NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A BALANCED APPROACH TO FUNDING HOMELAND SECURITY

by

Steven G. Kral

December 2014

Thesis Advisor:	Ellen Gordon
Second Reader:	Ted G. Lewis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2014	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE A BALANCED APPROACH TO FUNDING HOMELAND SECURITY	5. FUNDING NUMBERS
6. AUTHOR(S) Steven G. Kral	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

State and local funds are currently inadequate for completely securing local infrastructures. This thesis poses a solution to the funding issues by looking at the problem from two perspectives: risk assessment methodology and civic involvement. Risk assessment reduces the need for funding by funding the highest risk return on investment assets only. It is the foundation for determining the funding and resources required for hazard mitigation; however, the current risk methodology used by the Department of Homeland Security, Threat and Hazard Identification Risk Assessment, is flawed because it lacks adequate rigor and does not incorporate a major goal in measuring effectiveness—return on investment.

Citizen involvement may provide an alternative source of funding through crowdsourcing, rather than taxation. Involving citizens in making decisions about resources and raising capital for security measures provides a viable alternative to federal funding and supports public desire to play a role against terrorism. But in order to make such a shift in expectations attainable, citizens must have the trust and transparency that is fostered through accurate assessments, communication, engagement, and reporting.

This thesis evaluates the current risk methodology and its shortcomings and proposes a more rigorous approach based on in-depth, holistic risk analysis to reduce vulnerabilities within a vast network of critical infrastructure assets, and proposes crowdsourcing, crowdfunding, and bonding as alternatives to traditional federal government grant funding.

14. SUBJECT TERMS: return on investment, threat and hazard identification risk assessment, grant funding, Boston Marathon, risk methodology, crowd funding, and crowd sourcing.	15. NUMBER OF PAGES 105
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A BALANCED APPROACH TO FUNDING HOMELAND SECURITY

Steven G. Kral
Homeland Security Government Affairs Advisor,
Washington Metropolitan Area Transit Authority
B.S., Fordham University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
December 2014**

Author: Steven G. Kral

Approved by: Ellen Gordon
Thesis Advisor

Ted G. Lewis
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

State and local funds are currently inadequate for completely securing local infrastructures. This thesis poses a solution to the funding issues by looking at the problem from two perspectives: risk assessment methodology and civic involvement. Risk assessment reduces the need for funding by funding the highest risk return on investment assets only. It is the foundation for determining the funding and resources required for hazard mitigation; however, the current risk methodology used by the Department of Homeland Security, Threat and Hazard Identification Risk Assessment, is flawed because it lacks adequate rigor and does not incorporate a major goal in measuring effectiveness—return on investment.

Citizen involvement may provide an alternative source of funding through crowdsourcing, rather than taxation. Involving citizens in making decisions about resources and raising capital for security measures provides a viable alternative to federal funding and supports public desire to play a role against terrorism. But in order to make such a shift in expectations attainable, citizens must have the trust and transparency that is fostered through accurate assessments, communication, engagement, and reporting.

This thesis evaluates the current risk methodology and its shortcomings and proposes a more rigorous approach based on in-depth, holistic risk analysis to reduce vulnerabilities within a vast network of critical infrastructure assets, and proposes crowdsourcing, crowdfunding, and bonding as alternatives to traditional federal government grant funding.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACE	Atlantic City Electric
BPHC	Boston Public Health Commission
BPU	Bureau of Public Utilities
BRIC	Boston Regional Intelligence Center
C	consequence
CDC	Center for Disease Control
CDP	Center for Domestic Preparedness
CPG	Comprehensive Preparedness Guide
CRS	Congressional Research Service
DARPA	Defense Advanced Research Project Agency
DHS	Department of Homeland Security
DIB	defense industrial base
DOT	Department of Transportation
EOC	Emergency Operations Center
EMS	Emergency Medical Services
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Service
FTA	fault tree analysis
GAO	Government Accounting Office
GOAL	National Preparedness Goal
HAZMAT	hazardous materials
HIV	high-interest vessel
HPFF	high-pressure fluid-filled
HPGF	high-pressure gas-filled
HSGP	Homeland Security Grant Program
HSPD-7	Homeland Security Presidential Directive 7
ICS	Incident Command System
IED	improvised explosive device
IMAT	Incident Management Assistance Team

IRS	Internal Revenue Service
ISO	International Organization for Standardization
JCP&L	Jersey Central Power and Light
JOBS	Jumpstart Our Business Startups Act
JTTF	joint terrorism task force
L	likelihood
MBHSR	Metro Boston Homeland Security Region
MBRA	model based risk assessment
MCI	mass casualty incident
MIT	Massachusetts Institute of Technology
MPD	Metropolitan Police Department
NCR	National Capital Region
NDPC	National Domestic Preparedness Consortium
NIMS	National Incident Management System
NPPD	National Protection and Programs Directorate
NPS	National Preparedness System
NRF	National Response Framework
NWC	National Watch Center
OIG	Office of Inspector General
OMB	Office of Management and Budget
OEC	Office of Emergency Communications
PPD-8	Presidential Policy Directive 8
PSA	protective security advisor
PSE&G	Public Service Electric and Gas
PSGP	Port Security Grant Program
RCCP	Regional Catastrophic Coordination Plan
RRCC	Regional Response Coordination Center
RICCS	Regional Incident Communication and Coordination System
ROI	return on investment
SCFF	self-contained fluid-filled
SEAR	special events assessment rating
SEWG	Special Events Working Group

