis Decision Support System. Retrieved from <http://ecet.ecs.ru.acad.bg/cst04/Docs/sIIIA/310.pdf>

- Gap Assessment in the Emergency Response Community*. (2010). Gap Analysis Report Prepared for the U.S. Department of Homeland Security by Pacific Northwest National Laboratory. Richland, Washington.
- Gigerenzer, G. and Goldstein, D. G. (2011). The recognition heuristic: A decade of research. *Judgment and Decision Making*, Vol. 6, No. 1, January 2011, pp. 100–121.
- Gigerenzer, G. and Gaissmaier, W. (2011). Heuristic decision making. *Annu. Rev. Psychol.* 2011.62:451-482.
- Graumann, A., Houston T., Lawrimore, J., Levinson, D., Lott, N., McCown, S., Stephens, S. and Wuertz, D. (2005). Hurricane Katrina, a climatological perspective. Preliminary Report. NOAA's National Climatic Data Center.
- Griffin, D., Shaw, P. and Stacey, R. D. (2000). Complexity of management. Fad or radical challenge to systems thinking? Routledge. Taylor and Francis Group.
- Gheorghe, A. and Vamanu, D. (1996). *Emergency Planning Knowledge*. Zurich: VDF
- Guard Duty*. (1971). Field Manual 22-6. Headquarters, Department of the Army.
- Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, Volume 8, Number 4, (597-607).
- Hidek, M. A. (2010). *Cultures of security: military tactics and city planning in lower Manhattan since 11 September 2001*. Dissertation. Graduate School of Syracuse University
- Hester, P. T. (2010). *Decision tree primer 2*. Norfolk: Department of Engineering Management and Systems Engineering, Old Dominion University.

Homeland security: physical security. (2003). Prevention and restoration report.

Network Reliability and Interoperability Council VI (Focus Group 1A). Retrieved from

www.nric.org/fg/charter_vi/.../9_15_03_KARL_RAUSCHER_fg1a.p...

Homeland Security. (2005). *Joint Publication 3-26.* Joint Chiefs of Staff.

Homeland Defense. (2007). *Joint Publication 3-27.* Joint Chiefs of Staff.

Hofmann, M. (2013). *Ontologies in modeling and simulation: an epistemological perspective.* In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 59-87). Heidelberg, New York, Dordrecht, London: Springer.

Health, B.L. and Jackson, R.A. (2013). *Ontological implications of modeling and simulation in postmodernity.* In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer.

Hurricane Katrina: DoD Disaster Response. (2005). Congressional Research Service Report for Congress. Retrieved from

<http://www.fas.org/sgp/crs/natsec/RL33095.pdf>

Hurricane Katrina. (2006). Service assessment. National Oceanic and Atmospheric Administration (NOAA) National Weather Service (NWS), Silver Spring, Maryland. Retrieved from

<http://www.nws.noaa.gov/os/assessments/pdfs/Katrina.pdf>

Hurricane Katrina: Managing Law Enforcement and Communications in a Catastrophe. (2006). Hearing before the committee on Homeland Security and Governmental Affairs United States Senate. Retrieved from

<https://bulk.resource.org/gpo.gov/hearings/109s/27025.pdf>

Hake, R.R. (2009). *Over two-hundred annotated references on systems thinking*.

Retrieved from www.physics.indiana.edu/~hake/200RefsSystems2c.pdf

Joint Urban Operations. (2009). Joint Publication 3-06. Joint Chiefs of Staff.

Johannessen, J, Olaisen, J. (2005). Systemic Philosophy and the Philosophy of Social Science. Part II: The Systemic Position. Retrieved from

http://www.emeraldinsight.com/journals.htm/journals.htm?articleid=1524343&show=html&WT_mc_id=alsoread&PHPSESSID=a8j8kegc37g4rcrppn2rc4al84&&nolog=231901

Joint Operations. (2011). Joint Publication 3-0. Joint Chiefs of Staff.

Johansson, J. (2010). *Risk and vulnerability analysis of interdependent technical infrastructures addressing socio-technical systems*. Doctoral Thesis. Lund University.

Joint Security Operations in Theater. (2010). Joint Publication 3-10. Joint Chiefs of Staff.

Jin, L. (2005). *A fuzzy multi-criteria decision analysis for assessing technologies of air pollution abatement at coal-fired power plants*. Master of Engineering Project. University of Regina.

Kiefer, J. J. (2001). *Urban terrorism: strategies for mitigating terrorist attacks against the domestic urban environment*. Dissertation. Norfolk: Old Dominion University.

Keeney, R.L. (1992). *Value focused thinking: a path to creative decision making*. Cambridge, Massachusetts: Harvard University Press.

- Keating, C.B.; Sousa-Poza, A. and Mun, J.H. (2003). Towards a methodology for system of systems engineering. *Proceedings of the American Society for Engineering Management*.
- Korb, K.B., Geard, N., Dorin, A. (2013). *A Bayesian approach to the validation of agent-based models*. In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer.
- Keating, C. B. (2008). Systems analysis perspective for systems analysis. ENMA 715/815. Old Dominion University, Engineering Management & Systems Engineering Department.
- Koksalan, M., Wallenius, J. and Zionts, S. (2011). *Multiple criteria decision making: from early history to the 21st century*. New Jersey: World Scientific.
- Keating, C. B. (2000). A systems-based methodology for structural analysis of health care operations. *Journal of Management in Medicine*, Vol. 14 No. 3/4, 2000, pp. 179-198.
- Lewis, M. P. and Ogra, A. (2010). An approach of geographic information system (GIS) for good urban governance dept. of town & regional planning. University of Johannesburg, Johannesburg, South Africa.
- Linkov I., Steveens. J. (n.d.). *Multi-criteria decision analysis*. Retrieved from http://www.epa.gov/cyano_habs_symposium/monograph/Ch35_AppA.pdf
- Lindsay, B. R. (2010). *U.S. disaster policy: an analysis of federal emergency supplemental appropriations*. Dissertation. University of Delaware.

- Little, R. G. (2004). Holistic strategy for urban security. *Journal of Infrastructure Systems, ASCE, June 2004, 52-59*. doi: 10.1061/(ASCE)1076-0342(2004)10:2(52)
- Law enforcement deployment teams*. (2007). Recommendations for a rapid response law enforcement support system. Major Cities Chiefs Association. Retrieved from https://www.majorcitieschiefs.com/pdf/LEDT_Report_FINAL.pdf
- Law and Order Operations*. (2011). Army Tactics, Techniques, and Procedures (ATTP) 3-39.10. Headquarters, Department of the Army.
- Losee, J. (2001). *A historical introduction to the philosophy of science, fourth edition*. New York: Oxford University Press Inc.
- Laurent, R. (2006). *Elimination by aspects and probabilistic choice*. Retrieved from reynald.laurent.free.fr/EPA_choix_proba_short_GB2.pdf
- Laszlo, K. C. (1998). *Dimensions of systems thinking*. Retrieved from http://archive.syntonyquest.org/elcTree/resourcesPDFs/Systems_Thinking.pdf
- LSP Hurricane Katrina timeline of events*. (2005). Department of Public Safety and Corrections. Louisiana: Office of State Police.
- McEntire, D. A. (n.d.). *Emergency management in the United States: disasters experienced, lessons learned, and recommendations for the future*. Retrieved from www.iapa-il.org/news/ComparativeEM_Book.pdf
- McEntire, D. A. & Marshall, M. (2003). Epistemological problems in emergency management: Theoretical dilemmas and implications. *ASPEP Journal*, p. 119-129.
- McEntire, D. A. (2004). *The status of emergency management theory:*

issues, barriers, and recommendations for improved scholarship. Retrieved from <http://www.training.fema.gov/emiweb/downloads/David%20McEntire%20-%20%20Status%20of%20Emergency%20Management%20Theory.pdf>

McGill, W. L. (2008). *Critical asset and portfolio risk analysis for homeland security*. Dissertation. University of Maryland.

Malczewski, (1999). *Multi-criteria decision analysis*. Retrieved from <http://www.spatial.redlands.edu/sds/SDSSMethodsAndTechniquesMulticriteriaDecisionAnalysis.aspx>

Moffat, J. (2008). *The response to Hurricane Katrina: A case study of changing C2 maturity*. Hampshire, United Kingdom: Defence Science and Technology Laboratory.

Mener, A.S. (2007). Disaster response in the United States of America: An analysis of the bureaucratic and political history of a failing system. *College Undergraduate Research Electronic Journal*. University of Pennsylvania. Retrieved from repository.upenn.edu/cgi/viewcontent.cgi?article=1068&context...

Machamer, P, 1998, Philosophy of science: An overview for educators. *Science & Education*, 7, 1-11. Retrieved from http://web.utk.edu/~appalsci/docs/Philosophy_Sci_Machamer_98.pdf

M'Pherson, P. K. (1974). A perspective on systems science and systems philosophy. *Futures*, June 1974, pp. 219-239.

Merriam-Webster, Axiology. (n.d.). Retrieved from <http://www.merriam-webster.com/dictionary/axiology>

Merriam-Webster, Forensic. (n.d.). Retrieved from

<http://www.merriam-webster.com/dictionary/forensic>

Mitroff, I. I. (1998). *Solving the right problems. Innovative Leader* (328), Volume 7, Number 3.

Military Police Operations. (2001). Field Manual 3-19.1. Headquarters, Department of the Army.

Military Police Leaders' Handbook (Incl Chg 1). (2002). Field Manual 3-19.4. Headquarters, Department of the Army.

Manning, R. A. (2012). *Envisioning 2030: US strategy for a post-western world*. A report of the strategic foresight initiative. Atlantic Council. Retrieved from http://www.acus.org/files/publication_pdfs/403/Envisioning2030_web.pdf.pdf

National strategy for the physical protection of critical infrastructures and key assets. (2003). The White House/ Washington.

National preparedness, presidential policy directive (PPD-8). (2011). The White House, Washington.

Neiman, M. (2001). *Soldiers in cities: military operations on urban terrain (Chapter 10: Urban operations: Social meaning, the urban built form, and economic function)*. Strategic Studies Institute, U.S. Army War College. Retrieved from <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub294.pdf>

National response framework. (2008). Department of Homeland Security.

National incident management system. (2008). Department of Homeland Security.

National strategy for homeland security. (2002). The White House, Washington.

National strategy for homeland security. (2007). The White House, Washington.

- NATO CBRN Forensics capability roadmap report.* (2012). Serial Nu: AC/225(CBRND)D(2012)0001 (PFP). North Atlantic Council.
- National strategy for combating terrorism.* (2006). The White House, Washington.
- National security strategy.* (2010). The White House, Washington.
- National infrastructure protection plan.* (2006). Department of Homeland Security.
- National infrastructure protection plan.* (2009). Partnering to enhance protection and resiliency. Department of Homeland Security.
- National response framework.* (2012). Pre-decisional working draft. Department of Homeland Security.
- National response plan.* (2004). Department of Homeland Security.
- Nelson, R.O., Bodurian, B., and McEvoy, A. (2010). *Five years after Katrina.* Commentary. Washington: Center for Strategic and International Studies (CSIS).
- National preparedness.* (2003). Homeland Security Presidential Directive (HSPD-8). The White House, Washington.
- Oscar, C. T. (2006). *Post Katrina: Redefining the military role in homeland security.* USAWC Strategy Research Project. Carlisle Barracks, Pennsylvania. Retrieved from <http://www.strategicstudiesinstitute.army.mil/pdf/files/ksil447.pdf>
- Operations.* (2011). Field Manual 3-0. Headquarters, Department of the Army.
- Overview of triangulation methodology.* (n.d.). Retrieved from http://gametlibrary.worldbank.org/files/67_Triangulation%20Guidelines-CDC.pdf
- Offense and defense.* (2012). Army Doctrine Reference Publications (ADRP) 3-90. Headquarters, Department of the Army

- Oren, T. and Yilmaz, L. (2013). *Philosophical aspects of modeling and simulation*. In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer
- Pickup, S. (2006). *Hurricane Katrina: Better Plans and exercises need to guide the military's response to catastrophic natural disasters*. Retrieved from <http://www.gao.gov/assets/90/82271.pdf>
- Posen, B. R. (2001). *Soldiers in cities: military operations on urban terrain (Chapter 11: Urban Operations: Tactical realities and strategic ambiguities)*. Strategic Studies Institute, U.S. Army War College. Retrieved from <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub294.pdf>
- Protection*. (2009). Army Doctrine Reference Publications (ADRP) 3-37. Headquarters, Department of the Army.
- Police intelligence operations*. (2010). Army Tactics, Techniques, and Procedures (ATTP) 3-39.20. Headquarters, Department of the Army.
- Pyka, A. and Deichsel, S. (2013). *Cutting back models and simulations*. In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer.
- Physical security*. (2001). Field Manual 3-19.30. Headquarters, Department of the Army.
- Physical security handbook*. (2005). 440-2-H. U.S. Geological Survey Manual.
- Physical security*. (2010). Army Tactics, Techniques, and Procedures (ATTP) 3-39.32. Headquarters, Department of the Army.