SHSP	State Homeland Security Program
SNRA	strategic national risk assessment
T	threat
TARP	Threat Awareness and Reporting Program
THIRA	Threat and Hazard Identification Risk Assessment
TSA	Transportation Security Administration
UASI	Urban Area Security Initiative
V	vulnerability
WAWAS	Washington Area Warning and Alert System
WebEOC	Web Emergency Operations Center
WMATA	Washington Metropolitan Area Transit Authority
XLPE	cross-linked polyethelene

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to say THANK YOU to my wife, Preeti; my daughter, Priya; and my son, Max, who have patiently afforded me the time to participate in the Center for Homeland Security and Defense master's program. The earlier mornings at the kitchen counter writing and the time away attending classes could not have been done without the unselfish support of you all. Love you with all my heart.

THIS PAGE INTENTIONALLY LEFT BLANK

I. CURRENT STATE OF DHS' RISK ASSESSMENT METHODOLOGY

The Government Accounting Office (GAO), the National Research Council, the Congressional Research Service (CRS), and various risk experts have disputed the Department of Homeland Security's (DHS's) risk assessment methodology, utilized for allocating the $16.3 billion of State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI) grants since 2003. GAO questions the analysis and calculations associated with the methodology.[1] The National Research Council believes that a group of outside experts needs to take an unbiased look at the DHS grant allocation formulas. CRS has provided numerous studies, which question both the DHS risk methodology and grant allocation formulas. Finally, other experts, such as John Mueller, Mark G. Stewart, and Greg F. Treverton, believe that America needs to examine massive homeland security expenditures by applying analytical risk management approaches that emphasize cost-benefit analysis and determinations of acceptable and unacceptable risks when developing regulations and future funding approaches.[2]

A. CURRENT DHS RISK APPROACH

If DHS is to prevent terrorist attacks within the U.S.,[3] one of its primary statutory missions, it needs to assess risk in an accurate manner. The DHS risk analysis model includes empirical risk analysis and policy judgments. The vulnerability element of the risk analysis model has limitations that reduce its value.[4] Measuring vulnerability is considered a generally accepted practice in assessing risk; however, the DHS risk analysis model does not measure vulnerability for each state and urban area.[5] Rather, DHS considers all states

[1] Government Accounting Office, *DHS Risk-Based Grant Methodology is Responsible, but Current Version's Measure of Vulnerability is Limited* (GAO-08-852) (Washington, DC: Government Accounting Office, 2008), abstract.

[2] John Mueller, and Mark G. Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (Ohio State University, Columbus OH, 2011), abstract.

[3] See P.L. 107–296, § 101, codified at 6 U.S.C. §111.

[4] Government Accounting Office, *DHS Risk-Based Grant Methodology*, abstract.

[5] Ibid.

and urban areas equally vulnerable to a successful attack, and it does not take into account any geographic differences.[6] Thus, as a practical matter, the final risk scores are determined by the threat and consequences scores,[7] which have also been disputed.

B. SIMPLE RISK

Before discussing the issues associated with the DHS risk assessment methodology, one must have a basic understanding of simple risk. Simple risk[8] (R) can be defined as the product of likelihood (L) times consequence (C). Likelihood is defined as the probability of an event, incident, or attack, which can also be defined as the likelihood of a fault, and is depicted by the Greek symbol gamma (γ). Assuming there are multiple assets affected by the attack or incident, each asset is numbered and depicted by its numerical index (i). Therefore, γ_i represents the likelihood that asset i will suffer damages from some hazard.

$$r_i = \gamma_i C_i \qquad \text{Eq. 1}$$

Likelihood and consequence have little meaning without a target and a threat. An estimate of likelihood and consequence is relative to the asset and the threat and is often referred to as the asset/threat pair. Once the asset and threat are known, estimates of the likelihood and consequence make sense. When more than one asset/threat pair exists, aggregate risk is the sum of the risk of the individual asset/threat pairs.

$$R = \Sigma\,(\gamma_i C_i) = r_1 + r_2 \ldots + r_n \qquad \text{Eq. 2}$$

Aggregate risk is the expected loss across all asset/risk pairs. This model assumes that threats, vulnerabilities, and consequences are independent of one another. That is, threat is not affected by vulnerability, and consequence is not affected by threat or vulnerability.

Risk may also be the sum of multiple risks to a single asset. Assuming each threat is independent of all others and only one incident at a time occurs, one can aggregate simple risk across all threats by summation. There is an assumption that threats are independent and that there is no correlation between attack types.

---

[6] Ibid.

[7] Ibid.

[8] Ted Lewis, "Simple Risk," course lecture, Naval Postgraduate School, Monterey, CA.