- Post-Katrina emergency management reform act.* (2006). Title VI-National Emergency Management. Retrieved from <http://www.vacationlanegrp.com/pdf/getdoc-fema.pdf>
- Philosophy, Dictionary. (n.d.). Retrieved from <http://dictionary.reference.com/browse/philosophy>
- Quadrennial homeland security review report.* (2010). *A Strategic Framework for a Secure Homeland.* Department of Homeland Security.
- Rapid visual screening of buildings for potential seismic hazards seismic hazards.* (2002). A Handbook, FEMA 154, Edition 2. Department of Homeland Security.
- Ruona, W. E. A. & Lynham, S. A. (2004). A philosophical framework for thought and practice in human resource development. *Human Resource Development International*, 7(2), 151-164.
- Saaty, T. L. (2005). *Theory and applications of the analytic network process.* Pittsburgh, Pennsylvania.
- Strategic guidance.* (2012). Sustaining U.S. global leadership: priorities for 21st century defense. White House, Washington.
- Stability operations.* (2008). Field Manual 3-07. Headquarters, Department of the Army.
- Stability operations.* (2011). *Joint Publication 3-07.* Joint Chiefs of Staff.
- Smith, B. (2003). *Ontology.* In L. Floridi (Ed.), *Blackwell guide to the philosophy of computing and information*, p. 155-166, Oxford: Blackwell.
- Smith, R. (2013). *On the value of taxonomy in modeling.* In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer.

- Solem, O. (2003). Epistemology and logistics: A critical overview. *Systemic Practice and Action Research*, 16(6), 437-454.
- Szabo, C. and Teo, Y.M. (2013). *Semantic validation of emergent properties in component-based simulation models*. In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer.
- Secilmis, M. (2012). The need for a holistic vision. *Transformer*, Vol. 8, Issue 1, 2012. Retrieved from <http://www.act.nato.int/transformer-2012-01/article-18a>
- Secilmis2, M. (2012). Complexity of post-disaster security environment and law enforcement. *Transformer*, Vol. 8, Issue 2, 2012. Retrieved from <http://www.act.nato.int/transformer-2012-02/article-2012-2-27>
- Systems analysis*. (2010). Guidance: Research paper on systems philosophy requirements and preparation. ENMA 815. Norfolk: Old Dominion University.
- Select Bipartisan Committee. (2006). *A failure of initiative: final report of the Select Bipartisan Committee to investigate the preparation for and response to Hurricane Katrina*. Washington.
- Urban operations*. (2006). Field Manual 3-06, Headquarters, Department of the Army.
- Unified facilities criteria*. (2012). UFC 4-010-01. DoD Minimum Antiterrorism Standards for Buildings. Department of Defence.
- Thirunavukarasu, P. (n.d.). *An integrated approach to disaster management, madras medical college*. Retrieved from <http://www.icm.tn.gov.in/article/disaster.htm>
- The federal response to Hurricane Katrina: Lessons learned*. (2006). The report of department of homeland security. White House, Washington.

- Terrorism incident law enforcement and investigation annex.* (2004). National Response Plan. Department of Justice.
- The operations process.* (2012). Army Doctrine Reference Publications (ADRP) 5-0. Headquarters, Department of the Army.
- Tactics in counterinsurgency.* (2009). Field Manual 3-24.2. Headquarters, Department of the Army.
- Tactics.* (2001). Field Manual 3-90. Headquarters, Department of the Army.
- The infantry rifle platoon and squad.* (2007). Field Manual 3-21.8. Headquarters, Department of the Army.
- Timeline Hurricane Katrina history.* (2005). The People History. Retrieved from <http://www.thepeoplehistory.com/timelines/hurricanekatrina.html>
- Hurricane Katrina timeline.* (2005). The Brookings Institution. Retrieved from www.brookings.edu/fp/projects/homeland/katrinatimeline.pdf
- Philosophy. The Free Dictionary.* (n.d.). <http://www.thefreedictionary.com/philosophy>
- Tolk, A. (2013). *Ontology, epistemology, and teleology for modeling and simulation.* Heidelberg. New York, Dordrecht, London: Springer
- Wang, W., Wang, W., Li, Q., and Yang, F. (2013). *Ontological, epistemological, and teleological perspectives on service-oriented simulation frameworks.* In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer.
- Weck, O.L., Roos, D., Magee and C.L. (2011). *Engineering systems: meeting human needs in a complex technological world.* England: The MIT Press.

- Weirich, P. (2013). *Models as partial explanations*. In A. Tolk (Ed.), *Ontology, epistemology, and teleology for modeling and simulation* (pp. 89-103). Heidelberg, New York, Dordrecht, London: Springer.
- Wigginton, M. P. (2007). *The New Orleans police response to Hurricane Katrina: A case study*. Dissertation. The University of Southern Mississippi.
- Wombwell, J. A. (2009). *Army support during the Hurricane Katrina disaster*. The Long War Series Occasional Paper 29. Kansas: US Army Combined Arms Center Combat Studies Institute Press.
- Wollman, L.F. (n.d.). *Research paradigms*. Retrieved from https://www.chds.us/coursefiles/research/lectures/research_paradigms/script.pdf
- What is emergency management*. (n.d.). NEMA, National Emergency Management. Retrieved from <http://www.nemaweb.org/>
- Ye, C. (2006). *Multiple criteria decision analysis: Classification problems and solutions*. Waterloo, Ontario, Canada.
- Yeh, C.H.; Deng, H. (1997). *An algorithm for fuzzy multi-criteria decision-making*. IEEE International Conference on Intelligent Processing Systems October 28 – 31. Beijing, China.
- Yoe, C. (2002). *Trade-off analysis planning and procedures guidebook*. Retrieved from <http://www.iwr.usace.army.mil/docs/iwrreports/02-R-2.pdf>
- Zadeh, L.A. (1965). Fuzzy sets. *Information and Control*, 8, 338-353. Retrieved from www-bisc.cs.berkeley.edu/Zadeh-1965.pdf

APPENDIX A - BACKGROUND INFORMATION FOR THE SPECIFICATION OF ANALYSIS PROBLEMS

1. General and Coordination Issues:

The past three decades have presented the emergency management community with significant challenges and conditions that have necessitated reevaluation of strategic and operational approaches to delivering emergency management services. (FEMA Strategic Plan, 2011, p. 1)

This country has had a great deal of experience with disasters, and it has been – in many instances – both innovative and successful in emergency management. In spite of its many advances in this burgeoning profession, the U.S. suffers from many problems that are both unique and similar to those that affect other countries. In addition, the U.S. has witnessed numerous setbacks and disappointing mistakes from which others may learn. (McEntire, (n.d.), p. 1)

While the United States has been a model for emergency management programs around the world, it is not without numerous weaknesses. The emergency management profession has much room for improvement in the U.S. as it does elsewhere. (McEntire, (n. d.), p. 18)

Topics such as the National Incident Management System (NIMS) and the National Response Plan (NRP) are clearly and effectively described and explained, but virtually no research seems available to offer emergency managers concerning the usefulness or performance in practice of NIMS and NRP. (Barbee, 2007, p. 4)

Homeland security is a step back from the proactive approaches being recommended today, and it de-emphasizes all hazards other than terrorism. This rivalry among divergent and incomplete paradigms has created confusion for a discipline that so desperately needs both inclusion and direction. (McEntire, 2004, p. 8)

On the domestic front, federal security planners faced what seemed like an infinite amount of pressing tasks, with no real ability to determine whether or not their work would turn out to be something like a military victory. Federal planners also faced a serious dilemma concerning the comprehensive nature of the homeland security mission, the sheer number of agencies involved at all levels of government, and extensive private sector involvement. Furthermore, the complicated daily workings of the Homeland Security Council and the President's Office of Homeland Security were accompanied by a maze-like jumble of congressional oversight and appropriations committees. (Hidek, 2010, p. 102)

Another problem that must be addressed is coordination among all of the actors involved in emergency management in the United States. Ways must be found to improve communication among all pertinent actors during disasters and work harmoniously to promote recovery in the aftermath of such events. (McEntire, (n. d.), p. 17)

As currently structured, the degree of fragmentation and antagonism between DHS and its institutional subcomponents have created a veritable 'uncoordinated network. (Hidek, 2010, p. 212)

The pre-9/11 planning designed to meet the new governmental mission of 'homeland defense' focused on developing an 'integrated intelligence' and planning capability to support tactical antiterrorism objectives. The result was the emergence of a complex web of institutional relationships, generating clashes to come over function, purpose, and influence. (Hidek, 2010, p. 99)

The American disaster response system functions admirably during the vast majority of disasters. The system quickly arranges for emergency shelter, food distribution, medical care, and monetary distributions to disaster victims. However, the disaster response system is imperfect since the coordination of these fragmented resources is extremely cumbersome. (Mener, 2007, p. 56)

Since 9/11, the principles of transparency, cooperation, and collaboration at the core of disaster management appear to be replaced a new command-and-control-based domestic security system. Furthermore, security initiatives to protect cities have gone forward following the creation and subsequent reorganization of DHS, complicating shared governance. (Hidek, 2010, p. 51)

As we continue to search for more optimal pathways, we can expect domestic preparedness to be complicated by a national system where disasters are governed by multiple regulations – namely the Stafford Act, the Homeland Security Act of 2002, the Post Katrina Emergency Management Reform Act of 2006, and the National Response Framework. These many plans reflect the long history of U.S. disaster policy, through which competing interests and groups have been cobbled together to build new agencies, and layers of statutes have been built upon existing guidelines without modifying previous statutes or reassessing the assumptions upon which they rest. (Hidek, 2010, p. 253)

2. Poor Policy Formulation (Epistemological Problems) and Lack of Training

The United States must acknowledge that disaster losses are rising and that a more proactive approach will be required (p. 17). Policy makers need to develop a more coherent disaster policy that is integrated at all levels of government (p. 18). Instead of writing emergency operations plans, we need to find ways to reduce vulnerability and enhance capabilities. (McEntire, (n.d.), p. 17)

If you surveyed my American colleagues, you would find little to no understanding of the disaster response system. Virtually nobody has read the 426 page all-hazards plan titled the National Response Plan, and with the exception of some major cities, few emergency response agencies have reinforced or protected emergency infrastructure. (Mener, 2007, p. 2)

Poor policy formulation and lack of training limit the ability of public officials to prevent disasters or react to them in an effective manner. (McEntire, (n.d.), p. 4)

There is not an established Emergency Management Doctrine. (Blanchard, 2007, p. 3)

Although there is obviously a need to develop a theory of emergency management, there is no guarantee that this task will be easy. In fact, there are several major epistemological problems that are hindering the development of knowledge in this area. (McEntire, 2004, p. 5)

To be successful, emergency managers need sufficient knowledge, training, and experience to be able to navigate within the bigger waters. (Blanchard, 2007, p. 3)

An epistemological hurdle hinges on the definition of emergency management, which is analogous to the conceptual problem of disaster. The term emergency management has at least two significant defects. The very name of the field we study is a misnomer. Emergency managers are not really concerned about emergencies; they are instead interested in larger events that have community-wide impact. (McEntire and Marshall 2003, p. 222)

There are serious epistemological problems facing those who study emergency management. These challenges range from disagreement about theoretical concepts and faulty assumptions about the human role in disasters to disputes about the inclusion of various disciplines and the relative merit of competing paradigms. (McEntire and Marshall 2003, p. 226)

Emergency Management is an oxymoron. It may unintentionally suggest that we can control or always effectively deal with extreme events. While it is true that we are able to prevent some disasters or reduce their adverse impacts, we are less likely to manage our responses to these events in a totally effective manner. (McEntire and Marshall 2003, p. 223)

The term “emergency management” has at least three significant problems. First, as scholars we are really interested in disasters, not emergencies. Second, the focus on “emergency” makes the field reactive and limits its applicability to first responders. Third, emergency management may imply that we have total control in our ability to deal with the adverse occurrences we call disasters. Hence, emergency management is both a misnomer and an oxymoron. But a suitable replacement has not been found, and one may never be accepted due to the increasing professional recognition of the name emergency management. (McEntire, 2004, p. 5)

The current language of emergency management (and homeland security) seems to confirm the theorems suggested by Kaplan (Baird, 2010, p. 42):

Theorem 1: 50% of the problems in the world result from people using the same words with different meanings.

Theorem 2: The other 50% comes from people using different words with the same meaning.

The four phases of emergency management present an additional epistemological problem and the complexities of these phases have already been explored by researchers in terms of overlap and fluidity. (McEntire and Marshall 2003, p. 224)

Although the “four phases” are part of the common language and theoretical underpinning of emergency management in the U.S., a number of adaptations can be found. Some sources now refer to five phases rather than four. Others have changed the descriptive terms for one or more of the phases. Important sources appear to disagree on the language, and a number of government publications examined as part of this research are more confusing than informative. (Baird, 2010, p. 7)

Adding to the confusion, the core National Response Framework document also refers to “the three phases of effective response: prepare, respond, and recover”. That is not a typo, three phases of response. (Baird, 2010, p. 10)

Confusing matters a bit, after the creation of the Department of Homeland Security, RAND Corporation employees under contract to DHS to develop the National Response Plan and the National Incident Management System invented their own terminology – what I call the Five Phases of Homeland Security: Prevention, Mitigation, Readiness, Response and Recovery. This new terminology was invented, according to those I have communicated with

who came into contact with RAND personnel during the review phase of the earlier conceptions of the NRP, to play to the law enforcement and intelligence communities and their mission of preventing terrorism. As noted earlier, emergency management and homeland security are not synonymous. The newly invented Five Phases of Homeland Security operate within Homeland Security and do not supplant or replace the Four Phases of Emergency Management – which is, again, all-hazards, all-phases, all-actors. (Blanchard, 2007, p. 19)

Despite having responded to thousands of natural disasters and numerous terrorist attacks, at present the United States government at the federal, state, and local levels is exceedingly unprepared to handle the immediate aftereffects of disasters. The federal government has created numerous large bureaucracies and congressional panels as well as generated hundreds of official reports each of which purports to detail appropriate disaster response guidelines. Nonetheless, the improvements since the first disaster response plan was implemented during World War I are not palpable. (Mener, 2007, p. 3)

Blanchard (2007) acknowledges the communication of Mike Selves, the Emergency Manager for Johnson County Kansas, and President of the International Association of Emergency Managers, a summary follows as:

...Our current problems with FEMA and the role of emergency management in the federal structure stems, in my humble opinion, almost entirely from the lack of any generally understanding or acceptance of these basics... We are requiring NIMS training of virtually everyone in the country, what good is NIMS training if you don't understand the context within which NIMS must operate. The current screw up of preparedness and response concepts at the Federal level is due to this problem of defining everything using an "emergency services" first responder framework. Our efforts on Capitol Hill have only born any fruit at all because we are finally getting some key members and staffers to understand this bigger picture. The system is not failing because first responders need more attention; it is failing because the coordinators and decision-makers need more attention... (p. 2)

...one of the biggest challenges emergency managers face, as a profession, is dispelling the misconception that our function is simply the sum total of the efforts and resources of the emergency services. The public can identify with firefighters, police and EMTs. However, the idea that there is a profession of public administration, called Emergency Management, whose job is to facilitate the creation of basic disaster policy framework and to coordinate the implementation of the policy during a disaster, is not well understood. Our job ties together not only the responders but also the decision makers, public and private agencies not normally associated with emergency response and a whole array of other elements of the local community before, during and after any disaster event... (p. 6)

APPENDIX B - SECURITY OPERATIONS

During the long history of Homeland Security, including 'disaster response,' which dates back to 1800s, military doctrine has had a significant role in the development of relevant concepts linked to disaster response activities, particularly Public Safety and Security. As Neiman (2001) and Hidek (2010) discussed in a similar way, Mener (2007) highlights the security aspects of the military doctrine on the disaster management:

The overwhelming influence of the military doctrine on the disaster management and security related planning efforts is undeniable since the historical references of the military knowledge dates back for a long time. When federal disaster management was necessary, the military was the primary coordinator and source of manpower. (p. 7)

In the military literature, although 'security' usually implies defensive characteristics,⁴³ it is one of the twelve principles of Joint Operations. *Joint Publication 3-0 (Joint Operations, 2011)* states "the purpose of security is to prevent the enemy from acquiring unexpected advantage; security enhances freedom of action by reducing friendly vulnerability to hostile acts, influence, or surprise" (p. A-3), while *Offense and Defense (2012)* states "the ultimate goal of security operations is to protect the force from surprise and reduce the unknowns in any situation. Security operations encompass five tasks: screen, guard, cover, area security, and local security" (p. 5-3). In the context of the Joint Security Operations concept, the key joint security related functions and nodes are depicted in Figure 36.

⁴³ There are five general characteristics of the successful defense: preparation, security, disruption, massing effects, and flexibility (Urban operations, 2006, p. 8-1).

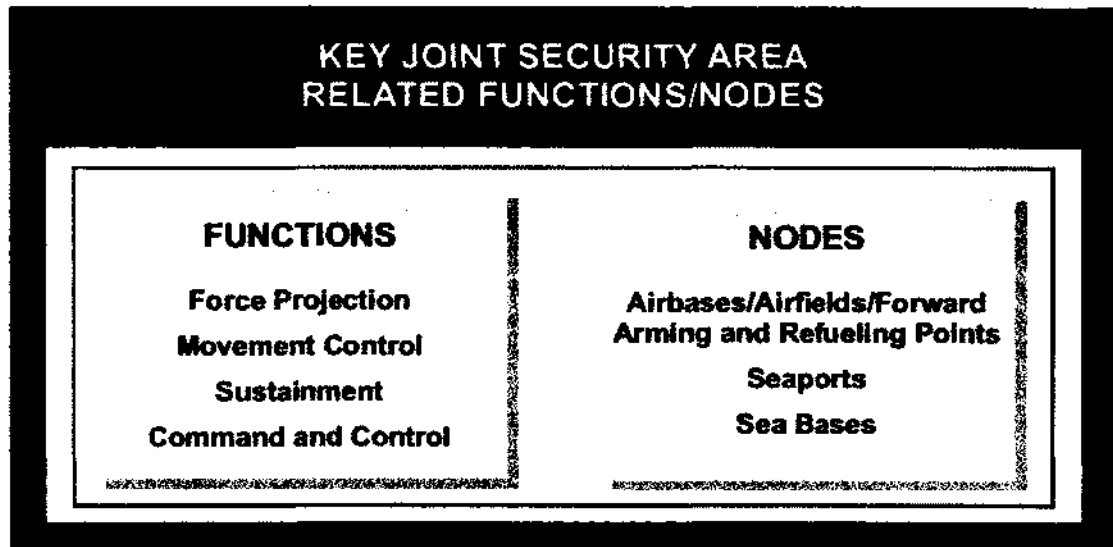


Figure 36 Key Joint Security Functions and Nodes (Joint Security Operations in Theater, 2010, p. I-6)

Stability Operations (2008) defines the basic elements of the security sector and their characteristics: “The security sector consists of both uniformed forces - police and military - and civilian agencies and organizations operating at various levels within the operational environment. Elements of the security sector are interdependent; the activities of one element significantly affect other elements” (p. 6-13). In a wider context, the excerpts in Table 17 provide a panoramic perspective for the concept of Security Operations, which has been delineated in various military references.

Table 17 Security Operations

<p>JP 3-07, Stability Operations, (2011)</p>	<p>Population Security. To provide protection to the population, JFCs employ a range of techniques (p. III-15);</p> <ol style="list-style-type: none"> (1) Static protection of key sites (e.g., market places or refugee camps) (2) Persistent security in areas secured and held (e.g., intensive patrolling and check points) (3) Targeted action against adversaries (e.g., search or strike operations) (4) Population control measures (e.g., curfews and vehicle restrictions).
<p>JP 3-10, Joint Security Operations in Theater, (2010)</p>	<p>Active Security. The active Lines of Communications (LOC) security techniques include measures initiated to achieve positive control of the LOCs and reduce the threat. Active security includes (p. V-4);</p> <ol style="list-style-type: none"> (1) Patrols (2) Snipers (3) Fighting positions along LOCs (4) Check points (5) Route sweeps
<p>FM 3-07.31, Peace Operations Multi-Service Tactics, Techniques, and Procedures for Conducting Peace Operations (w/change 1), (2003)</p>	<p>Fixed Site Security techniques. Commanders may combine and vary these techniques according to the local situation (p. III-3);</p> <ol style="list-style-type: none"> (1) Periodic observation by patrols, to include over flights (2) Obstacles (3) Electronic monitoring (4) Guards – periodic or permanent (5) Patrols should make periodic, random checks of guard posts
<p>FM 3-21.8, The Infantry Rifle Platoon and Squad, (2007)</p>	<p>Techniques used to perform Security Operations are (p. H-2);</p> <ol style="list-style-type: none"> (1) Observation post (2) Combat outpost (3) Battle position (4) Patrols (5) Combat formations (6) Movement techniques (7) Infiltration (8) Movement to contact (9) Dismounted, mounted, and air insertion (10) Roadblocks (11) Checkpoints (12) Convoy and route security (13) Searches

Table 17 Continued

<p>ADRP 3-90, Offense and Defense, (2012)</p>	<p>Security operations encompass five tasks (p. 5-3);</p> <ol style="list-style-type: none"> (1) Screen (2) Guard (3) Cover (4) Area security (5) Local security
<p>FM 3-21.8, The Infantry Rifle Platoon and Squad, (2007)</p>	<p>Security in the defense includes all active and passive measures taken to avoid detection by the enemy, deceive the enemy, and deny enemy reconnaissance elements accurate information on friendly positions. The two primary tools available to the platoon leader are Observation Posts and Patrols (p. 8-21).</p>
<p>ATTP 3-39.10, Law and Order Operations, (2011)</p>	<p>Law Enforcement specific activities include (p. 3-8);</p> <ol style="list-style-type: none"> (1) Police station operations (2) LE patrolling (3) Traffic enforcement operations (4) Criminal investigations (5) Employment of forensic and biometric capabilities (6) Detention cell operations
<p>FM 3-19.4, Military Police Leaders' Handbook, (2002)</p>	<p>Area Security. Military Police activities that support Area Security include reconnaissance operations, Area Damage Control (ADC), base and Air Base Defense (ABD), response force operations, and critical site asset and high-risk personnel security (p. 6-1).</p>
<p>FM 3-24.2, Tactics in Counterinsurgency, (2009)</p>	<p>Security. Early warning of pending actions ensures the base commander time to react to any insurgent threat. Outposts, patrols, ground surveillance and counter mortar radar, military working dogs teams, and air reconnaissance and surveillance provide early warning (p. 6-11).</p>
<p>FM 3-19.1, Military Police Operations, (2001)</p>	<p>Military Police support law-enforcement operations by (p.3-2);</p> <ol style="list-style-type: none"> (1) Providing liaison teams with local, state, and federal agencies; Host Nation police; and joint and multinational agencies. (2) Employing Special Reactions Teams and hostage-negotiation teams. (3) Providing traffic enforcement, Main Supply Route regulation enforcement, and other route-control measures. (4) Employing Military Working Dogs. (5) Conducting Military Police investigations (criminal and noncriminal). (6) Conducting patrolling, area security, and surveillance measures. (7) Implementing applicable threat-condition measures. (8) Conducting and implementing other law-enforcement measures as required by the commander.

As a snapshot that epitomizes the whole picture, the techniques or missions employed in security operations could be classified into four groups: active security, early warning, static physical security and other techniques (listed in Table 18). Within these techniques, patrol or 'patrolling' is the most significant, and mostly employed technique for uniformed forces to maintain the security of urban areas. The quotes included in Table 19 provide insight that supports the rationale behind this assumption. Usually patrols are executed by the Patrol Divisions of Police Departments in the sectors assigned within borders of the jurisdiction.

Table 18 Security Operations Techniques/Missions

Active Security Techniques	Patrol
	Guard
	Response/Reaction Force
Early Warning Techniques	Intelligence, Surveillance, and Reconnaissance (ISR)
Static Physical Security Techniques	Fences, Barriers, Intrusion Detections Systems, Lighting, etc.
Other Techniques	Curfew, Restrictions, Criminal Investigations, Employment of Forensic and Biometric Capabilities, etc.

Table 19 Patrolling in the Urban Areas

Emergency Support Function #13 (2008)	Providing basic law enforcement assistance to Federal, State, tribal, and local agencies during incidents that require a coordinated Federal response. Such assistance may include conducting routine patrol functions and making arrests as circumstances may require (p. 4).
Norfolk Police Department Annual Report (2010)	Police services are provided to communities using a variety of traditional and non-traditional means, including marked patrol units, bicycle patrol, walking beats, and concentrated enforcement sweeps (p. 34).
Select Bipartisan Committee (2006)	These agencies brought a wide array of capabilities and tactical teams to help restore and maintain law and order. Most of the federal personnel were deputized as state law enforcement officials, so they could fully partner with local police by participating in patrols, investigating crimes, and arresting suspects (p. 242).
	The Louisiana National Guard was deployed before landfall, and provided security at the Superdome that helped maintain order there. Once looting broke out in New Orleans, they also patrolled the streets (p. 242).

In the context of military concept of operations, other techniques like 'Guard' and 'Intelligence, Surveillance, and Reconnaissance' (ISR) are also critical for the sustainment of security. They are usually performed with patrol missions to support each other. The deployment of 'response' or 'reaction' forces is a common practice to maintain the security of military bases or base clusters when necessary. Brief explanatory information is included below:

Patrol. The Infantry Rifle Platoon and Squad (2007) defines 'patrol,' which is the major technique in practice for the execution of security operations:

A patrol is sent out by a larger unit to conduct a specific combat, reconnaissance, or security mission. The terms "patrolling" or "conducting a patrol" are used to refer to the semi-independent operation conducted to

accomplish the patrol's mission. Patrols require a specific task and purpose.
(p. 9-1)

Guard. A guard force is “an effective and useful component of a facility’s physical security program” (Physical Security Handbook, 2005, p. 61). A guard is “a security task to protect the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of and direct fire against the main body” (Offense and Defense, 2012, p. 5-3). Guard is a term used when referring to:

- A special unit responsible to the officer of the day for the protection and security of an installation or area.
- An individual responsible to keep watch over, protect, shield, defend, warn, or any duties prescribed by general orders and/or special orders (Guard Duty, 1971, p. 2-2).

Intelligence, Surveillance, and Reconnaissance (ISR). ISR is “an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations” (Operations, 2011, p. 4-8).

ISR “identifies information gaps and the most appropriate assets for collecting information to fill them; ISR synchronization considers all assets - both internal and external to the organization” (Operations, 2011, p. 4-8). Within this context, satellites, radars, detection sensors, stationary or mobile cameras, unmanned aerial vehicles (UAV), planes, helicopters, etc. are the most common ISR assets utilized in military and police

security operations. Buddelmeyer (2007) underlines the significance of ISR assets which have supported the Hurricane Katrina post-disaster activities:

Hurricane Katrina also demonstrated the exceptional value of military Intelligence, Surveillance and Reconnaissance (ISR) assets for use in disaster relief operations. For the first time, Air Force, Air National Guard, and DHS ISR assets were called to domestic contingency service to provide imagery and full-motion video to military decision-makers and on-scene response providers. (p. 26)

Response/Reaction Force. *Military Police Operations* (2001) states that “a response force is summoned when the base or base cluster is faced with threat forces that are beyond their self-defense capability” (p. 3-7), while *Tactics* (2001) states “the response force moves quickly to counter the enemy before he can extensively damage the base; the base commander lifts or shifts base defense fires to support the maneuver of the response force” (p. E-28). *Tactics in Counterinsurgency* (2009) also defines the Quick Reaction Force (QRF) as “a designated organization for any immediate response requirement that occurs in a designated area of operation; a QRF increases the overall flexibility of a base defense and is available for contingencies” (p. 6-12). In a similar vein, *Physical Security* (2010) groups the forces that respond to major threats on military installations in the following categories (p. 9-3):

- Emergency responders
- Special reaction teams
- Other response forces

APPENDIX C – URBAN AREA DEFENSE

Public Safety and Security in the context of the post-disaster urban environment can be best linked to Urban Area Defense in the military concept of operations. However, as already been said before, there is limited information in the military literature regarding the identification of force tailoring and unit positioning requirements of the troops to be deployed, or security operations techniques which could be executed in the post-disaster urban area.

In the context of Military security concept of operations; the security paradigm is usually managed through the principles of MDMP as a common approach applied for all military actions that requires the commander's decision. For the particular requirements linked to post-disaster urban security, the military references usually advice general approaches and techniques without providing specified direction, guidance, criteria sets, etc.

In this sense, the following paragraphs, which represent the best tangible military considerations, have been excerpted from *Urban Operations* (2006). They could be exploited during the assessment of post-disaster urban security requirements noted in this research:

The urban operational framework - understand, shape, engage, consolidate, and transition - provides structure to developing considerations for defensive operations. The considerations can vary depending on the level of war at which the operation is conducted, the type of defense, and the situation. Most issues discussed may, in the right circumstances, apply to both commanders conducting major Urban Operations and commanders at lower tactical levels of command. (p. 8-9)

The urban operational framework assists commanders in visualizing urban operations. This framework is simply an aid to the commander. It is not

sequential, nor is it a planner's tool for phasing an operation. Commanders should combine the urban operational framework with (p. 6-1):

- The principles of war.
- The tenets of Army operations.
- The components of operational design.
- Considerations for stability operations and civil support operations.
- Sustainment characteristics.
- Running estimates.
- Commander's critical information requirements (CCIR).
- Each commander's experience.

The commander defending in the urban area must assess many factors. His mission statement and guidance from higher commanders help him focus his assessment. If the mission is to deny a threat access to port facilities in an urban area, the commander's assessment will be focused much differently than if the mission is to deny the threat control over the entire urban area. The mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC)⁴⁴ structure guides the commander's assessment. Of these, the impacts of the threat and environment—to include the terrain, weather, and civil considerations—are significant to the commander's understanding of urban defensive operations. (p. 8-9)

In the urban defense, a key element is the commander's understanding of the threat. One of his primary concerns is to determine the attacker's general scheme, methodology, or concept. Overall, the attacker may take one of two approaches. The most obvious would be a direct approach aimed at seizing the objectives in the area by a frontal attack. A more sophisticated approach would be indirect and begin by isolating Army forces defending the urban area. Innumerable combinations of these two extremes exist, but the threat's intentions toward the urban area will favor one approach over another. The defending Army commander (whose AO includes but is not limited to the urban area) conducts defensive planning, particularly his allocation of forces, based on this initial assessment of threat intentions. This assessment determines whether the commander's primary concern is preventing isolation by defeating threat efforts outside the area or defeating a threat attacking the urban area directly. For the higher commander, this assessment determines how he allocates forces in and outside the urban area. For the commander in the urban area, this assessment clarifies threats to sustainment operations and helps shape how he arrays his forces. (p. 8-9)

⁴⁴ METT-TC is a memory aid that identifies the mission variables: Mission, Enemy, Terrain and weather, Troops and support available, Time available, and Civil considerations. It is used in information management (the major categories of relevant information) and in tactics (the major variables considered during mission analysis). Mission analysis describes characteristics of the area of operations in terms of METT-TC, focusing on how they might affect the mission (Operations, 2011, 6-8).

A second key assessment is the defensive qualities of the urban environment. This understanding, as in any defensive scenario, is based on mission requirements and on a systemic analysis of the terrain in terms of observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (**OAKOC**). It is also based on potential chemical, biological, radiological, nuclear and fire hazards that may be present in the urban area. This understanding accounts for the unique characteristics of urban terrain, population, and infrastructure. (p. 8-9)

Generally, units occupy less terrain in urban areas than more open areas. For example, an infantry company, which might occupy 1,500 to 2,000 meters in open terrain, is usually restricted to a frontage of 300 to 800 meters in urban areas. The density of building in the urban area, building sizes and heights, construction materials, rubble, and street patterns will dictate the actual frontage of units; however, for initial planning purposes, Table 20 provides approximate frontages and depths for units defending in an urban area. (p. 8-9)

Table 20 Approximate Defensive Frontages and Depths (Urban Operations, 2006, p. 8-10)

UNIT	Frontage (Blocks*)	Depth (Blocks*)
Battalion	4 – 8	3 – 6
Company	3 – 4	2 – 3
Platoon	1 – 2	1
*Average block is 175 meters		

Furthermore, the intelligence preparation of the battlefield (**IPB**) is a methodology which allows commanders to develop the situational understanding necessary to visualize, describe, and direct subordinates in successfully accomplishing the mission especially when the complexity of the urban environment and increased number of variables (and their infinite combinations) increases the difficulty of providing timely, relevant, and effective intelligence support to urban operations). (p. B-1)

IPB is the systematic process of analyzing the threat and environment in a specific geographic area - the area of operations (AO) and its associated area of interest (see Figure 37). It provides the basis for intelligence support to current and future UO, drives the military decision-making process, and supports targeting and battle damage assessment. The procedure is performed continuously throughout the planning, preparation, and execution of an urban operation. (p. B-1)

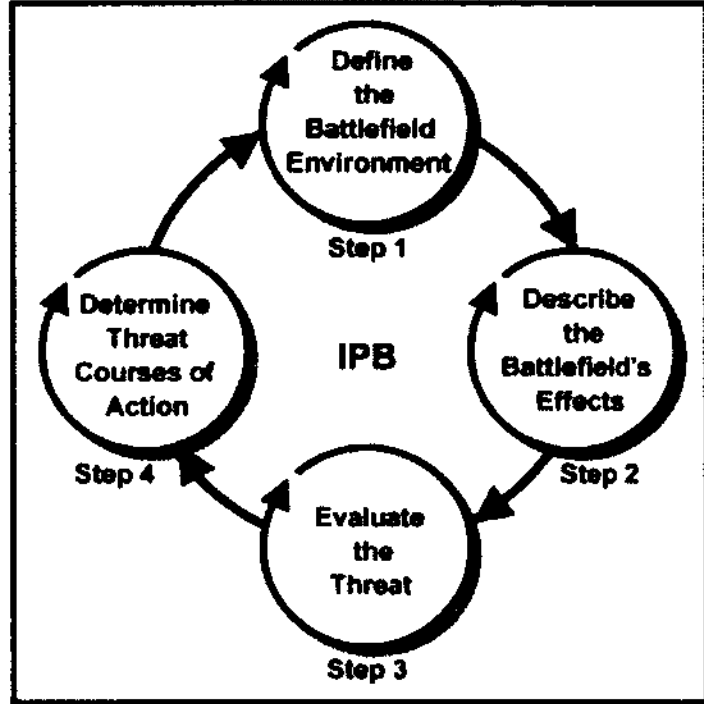


Figure 37 Steps of IPB (Urban Operations, 2006, p. B-1)

APPENDIX D – MEASUREMENT OF BASIC CRITICALITY INDEX (BCI)

The BCI provides a relative score between 0 and 1. BCI, for each critical asset, is obtained through the process of the formula which is included in the relevant key sector/service row at Table 21.

Table 21 Basic Criticality Index (BCI) Assessment Matrix

No	Urban Area Key Sectors/Services	BCI(i)	
1	Governance, Homeland Security, Law Public Order, Emergency Service	BCI1	$S1 \times (SRW1 \cup EW1)$
2	Housing Accommodation	BCI2	$S2 \times (EW2 \cup OW2)$
3	Power/Energy Service (Power plants, nuclear reactors, dams, fuel supply stations, etc.)	BCI3	$S3 \times (SRW3 \cup EW3)$
4	Healthcare and Public Health	BCI4	$S4 \times (SRW4 \cup EW4)$
5	Telecommunication (including Information Technology)	BCI5	$S5 \times (SRW5 \cup EW5)$
6	Transportation/Postal and Shipping Service (including airports, major transportation terminals)	BCI6	$S6 \times (SRW6 \cup EW6)$
7	Food/Water and Other Goods Service (Shopping malls, major retail, etc.)	BCI7	$S7 \times (EW7 \cup SW7)$
8	Banking and Finance (including banks/ATMs, etc.)	BCI8	$S8 \times (SRW8 \cup EW8)$
9	Critical Manufacturing (including major industrial facilities)	BCI9	$S9 \times (EW9 \cup IW9)$
10	Training and Education Activities (including schools)	BCI10	$S10 \times (EW10 \cup STW10)$
11	Worship Activities (Places of worship, etc.)	BCI11	$S11 \times (EW11 \cup SCW11)$
<p>Variables: Si: Scaling Constant; SRW: Service Relativity Weight; EW: Employment Weight; OW: Occupancy Weight; SW: Size Weight; IW: Investment Weight; STW: Student Capacity Weight; SCW: Seating Capacity Weight</p> <p>The combination rule for the formulas: $A \cup B = (A+B) - (A \times B)$</p>			

Measurement of the Variables⁴⁵

1. Scaling Constant (Si):

The Scaling Constant is a number between 0 and 1 which indicates the relative importance of each urban area key sector/service component with respect to each other (Table 22). To ensure consistency throughout the assessment process, scaling constants should be assigned by local, state or federal authorities centrally, and the assigned weights should be applied for all assets located at the assessment area of responsibility.

Table 22 Scaling Constant Matrix (Relative Importance of Urban Area Key Sectors/Services)

No	Urban Area Key Sectors/Services	Scaling Constant (Si)
1	Governance, Homeland Security, Law/Public Order, Emergency Service	
2	Housing/Accommodation	
3	Power/Energy Service (Power plants, nuclear reactors, dams, fuel supply stations, etc.)	
4	Healthcare and Public Health	
5	Telecommunication (including Information Technology)	
6	Transportation/Postal and Shipping Service (including airports, major transportation terminals)	
7	Food/Water and Other Goods Service (Shopping malls, major retail, etc.)	
8	Banking and Finance (including banks/ATMs, etc.)	
9	Critical Manufacturing (including major industrial facilities)	
10	Training and Education Activities (including schools)	
11	Worship Activities (Places of worship, etc.)	

⁴⁵ Measurement of the variables should be performed by the subject matter experts and the scales assigned for each assessment matrix should be optimized in future with further experimentation to produce more precise results.

2. Service Relativity Weight (SRW):

Service Relativity Weight is a number between 0 and 1 (see Table 23) that indicates the relative importance of the asset with respect to ones that perform similar functions in that specific sector/service which is one of the 12 key urban area sectors/services.

Table 23 Service Relativity Weight Assessment Matrix

Service Relativity Weight (SRW)								
Semantic Description	Seven-level linguistic scale							
Relative importance of the asset with respect to ones which perform similar functions in that specific sector/service	None	Very Low	Low	Medium Low	Medium	Medium High	High	Very High
	Numerical scale							
	0.01	0.1	0.2-0.3	0.4	0.5-0.6	0.7	0.8-0.9	1

3. Employment Weight (EW):

Employment Weight is a number between 0 and 1 (see Table 24) that indicates the relative weight of the asset with respect to employee occupancy during day and night.

Table 24 Employment Weight Assessment Matrix

Employment Weight (EW)											
Approximate Number of Employees/Personnel		Below 20	20-50	50-100	100-150	150-250	250-400	400-600	600-800	800-1000	Above 1000
Occupancy Time	Day (D)	0.01	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
	Night (N)	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
EW		$(D+N)/2$									

4. Occupancy Weight (OW):

Occupancy Weight is a number between 0 and 1 (see Table 25) that indicates the relative weight of the asset with respect to approximate inhabitant/visitor occupancy during day and night.

Table 25 Occupancy Weight Assessment Matrix

		Occupancy Weight (OW)									
Approximate Number of Inhabitants/Visitors		Below 10	10 - 25	25 - 50	50 - 100	100 - 200	200 - 300	300 - 400	400-600	600-800	Above 800
Occupancy Time	Day (D)	0.01	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
	Night (N)	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
OW		$(D+N)/2$									

5. Size Weight (SW):

Size Weight is a number between 0 and 1 (see Table 26) that indicates the relative weight of the asset with respect to the size of itself (the weight which locates at box of intersection of the matching story number row and size column gives the relative weight).

Table 26 Size Weight Assessment Matrix

Asset Size/Area (Square Feet)		Size Weight (SW)									
		Below 1000	1000 - 2000	2000 - 4000	4000 - 6000	6000 - 10,000	10,000 - 20,000	20,000 - 50,000	50,000 - 100,000	100,000 - 200,000	Above 200,000
Single Story	1	0.01	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
Multistorey	2-3	0.025	0.125	0.225	0.325	0.425	0.525	0.625	0.725	0.825	0.925
	4-5	0.05	0.15	0.25	0.35	0.45	0.55	0.65	0.75	0.85	0.95
	6-10	0.075	0.175	0.275	0.375	0.475	0.575	0.675	0.775	0.875	0.975
	Above 10	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1

6. Investment Weight (IW):

Investment Weight is a number between 0 and 1 (see Table 27) that indicates the relative weight of the asset with respect to the amount of the money invested for it.

Table 27 Investment Weight Assessment Matrix

Investment Weight (IW)	
Amount of Investment (\$ x 1000)	
	Below 50
	50-200
	200-500
	500-1,000
	1,000-2,000
	2,000-4,000
	4,000-10,000
	10,000-50,000
	50,000-100,000
	Above 100,000
IW	0.1
	0.2
	0.3
	0.4
	0.5
	0.6
	0.7
	0.8
	0.9
	1

7. Student Capacity Weight (STW):

Student Capacity Weight is a number between 0 and 1 (see Table 28) that indicates the relative weight of the training and education related asset with respect to the amount of the student capacity that the asset offers.

Table 28 Student Capacity Weight Assessment Matrix

Student Capacity Weight (STW)										
Student Capacity	Below 500	500-700	700-900	900-1100	1100-1500	1500-2000	2000-3000	3000-5000	5000-10,000	Above 10,000
STW	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1

8. Seating Capacity Weight (SCW)

Seating Capacity Weight is a number between 0 and 1 (see Table 29) that indicates the relative weight of the worship related asset with respect to the amount of the seating capacity that the asset offers.

Table 29 Seating Capacity Weight Assessment Matrix

Seating Capacity Weight (SCW)										
Seating Capacity	Below 100	100-250	250-500	500-800	800-1200	1200-2000	2000-3000	3000-5000	5000-10,000	Above 10,000
SCW	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1

APPENDIX E – MEASUREMENT OF INPUT VARIABLES

1. Scaling Constants (sc):

The Scaling Constants (sc) are numbers between 0 and 1 which indicates the relative importance of each criterion in comparison with the others (Table 30). Scaling Constants are assigned by subject matter experts.

Table 30 Scaling Constants per each Criterion

Criterion	Scaling Constant (0-1)	
Physical Security	sc1	
Number of Inhabitants/Visitors	sc2	
Size/Area	sc3	
Traffic Access/Mobility	sc4	

2. Vulnerability Indexes of the Critical Asset per each Criterion:

a. V(C1): Vulnerability Index of the Critical Asset for Physical Security:

Physical Security Vulnerability Index V(C1) for each critical asset is obtained through the utilization of Table 31, 32, 33, 34. V(C1) provides a weight between 0 and 10.

Table 31 Physical Security Vulnerability Index

Physical Security Vulnerability Index - V(C1)		
1	Perimeter security index (Vp)	
2	Building envelope wall type index (Vw)	
3	Building envelope fenestration index (Vf)	
$V(C1) = (Vp+Vw+Vf) / 3$		

Table 32 Perimeter Security Index

Perimeter Security Index (Vp)							
Semantic Description	The overall efficiency of perimeter fences/walls, gates, access control, outdoor barriers, etc.						
Seven-level linguistic scale	Very Low	Low	Medium Low	Medium	Medium High	High	Very High
Ten-point numerical scale (V)	10	8-9	6-7	4-5	2-3	1	0.1
Vp							

Table 33 Building Envelope Wall Type Index

Building Envelope Wall Type Index (Vw)*		
Wall Type	Mean value of standoff distances (Ms) (ft)	Normalized Wall Type Index $Vw = Ms/Ms_{max} * 10$
Reinforced Concrete	29.5	1.2
Reinforced Masonry	38.5	1.6
Girts	53.3	2.2
Wood Studs – Brick Veneer	58.3	2.5
European Block	66.8	2.8
Metal Panels	88.5	3.7
Unreinforced Masonry	110.5	4.6
Metal Studs – Brick Veneer	120.4	5.1
Wood Studs – EIFS	126.4	5.3
Metal Studs – EIFS	237.9	10
* Wall Type Index values have been derived from the mean values of the conventional construction standoff distances identified for each type of the wall (Unified Facilities Criteria, 2012, p.51). The Wall Type Index represent the weight of the asset's vulnerability in terms of the protection degree of them.		

Table 34 Building Envelope Fenestration Index

Building Envelope Fenestration Index (Vf)							
The percentage of the area of glazed surface in each façade (%)	5	5-10	10-15	15-30	30-45	45-70	70-100
Index Value*	1	2	3	4	5-6	7-8	9-10
Vf	$\sum Vi^{**} / (\text{Total number of façades} + 1)$						
Vi: Utility value for each façade/direction							
* Index Value scale represent the general guidelines for windows and glazing delineated in FEMA 426 (Reference Manual, 2003).							
**Utility value for the primary façade (street side) is doubled while processing the formula since it is exposed to potential threats directly.							

b. **V(C2): Vulnerability Index of the Critical Asset for Number of**

Inhabitants/Visitors:

Inhabitant/Visitor Number Vulnerability Index V(C2) for each critical asset is obtained through the utilization of Table 35. V(C2) provides a weight between 0 and 10.

Table 35 Inhabitant/Visitor Number Vulnerability Index

Inhabitant/Visitor Number Vulnerability Index - V(C2)											
Approximate Number of Inhabitants/Visitors		Below 10	10 - 25	25 - 50	50 - 100	100 - 200	200 - 300	300 - 500	500 - 750	750 - 1000	Above 1000
Occupancy Time	Day (D)	0.1	1	2	3	4	5	6	7	8	9
	Night (N)	1	2	3	4	5	6	7	8	9	10
V(C2)		$(D+N)/2$									

c. **V(C3): Vulnerability Index of the Critical Asset for Size/Area:**

Size/Area Vulnerability Index $V(C3)$ for each critical asset is obtained through the utilization of Table 36. $V(C3)$ provides a weight between 0 and 10.

Table 36 Size/Area Vulnerability Index

Size/Area Vulnerability Index - $V(C3)$											
Asset Size/Area (sf)		Below 1000	1000 - 2000	2000 - 4000	4000 - 6000	6000 - 10,000	10,000 - 20,000	20,000 - 50,000	50,000 - 100,000	100,000 - 200,000	Above 200,000
Single Story	1	0.1	1	2	3	4	5	6	7	8	9
Multistorey	2-3	0.25	1.25	2.25	3.25	4.25	5.25	6.25	7.25	8.25	9.25
	4-5	0.5	1.5	2.5	3.5	4.5	5.5	6.5	7.5	8.5	9.5
	6-10	0.75	1.75	2.75	3.75	4.75	5.75	6.75	7.75	8.75	9.75
	Above 10	1	2	3	4	5	6	7	8	9	10
$V(C3)$											

d. **V(C4): Vulnerability Index of the Critical Asset for Traffic Access/Mobility:**

Traffic Access/Mobility Vulnerability Index $V(C4)$ for each critical asset is obtained through the utilization of Table 37, 38, 39, 40, 41. $V(C4)$ provides a weight between 0 and 10.

Table 37 Traffic Access/Mobility Vulnerability Index

Traffic Access/Mobility Vulnerability Index - V(C4)		
1	Periphery Road Width Index (Vp)	
2	Adjacent Primary Roads Proximity Index (Va)	
3	Bridge Dependency Index (Vb)	
4	Transportation Terminals Proximity Index (Vt)	
$V(C4) = (Vp+Va+Vb+Vt) / 4$		

Table 38 Periphery Road Width Index

Periphery Road Width Index (Vr)						
Road surfacing width (including median width) (ft)*	No Road	Below 25	25-50	50-80	80-150	Above 150
Index Value	10	8-9	6-7	4-5	2-3	1
The roads/streets encircling the asset	North side (Ni)					
	East side (Ei)					
	South side (Si)					
	West side (Wi)					
Vr	$(Ni+Ei+Si+Wi) / 4$					
<p>* Street patterns (and widths) influence all warfighting functions; however, they greatly affect movement and maneuver, command and control, and sustainment (Urban Operations, 2006, p. 6). Street widths are grouped into three major classes (Combined Arms Operations in Urban Terrain, 2011, p. A-11);</p> <ul style="list-style-type: none"> • Seven to 15 meters, located in older historical sections of pre-industrial cities. • Fifteen to 25 meters, located in newer planned sections of most cities. • Twenty-five to 50 meters, located along broad boulevards or set far apart on large parcels of land. 						

Table 39 Adjacent Primary Roads Proximity Index

Adjacent Primary Roads Proximity Index (Va)										
Approximate distance from the asset to access primary roads (ft/mi)	Below 500 ft	500-1000 ft	1000-1500 ft	1500-2000 ft	2000 ft - 0.5 mi	0.5 - 0.75 mi	0.75 - 1 mi	1 - 1.25 mi	1.25 - 1.5 mi	Above 1.5 mi
Expressways/Interstates (with 4 or more lanes) (Eli)	1	2	3	4	5	6	7	8	9	10
Arterials/Collectors (with 2 or more lanes) (ACi)	1	2	3	4	5	6	7	8	9	10
Va	(Eli+ACi)/2									

Table 40 Bridge Dependency Index

Bridge Dependency Index (Vb)							
Semantic Description	The level of dependency to bridges (one or more) for access to the asset within a circle around the asset with 10 miles radius						
Seven-level linguistic scale	Very Low	Low	Medium Low	Medium	Medium High	High	Very High
Ten-point numerical scale	0.1	1	2-3	4-5	6-7	8-9	10
Vb							

Table 41 Transportation Terminals Proximity Index

Transportation Terminals Proximity Index (Vt)										
Approximate distance to the nearest transportation terminals (mi)	Below 1	1 - 5	6 - 10	11 - 15	16 - 20	21 - 25	26 - 30	31 - 35	36 - 40	Above 40
Airport (APi)	1	2	3	4	5	6	7	8	9	10
Waterway Terminal (WTi)	1	2	3	4	5	6	7	8	9	10
Railway Terminal (RTi)	1	2	3	4	5	6	7	8	9	10
Vt	(APi+WTi+RTi) / 3									

3. Vulnerability Index Modifiers of the Critical Asset per each Possible System State:

- a. **M(S1): Vulnerability Index Modifier of the Critical Asset for Offences against Property:**

Vulnerability Index Modifier for Offences against Property (M(S1) for each critical asset is obtained through the utilization of Table 42. M(S1) provides a weight between 0 and 1.

Table 42 Vulnerability Index Modifier for Offences against Property

Vulnerability Index Modifier for Offences against Property - M(S1)							
System State (S1)	Offences Against Property (like looting, larceny/theft, burglary, arson, motor vehicle theft etc.)						
Semantic Description	Seven-level linguistic scale						
Since the asset has substantial material/property which could attract criminals, it has probability of having 'Offences Against Property' during post disaster environment.	Very Low	Low	Medium Low	Medium	Medium High	High	Very High
	Numerical Scale						
	0.1	0.2-0.3	0.4	0.5-0.6	0.7	0.8-0.9	1
M(S1)							

- b. **M(S2): Vulnerability Index Modifier of the Critical Asset for Offences against Persons:**

Vulnerability Index Modifier for Offences against Persons (M(S2) for each critical asset is obtained through the utilization of Table 43. M(S2) provides a weight between 0 and 1.

Table 43 Vulnerability Index Modifier for Offences against Persons

Vulnerability Index Modifier for Offences against Persons - M(S2)							
System State (S2)	Offences Against Persons [like murder, sexual assault, robbery, etc.]						
Semantic Description	Seven-level linguistic scale						
Since the asset is to have isolated characteristics in terms of location and building structure which exposes an attractive target for roving criminals, it has probability of having Offences Against Persons during post disaster environment.	Very Low	Low	Medium Low	Medium	Medium High	High	Very High
	Numerical Scale						
	0.1	0.2-0.3	0.4	0.5-0.6	0.7	0.8-0.9	1
M(S2)							

c. **M(S3): Vulnerability Index Modifier of the Critical Asset for Terrorist**

Attacks/ Warfare Threats:

Vulnerability Index Modifier for Terrorist Attacks/ Warfare Threats (M(S3))

for each critical asset is obtained through the utilization of Table 44. M(S3) provides a weight between 0 and 1.

Table 44 Vulnerability Index Modifier for Terrorist Attacks/ Warfare Threats

Vulnerability Index Modifier for Terrorist Attacks/ Conventional Warfare Threats - M(S3)							
System State (S3)	Terrorist Attacks/ Conventional Warfare Threats (aggregated assaults, sabotages, etc.)						
Semantic Description	Seven-level linguistic scale						
Since the asset is a potential high value target having either high occupancy or any symbolic value for local authorities, it has probability of having 'Terrorist Attacks/ Conventional Warfare Threats' during post disaster environment which could make a severe impact on the political scene.	Very Low	Low	Medium Low	Medium	Medium High	High	Very High
	Numerical Scale						
	0.1	0.2-0.3	0.4	0.5-0.6	0.7	0.8-0.9	1
M(S3)							

4. Generalizability Grades of Membership per each Criterion:

a. G(C1): Generalizability Grades of Membership for Physical Security:

G(C1) could be weighted in the city level and applied for all the other sub-level asset estimations. It is obtained through the utilization of Table 45, 46, 47, 48, and provides a weight between 0 and 1.

Table 45 Generalizability Grades of Membership for Physical Security

Generalizability Grades of Membership for Physical Security - G(C1)		
1	Seismicity Vulnerability Index (Si)	
2	Hurricane Vulnerability Index (Hi)	
3	Flood Vulnerability Index (Fi)	
G(C1) = (Si + Hi + Fi) / 3		

Table 46 Seismicity Vulnerability Index

Seismicity Vulnerability Index (Si)			
Region of Seismicity*	High	Moderate	Low
Numerical scale	0.8 - 1	0.4 - 0.7	0.1 - 0.3
Si			
* See Figure 38			

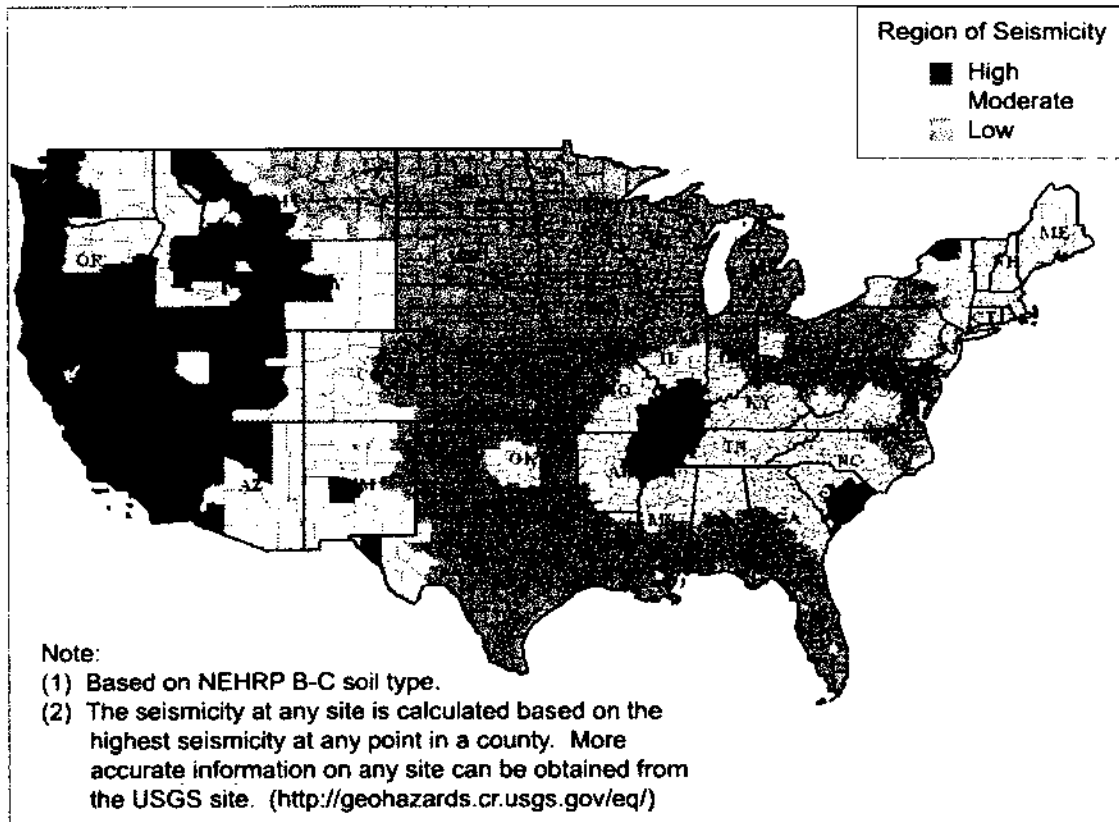


Figure 38 Seismicity Regions of the Conterminous United States (Rapid Visual Screening, 2002, p. 66)

Table 47 Hurricane Vulnerability Index

Hurricane Vulnerability Index (Hi)					
Five-level linguistic scale	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Numerical scale	1	0.75	0.5	0.25	0.01
The region stays on the historical tracks and seriously vulnerable to recurrent hurricanes					
Hi					

Table 48 Flood Vulnerability Index

Flood Vulnerability Index (Fi)					
Five-level linguistic scale	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Numerical scale	1	0.75	0.5	0.25	0.01
The region is close to water masses and seriously vulnerable to potential floods					
Fi					

- b. **G(C2):** Generalizability Grades of Membership for Number of Inhabitants/Visitors:

G(C2) could be weighted at least in the level of police patrol divisions' area of responsibility and applied for all the other sub-level asset estimations. It is obtained through the utilization of Table 49 and provides a weight between 0 and 1.

Table 49 Generalizability Grades of Membership for Number of Inhabitants/Visitors

Generalizability Grades of Membership for Number of Inhabitants/Visitors - G(C2)	
Ns: Approximate number of available security agents serving in the sector	
Pk: Approximate number of population inhabiting in the key assets in the sector (day/night)	
Pa: Approximate population in the sector	
$G(C2) = (Ns \times Pk) / Pa$	
Gmax(C2): Highest Generalizability Grades of Membership for Number of Inhabitants/Visitors estimated within the all area of responsibility in the sector level.	
Gn(C2): Normalized Generalizability Grades of Membership for Number of Inhabitants/Visitors which address vulnerability index.	
$Gn(C2) = 1 - G(C2) / G_{max}(C2)$	

c. **G(C3): Generalizability Grades of Membership for Size/Area:**

G(C3) could be weighted at least in the level of police patrol divisions' area of responsibility and applied for all the other sub-level asset estimations. It is obtained through the utilization of Table 50 and provides a weight between 0 and 1.

Table 50 Generalizability Grades of Membership for Size/Area

Generalizability Grades of Membership for Size/Area - G(C3)	
Ns: Approximate number of available security agents serving in the sector	
Ak: Approximate sum of the key asset areas in the sector (sq ft)	
As: Approximate area of the sector (sq ft)	
$G(C3) = (Ns \times Ak) / As$	
Gmax(C3): Highest Generalizability Grades of Membership for Size/Area estimated within the all area of responsibility in the sector level.	
G _N (C3): Normalized Generalizability Grades of Membership for Size/Area which address vulnerability index.	
$G_N(C3) = 1 - G(C3) / G_{max}(C3)$	

d. **G(C4): Generalizability Grades of Membership for Traffic Access/Mobility:**

G(C4) is obtained through the utilization of Table 51, 52, 53, 54, and provides a weight between 0 and 1.

Table 51 Generalizability Grades of Membership for Traffic Access/Mobility

Generalizability Grades of Membership for Traffic Access/Mobility - G(C4)		
1	Road Length Index (Ri)	
2	Transportation Lines Index (Ti)	
3	Bridges Index (Bi)	
$G(C4) = (Ri + Ti + Bi) / 3$		

Table 52 Road Length Index

Road Length Index (Ri)	
Es: Approximate sum of the length of Expressways/Interstates (with 4 or more lanes) in the sector (mi)	
As: Approximate sum of the length of Arterials/Collectors (with 2 or more lanes) in the sector (mi)	
Es(max): Highest length of Expressways/Interstates (with 4 or more lanes) in sector level estimated within the all area of responsibility (mi)	
As(max): Highest length of Arterials (with 2 or more lanes) in sector level estimated within the all area of responsibility (mi)	
$Ri = 1 - (Es/Es(max) + As/As(max)) / 2$	

Table 53 Transportation Lines Index

Transportation Lines Index (Ti)				
The Number of Transportation Terminals in the Sector	No Terminal	1	2	3 and above
Numerical Scale	1	0.7 - 0.9	0.3 - 0.6	0.1 - 0.2
Airport (Ai)				
Waterway Terminal (Wi)				
Railway Terminal (Ri)				
$Ti = (Ai + Wi + Ri) / 3$				

Table 54 Bridges Index

Bridges Index (Bi)					
The Number of Bridges in the Sector	No Bridge	1	2	3	4 and above
Numerical Scale	0.01	0.1 - 0.3	0.4 - 0.6	0.7 - 0.9	1
Bi					

5. Generalizability Grades of Membership per each Possible System State:

a. **G(S1):** Generalizability Grades of Membership for Offences against Property:

G(S1) is obtained through the utilization of Table 55 and provides a weight between 0 and 1.

Table 55 Generalizability Grades of Membership for Offences against Property

Generalizability Grades of Membership for Offences against Property - G(S1)	
Rcp: Property Crime Rate in the sector (yearly total number of incidents)	
Rcp(max): Maximum Property Crime Rate in the sector level (yearly total number of incidents)	
$G(S1) = Rcp / Rcp(max)$	

b. **G(S2):** Generalizability Grades of Membership for Offences against Persons:

G(S2) is obtained through the utilization of Table 56 and provides a weight between 0 and 1.

Table 56 Generalizability Grades of Membership for Offences against Persons

Generalizability Grades of Membership for Offences against Persons - G(S2)	
Rcv: Violent Crime Rate in the sector (yearly total number of incidents)	
Rcv(max): Maximum Violent Crime Rate in the sector level (yearly total number of incidents)	
$G(S2) = Rcv / Rcv(max)$	

- c. **G(S3):** Generalizability Grades of Membership for Terrorist Attacks/ Warfare

Threats:

G(S3) is obtained through the utilization of Table 57 and provides a weight between 0 and 1.

Table 57 Generalizability Grades of Membership for Terrorist Attacks/ Warfare Threats

Generalizability Grades of Membership for Terrorist Attacks/Conventional Warfare Threats - G(S3)							
System State (S3)	Terrorist Attacks/ Conventional Warfare Threats (aggregated assaults, sabotages, etc.)						
Semantic Description	Seven-level linguistic scale						
With respect to historical records/statistics and existing social and political spectrum, the level of security and stability in the city considering the potential terrorist attacks/conventional warfare threats	Very Low	Low	Medium Low	Medium	Medium High	High	Very High
	Numerical Scale						
	0.1	0.2-0.3	0.4	0.5-0.6	0.7	0.8-0.9	1
G(S3)							

APPENDIX F – SAMPLE MEASUREMENT

1. Identify Boundaries

For the implementation of the PDSI Model, the City of Delta territory is divided into small parts in line with the City Police Districts plan, and further into smaller parts of patrol division sectors and sub-sectors. Later, the Operations Bureau planning team decides to test the PDSI Model on a pilot area first. They identify the boundary of Alfa sub-sector (Figure 39) to proceed through the model algorithm.

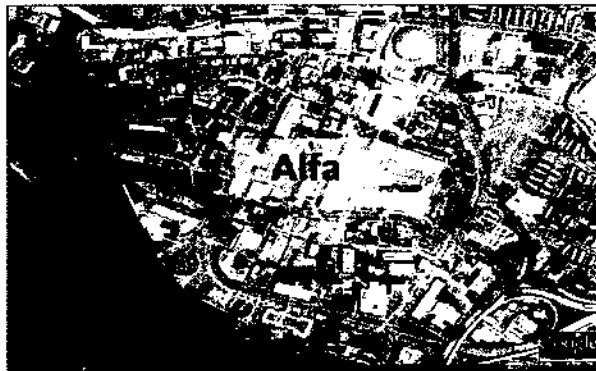


Figure 39 Boundaries of Alfa Subsector

2. Identify Critical Assets

The subject matter expert team assigned by the Operations Bureau roughly identifies and enumerates the critical assets (Figure 40) in Alfa sub-sector according to the set of criteria provided by the Mayor of Delta City, which defines general indices for the critical asset selection. The three critical assets within the Alfa subsector have been virtually generated to sample the assessment process;

- Blue Shopping Center (BSC)
- Delta City Hospital (DCH)
- City of Delta Department (CDD)

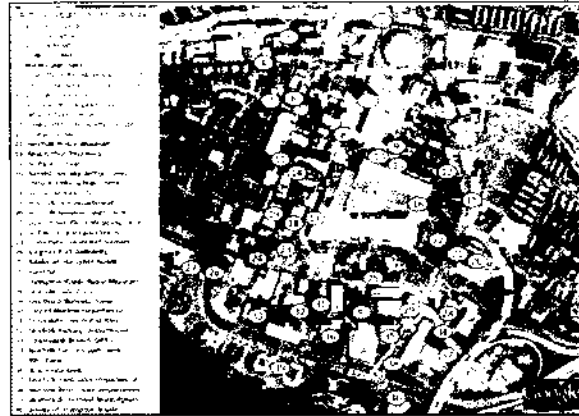


Figure 40 Critical Assets Identified in Alfa Subsector

3. Measure Basic Criticality Value (BCV)

The Scaling Constants (relative importance of the urban area key sectors/services) are assigned by the City Council in advance (see Table 58).

Table 58 Scaling Constant Matrix

No	Urban Area Key Sectors/Services	Scaling Constant (Si)
1	Governance, Homeland Security, Law/Public Order, Emergency Service	1
2	Housing/Accommodation	0.8
3	Power/Energy Service (Power plants, nuclear reactors, dams, fuel supply stations, etc.)	0.9
4	Healthcare and Public Health	0.9
5	Telecommunication (including Information Technology)	0.8
6	Transportation/Postal and Shipping Service (including airports, major transportation terminals)	0.6
7	Food/Water and Other Goods Service (Shopping malls, major retail, etc.)	0.8
8	Banking and Finance (including banks/ATMs, etc.)	0.7
9	Critical Manufacturing (including major industrial facilities)	0.7
10	Training and Education Activities (including schools)	0.6
11	Worship Activities (Places of worship, etc.)	0.5

Basic Criticality Values (BCV) for each critical asset are calculated in Table 59 with the weights generated randomly.

Table 59 Basic Criticality Values

No	Urban Area Key Sectors/Services	BCI(i)	
City of Delta Department (CDD)			
1	Governance, Homeland Security, Law/Public Order, Emergency Service	BCI1	$S1 \times (SRW1 \cup EW1)$
$BCI1 = 1 \times (0.9 \cup 0.5) = \mathbf{0.950}$			
Delta City Hospital (DCH)			
4	Healthcare and Public Health	BCI4	$S4 \times (SRW4 \cup EW4)$
$BCI4 = 0.9 \times (0.8 \cup 0.4) = \mathbf{0.792}$			
Blue Shopping Center (BSC)			
7	Food/Water and Other Goods Service (Shopping malls, major retail, etc.)	BCI7	$S7 \times (EW7 \cup SW7)$
$BCI7 = 0.8 \times (0.1 \cup 0.65) = \mathbf{0.548}$			
<p>Variables: Si: Scaling Constant; SRW: Service Relativity Weight; EW: Employment Weight; OW: Occupancy Weight; SW: Size Weight; IW: Investment Weight; STW: Student Capacity Weight; SCW: Seating Capacity Weight</p> <p>The combination rule for the equations: $A \cup B = (A+B) - (A \times B)$</p>			

4. Measure Post-Disaster Security Fuzzy Index (PDSFI)

Measurement of Input Variables

a. Scaling Constant per each Criterion is assigned by the Subject Matter Expert team employed by the Police Department (see Table 60).

Table 60 Scaling Constants per each Criterion

Criterion	Scaling Constant (0-1)	
	Physical Security	sc1
Number of Inhabitants/Visitors	sc2	0.8
Size/Area	sc3	1
Traffic Access/Mobility	sc4	0.9

b. Vulnerability Indexes of the Critical Assets per each Criterion are measured in Table 61 with the weights generated randomly.

Table 61 Vulnerability Indexes

VULNERABILITY INDEXES				CRITICAL ASSETS					
				Blue Shopping Center		Delta City Hospital		City of Delta Department	
V(C1)	Physical Security (Vp+Vw+Vf) / 3	Vp	Perimeter Security Index	8	6.87	7	3.87	3	3.6
		Vw	Building Envelope Wall Type Index	4.6		1.6		2.8	
		Vf	Building Envelope Fenestration Index	8		3		5	
V(C2)	Approximate number of inhabitants/visitors			6		7.5		5.5	
V(C3)	Asset size/area			6.25		6.75		4.5	
V(C4)	Traffic Access/Mobility (Vr+Va+Vb+Vt) / 4	Vr	Periphery Road Width Index	7	5.25	3	4.5	5	4.75
		Va	Adjacent Primary Roads Proximity Index	4		6		3	
		Vb	Bridge Dependency Index	4		5		4	
		Vt	Transportation Terminals Proximity	6		4		7	

c. Vulnerability Index Modifiers of the Critical Assets per each Possible System State are listed in Table 62 with the weights generated randomly.

Table 62 Vulnerability Index Modifiers

VULNERABILITY INDEX MODIFIERS		CRITICAL ASSETS		
		Blue Shopping Center	Delta City Hospital	City of Delta Department
M(S1)	Offences Against Property	0.8	0.4	0.2
M(S2)	Offences Against Persons	0.6	0.3	0.1
M(S3)	Terrorist Attacks/ Conventional Warfare Threats	0.7	0.4	0.6

d. Generalizability Grades of Membership per each Criterion is measured in Table 63 with the weights generated randomly.

Table 63 Generalizability Grades of Membership per each Criterion

Generalizability Grades of Membership per each Criterion				CRITICAL ASSETS					
				Blue Shopping Center		Delta City Hospital		City of Delta Department	
G(C1)	Generalizability Grades of Membership for Physical Security (Si+Hi+Fi) / 3	Si	Seismicity Vulnerability Index	0.6	0.62	0.6	0.62	0.6	0.62
		Hi	Hurricane Vulnerability Index	0.75		0.75		0.75	
		Fi	Flood Vulnerability Index	0.5		0.5		0.5	
G(C2)	Generalizability Grades of Membership for Number of Inhabitants/Visitors			0.45		0.45		0.45	
G(C3)	Generalizability Grades of Membership for Size/Area			0.58		0.58		0.58	
G(C4)	Generalizability Grades of Membership for Traffic Access/Mobility (Ri+Ti+Bi) / 3	Ri	Road Length Index	0.72	0.44	0.72	0.44	0.72	0.44
		Ti	Transportation Lines Index	0.34		0.34		0.34	
		Bi	Bridges Index	0.25		0.25		0.25	

e. Generalizability Grades of Membership per each Possible System State is listed in Table 64 with the weights generated randomly.

Table 64 Generalizability Grades of Membership per each Possible System State

Generalizability Grades of Membership per each Possible System State		CRITICAL ASSETS		
		Blue Shopping Center	Delta City Hospital	City of Delta Department
G(S1)	Offences Against Property	0.35	0.35	0.35
G(S2)	Offences Against Persons	0.20	0.20	0.20
G(S3)	Terrorist Attacks/ Conventional Warfare Threats	0.05	0.05	0.05

Measurement of Fuzzy Matrix Variables

a. The PDSFI Matrix of Blue Shopping Center (BSC) is shown in Table 65 with the variables measured according to equations discussed in Chapter 4.5.5.

Table 65 PDSFI Matrix of BSC

Post-Disaster Security Fuzzy Index (PDSFI) Matrix													
Ambient Criteria of Merit				Vulnerability Indexes				Possible System States					
Scaling Constant (sc)	{sc1}	0.8	C1: Physical Security	V(C1)	V(C2)	V(C3)	V(C4)	S1: Offences against Property S2: Offences against Persons S3: Terrorist Attacks/Conventional Warfare Threats					
	{sc2}	0.8	C2: Number of Inhabitants/Visitors	6.87	6	6.25	5.25						
	{sc3}	1	C3: Size/Area	Generalizability Grades of Membership									
	{sc4}	0.9	C4: Traffic Access/Mobility	G(C1)	G(C2)	G(C3)	G(C4)						
				0.62	0.45	0.58	0.44						
Fuzzy Matrix				{0.753, 4.39}	{0.643, 3.84}	{0.728, 5}	{0.636, 3.78}	0.35	G(S1)	Generalizability Grades of Membership	0.80	M(S1)	Vulnerability Index Modifiers
				{0.696, 3.3}	{0.560, 2.88}	{0.664, 3.75}	{0.552, 2.84}	0.20	G(S2)		0.6	M(S2)	
				{0.639, 3.85}	{0.478, 3.36}	{0.601, 4.38}	{0.468, 3.31}	0.05	G(S3)		0.7	M(S3)	

b. The PDSFI Matrix of Delta City Hospital (DHC) is shown in Table 66 with the variables measured according to equations discussed in Chapter 4.5.5.

Table 66 PDSFI Matrix of DHC

Post-Disaster Security Fuzzy Index (PDSFI) Matrix													
Ambient Criteria of Merit				Vulnerability Indexes				Possible System States					
Scaling Constant (sc)	{sc1}	0.8	C1: Physical Security	V(C1)	V(C2)	V(C3)	V(C4)	S1: Offences against Property S2: Offences against Persons S3: Terrorist Attacks/Conventional Warfare Threats					
	{sc2}	0.8	C2: Number of Inhabitants/Visitors	3.87	7.5	6.75	4.5						
	{sc3}	1	C3: Size/Area	Generalizability Grades of Membership									
	{sc4}	0.9	C4: Traffic Access/Mobility	G(C1)	G(C2)	G(C3)	G(C4)						
				0.62	0.45	0.58	0.44						
Fuzzy Matrix				{0.753, 1.24}	{0.643, 2.4}	{0.728, 2.7}	{0.636, 1.62}	0.35	G(S1)	Generalizability Grades of Membership	0.40	M(S1)	Vulnerability Index Modifiers
				{0.696, 0.93}	{0.560, 1.8}	{0.664, 2.03}	{0.552, 1.22}	0.20	G(S2)		0.30	M(S2)	
				{0.639, 1.24}	{0.478, 2.4}	{0.501, 2.7}	{0.468, 1.62}	0.05	G(S3)		0.40	M(S3)	

c. The PDSFI Matrix of City of Delta Department (CDD) is shown in Table 67 with the variables measured according to equations discussed in Chapter 4.5.5.

Table 67 PDSFI Matrix of CDD

Post-Disaster Security Fuzzy Index (PDSFI) Matrix													
Ambient Criteria of Merit				Vulnerability Indexes				Possible System States					
Scaling Constant (sc)	{sc1}	0.8	C1: Physical Security	V(C1)	V(C2)	V(C3)	V(C4)	S1: Offences against Property S2: Offences against Persons S3: Terrorist Attacks/Conventional Warfare Threats					
	{sc2}	0.8	C2: Number of Inhabitants/Visitors	3.6	5.5	4.5	4.75						
	{sc3}	1	C3: Size/Area	Generalizability Grades of Membership									
	{sc4}	0.9	C4: Traffic Access/Mobility	G(C1)	G(C2)	G(C3)	G(C4)						
				0.62	0.45	0.58	0.44						
Fuzzy Matrix				{0.753, 0.58}	{0.643, 0.88}	{0.728, 0.9}	{0.636, 0.86}	0.35	G(S1)	Generalizability Grades of Membership	0.20	M(S1)	Vulnerability Index Modifiers
				{0.696, 0.29}	{0.560, 0.44}	{0.664, 0.45}	{0.552, 0.43}	0.20	G(S2)		0.10	M(S2)	
				{0.639, 1.73}	{0.478, 2.64}	{0.601, 2.7}	{0.468, 2.57}	0.05	G(S3)		0.6	M(S3)	

Aggregation

In this step, PDSFI for each critical asset is obtained through the aggregation of the variables provided in the fuzzy matrix (of each asset) using the Equation 2.

- a. Blue Shopping Center (BSC)

$$\mathbf{PDSFI (BSC) = 2.334}$$

- b. Delta City Hospital (DCH)

$$\mathbf{PDSFI (DCH) = 1.121}$$

- c. City of Delta Department (CDD)

$$\mathbf{PDSFI (CDD) = 0.699}$$

5. Measure Post-Disaster Security Index (PDSI)

PDSI for each critical asset is obtained through Equation 3 as listed in Table 68.

Table 68 PDSI of the Critical Assets

Critical Asset	BCV	PDSFI	PDSI
Blue Shopping Center (BSC)	0.548	2.334	1279
Delta City Hospital (DCH)	0.792	1.121	887
City of Delta Department (CDD)	0.950	0.699	664

**APPENDIX G – POST-DISASTER SECURITY INDEX (PDSI) MODEL FACE
VALIDITY QUESTIONNAIRE**

SEMANTIC DESCRIPTION		Linguistic Scale				
		Totally Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Totally Agree
		Numeric Scale				
		1	2	3	4	5
1	Overall framework of the PDSI Model is congruent with the notion of the urban security operations.					
2	Measurement process roadmap proposed by the PDSI Model provides indexes in higher precision since its algorithm incorporates both multiple criterions and different system states.					
3	Embedded Criteria of Merit incorporated in the PDSFI Matrix are relevant to the expected outcomes of the model.					
4	Possible System States incorporated in the PDSFI Matrix represent the relevant threat spectrum and crime classifications to most extent.					
5	Generalizability Grades of Membership incorporated in the PDSFI Matrix enhance the applicability of the model in higher scales.					
6	Measurement matrix for each PDSI Model variables includes sufficient numbers of sub-criterions that enhance the reliability of the outputs.					
7	PDSI provides realistic scores for the security planning process in terms of force tailoring, unit positioning and identification of the security operations techniques to be executed in the area of operations.					

APPENDIX H - BASIC REALITY FACE-OFF DECISION TREE

The 'Basic Reality Face-off Decision Tree,' illustrated in Figure 41, was developed to validate the incorporation of 'Ambient Criteria of Merit' in the PDSFI Matrix. The design of the decision tree is based on the following scenario:

Scenario: A special firefighter team named Bravo under the command of Fire Captain Brown has been tasked to deploy to Compound Charlie as soon as possible by the immediate release of a fragmentary order (FRAGO). However, the only information provided to Captain Brown are the coordinates of the compound and a note, which says "There are three critical facility buildings (A, B and C). They are the only structures in the compound, and they are densely populated. Furthermore, all the personnel in the compound are stuck and vulnerable to upcoming emergent threats."

Mission: The mission of the team is to secure the critical buildings from an imminent collateral fire threat and evacuate/rescue people as necessary. Time is very critical and decisions should be made quickly and revised later after the initial action. Captain Brown has a single responsibility with an important caveat notified by the superior command.

Responsibility: Once the team arrives in the compound, Captain Brown will tailor the force structure, dividing the team into separate groups, and deploy (position) each group to vulnerable assets, and reassess his force tailoring and unit

positioning decisions, as the feedback report regarding the situation is sent to him by the troops deployed to first assignment positions.

Caveat: For any course of action, Captain Brown cannot reserve any inert units.

All the troops have to be assigned and deployed.

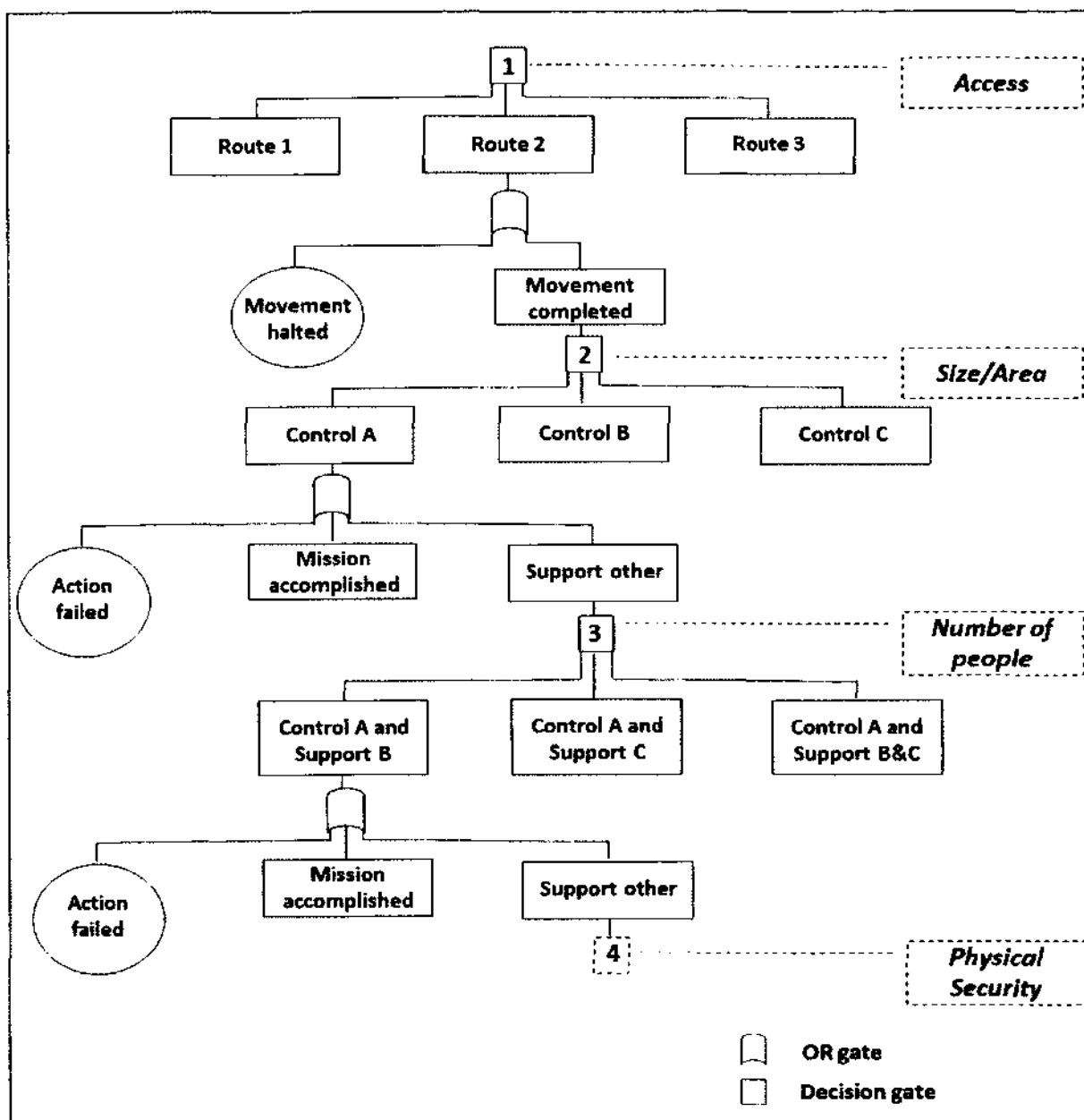


Figure 41 Basic Reality Face-off Decision Tree

From the simple tactical perspective of military security operations, the following assumptions have been generated to visualize the response continuum of the team Bravo:

Having received the FRAGO, Captain Brown's initial decision should be to start his team's movement towards the compound as a prompt action since he has the coordinates. However, he would need more information to decide the best route to ensure his team arrives in the compound quickly and safely. The requirement for this decision point is depicted with the square numbered '1' in the decision tree (Figure 39).

Once the team reaches the compound, the Captain faces another decision point, depicted with the square numbered '2' in the decision tree (Figure 39). As a matter of his responsibility, Captain Brown has to make decision on the force tailoring and unit positioning to deploy his troops. However, he only knows that all the three assets are critical and populated with personnel. While he has no idea about the criticality weights of the assets, he has to take action very quickly. So, he should make a decision to tailor his team into groups considering the sizes/areas of the assets, since he can only see the assets and their sizes/areas in that time.

When the troops are initially deployed to their first positions, regarding the causality principle, the three potential results could be:

- Troops may fail.
- Troops may accomplish.
- Troops may need to support other groups while they continue to perform their initial task.

Once the groups are deployed to critical assets, they would first report the number of the people trapped in the assets. Then the Captain would likely revise his previous decision to adjust the number of the assigned troops in accordance with the number of the people trapped in the assets. This decision point is depicted with the square numbered '3' in the decision tree (Figure 39).

While personnel are evacuated and preemptive actions are being taken to protect assets from imminent threat of fire, the troops could provide further information regarding the physical security characteristics of the assets (e.g. the features that make the assets more or less vulnerable to fire), and the Captain would think to revise his previous decision to optimize the force tailoring as appropriate. This decision point is depicted with the square numbered '4' in the decision tree (Figure 39).

In summary, although the decision tree could be extended further to the more specific branches in similar approach, the criteria that the Captain must consider in the first four decision points - best route selection (Traffic Access/Mobility), tailoring the team into groups considering the sizes/areas of the assets (Size/Area), adjusting the number of the assigned troops in accordance with the number of the people stuck in the assets (Number of Inhabitants/Visitors), and revising the previous decision to optimize the force tailoring according to the information about the physical security characteristics of the assets (Physical Security) - constitute the basic criteria set to complete the criticality and vulnerability assessments during the implementation of the PDSI Model.

APPENDIX I - A ROADMAP FOR COMPLETE COMPLEX ORGANIZATIONAL SYSTEM ANALYSIS

1. Establishment of Core Analysis Team (CAT)

The CAT to be established (which is isolated from any potential structural, organizational and hierarchical pressure) should directly report to highest level decision makers.⁴⁶ It should initially be manned by enough number of qualified subject matter experts who have already had a holistic perspective for the organization with necessary content knowledge and experience. Following the establishment of the CAT, the mission and desired end state is delivered with a brief direction and guidance.

2. Development of the CAT Terms of Reference (ToR)

The CAT is allowed for an ample incubation period to discuss the way ahead and draft a flexible ToR for its own operation principles, and the ToR is approved by the decision making committee.

3. Establishment of Analysis Working Group (AWG)

At the end of the incubation period, due to information to be provided by the CAT, the CAT is reinforced with necessary staff to ensure all major organizational system components are represented at least by one subject matter expert. Pursuant to participation of other representatives, the AWG is established to be governed by CAT

⁴⁶ A decision making committee, which is to include the optimal mix of decision makers who fairly represent the relevant system stakeholders/entities at the highest level, should be assigned to oversee the whole analysis process and navigate the CAT.

and the CAT ToR is modified to cover the AWG, and the changes approved by the decision making committee.

4. Development of the Analysis Methodology

Since every organization has unique characteristics, its analysis methodology should be an optimal blend of the available methods. In this sense, AWG is allowed to develop a draft analysis methodology (which could be as outlined in the next bullet - #5), and the analysis methodology approved by the decision making committee.

5. Conducting Analysis

- a. Major problem domains in the system are identified by AWG, and approved by the decision making committee.
- b. Main problem areas in each major problem domain are identified by AWG, and approved by the decision making committee.
- c. Sub-problems in each main problem area are identified, and approved by the decision making committee (Sub-problem identification continues until the AWG agrees that required granularity has been obtained to make each specified problem handled by any subject matter expert sub-committee that would be assigned afterwards).
- d. The major problem domains, main problem areas and sub-problems are analyzed in a sequential order or in a non-linear approach as necessary, and the courses of action are developed for possible solutions, to be approved by the decision making committee.

e. The personnel and logistic plans that will support the courses of action identified are developed and the coordination requirements completed.

6. Implementation

a. The implementation plan including the detailed timeline is developed and approved.

b. Execution.

c. Feedback mechanism is facilitated and course corrections are applied as required until the systems reaches full operational capability.

**APPENDIX J - RESPONSIBLE CONDUCT OF RESEARCH FOR ENGINEERS
CURRICULUM COMPLETION REPORT**

CITI Collaborative Institutional Training Initiative (CITI)

Learner: Mehmet Secilmis

Institution: Old Dominion University

Responsible Conduct of Research for Engineers

Stage 1. Basic Course Passed on 03/28/11 (Ref # 5487038)

Elective Modules	Date Completed	Score
Introduction to RCR for Engineers	02/13/11	no quiz
Research Misconduct	02/13/11	5/5 (100%)
Whistleblowing and the Obligation to Protect the Public	02/16/11	7/7 (100%)
Responsible Authorship in Engineering	03/07/11	3/4 (75%)
Ethical Issues in Peer Review and Publication in Engineering Research	03/15/11	3/4 (75%)
Conflicts of Interest in Engineering Research	03/15/11	4/5 (80%)
Environmental Ethics	03/16/11	3/4 (75%)
The Ethics of Mentoring	03/16/11	7/7 (100%)
Human Subjects Research in Engineering Fields	03/16/11	5/5 (100%)
The Use of Live Animals in Research	03/28/11	5/8 (63%)
Ethical Issues in the Management of Data in Engineering Research	03/28/11	9/9 (100%)
Collaborative Research in Engineering Fields	03/28/11	4/7 (57%)
Completing the RCR for Engineers Course	03/28/11	no quiz

For this Completion Report to be valid, the learner listed above must be affiliated with a CITI participating institution. Falsified information and unauthorized use of the CITI course site is unethical, and may be considered scientific misconduct by your institution.

Paul Braunschweiger Ph.D.
Professor, University of Miami
Director Office of Research Education
CITI Course Coordinator

VITA

Mehmet Secilmis
Engineering Management, Old Dominion University, Norfolk
mseci001@odu.edu

Education:

M.A. in National and International Security Strategies Management and Leadership.
Turkish Army War College, Istanbul, Turkey, 2008

B.S. in System Engineering, Turkish Military Academy, Ankara, Turkey, 1994

Professional Experience:

NATO Supreme Allied Command Transformation HQ Norfolk, Staff Tasking
Coordination Officer, VA, United States, 2010-2013

ISAF, Regional Command Capital (RCC), Chief of Operations Branch, Kabul,
Afghanistan, 2009-2010

Mechanized Division, Chief of Logistics Branch, Turkey, 2008-2009

Infantry Platoon Leader and Company Commander, Turkey 1994-2006