But what is the risk formula when intent is a factor in the equation? Let threat (T_i) be the probability of an attack.[9] Specifically, threat is the probability that an attack will be attempted but does not include the probability that the attack will be successful. This is the job of vulnerability (V_i). Vulnerability is the conditional probability that an attack or hazard will succeed if attempted. It describes the condition of the asset, while threat describes the intent. Consequence is defined as the damage caused by the event and can be measured in units of lives, dollars, or time. Risk is in the same units as consequence. Therefore, if consequence is in dollars, risk is as well.

$$r_i = T_i \times V_i \times C_i \qquad \text{Eq. 3}$$

Each of the elements of risk is difficult to estimate. Threat may be estimated by experts or deduced by intelligence analysis. Vulnerability and consequence maybe similarly obtained from experts or historical data. Nonetheless, estimating probability and damages is a challenge when applying simple risk analysis. Other methods of estimation, such as modeling and simulation, are used to obtain estimates of these elements (T_i, V_i, and C_i) by simulating the infrastructure system or situation. Game theory may also be used to estimate threat and vulnerability assuming the attacker maximizes risk, while the defender minimizes risk.

In summary, for the remainder of this thesis, risk will be defined as the simple product of threat, vulnerability, and consequence (represented in Eq. 4).

$$r_i = T_i \times V_i \times C_i \qquad \text{Eq. 4}$$

C. ACCEPTANCE OF A SIMPLE RISK FORMULA

With an understanding of simple risk, one can understand why Congress, the president, and the Secretary of Homeland Security have endorsed risk management as a way to direct finite financial resources to areas that are most at risk of terrorist attacks.[10] Risk management is a continuous process that includes the assessment of threats, vulnerabilities, and consequences to determine what actions should be taken to reduce one

[9] Ibid.

[10] Government Accounting Office, *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened* (GAO-12-47) (Washington, DC: Government Accounting Office, 2011), 8.

or more of these elements of risk.[11] DHS has applied risk management principles to the Homeland Security Grant Program (HSGP) through the use of a risk model to assess the relative risk posed to entities throughout the nation (e.g., states, urban areas, ports, mass transit systems) and to help determine eligibility and funding levels.[12] Data for each of the risk variables are collected from offices and components throughout DHS, as well as from other data sources, and then, using the model, each entity is ranked against one another and assigned a relative risk score.[13]

D. ISSUES ASSOCIATED WITH RISK VARIABLES: VULNERABILITY

In June 2008, GAO reported that DHS chose to hold vulnerability constant and consider all states and urban areas equally vulnerable in the HSGP risk analysis model.[14] But how could Atlanta be as vulnerable to a terrorist attack as New York City or the National Capital Region[15] (NCR)? GAO recommended that DHS formulate a method to measure vulnerability in a manner that captures variations across urban areas and states and apply this vulnerability measure in future iterations of the grant allocation model.[16]

1. Assessing Vulnerability: Population Density Is Not a Sufficient Measure

In response to these recommendations and other external feedback regarding the grant programs from Congress, DHS modified the vulnerability index in the fiscal year

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Ibid., 19.

[15] The National Capital Region (NCR) was created pursuant to the National Capital Planning Act of 1952, 40 USC §71. The act defines the NCR as the District of Columbia; Montgomery and Prince George's Counties in the state of Maryland; Arlington, Fairfax, Loudon, and Prince William Counties in the Commonwealth of Virginia; and all cities existing in Maryland or Virginia within the geographic area bounded by the outer boundaries of the combined area of said counties (e.g., Alexandria, Manassas, Manassas Park, Rockville).

[16] Government Accounting Office, *Port Security Grant Program*, 19.

2011 risk analysis model so that vulnerability is no longer held constant.[17] Instead, the new vulnerability index recognizes that different entities can have different vulnerability levels[18] by assessing counts of activities. For example, the vulnerability levels of passenger rail systems are prioritized utilizing the annualized number of passengers; the more passengers, the higher the vulnerability score. Such counts of activities do not allow for an actual vulnerabilities analysis of critical infrastructure but of the potential effects of a disruption to the infrastructure. In fact, if consequence is defined as the damage caused by an event and is measured in units of lives, dollars, or time, then the number of passengers utilizing a rail system is a factor to consider with consequence and not vulnerability.

2. Accounting for New Security Measures in the Vulnerability Calculation

The fiscal year 2011 vulnerability index also did not provide a mechanism to account for how new security measures—such as the installation of cameras or the provision of additional training to security officials—affect an entity's vulnerability, even if those security measures were funded using grant dollars.[19] This limitation was due to the fact that the data elements within the vulnerability index are counts of activities, which recognize the number of activities that may occur but do not account for the protective actions taken to secure them.[20] For example, if an entity installed security cameras throughout a rail mass transit system to monitor passenger activity, one would expect to reduce the system's vulnerability to attack. However, because the "transit passenger" data element within the model's vulnerability index is simply a count of passengers utilizing the transit system and is not a reflection of the security measures in place to protect the

[17] DHS officials reported that the decision to incorporate a vulnerability component in the fiscal year 2011 risk model was primarily based on feedback in the following three reports: (1) Government Accounting Office, *DHS Risk-Based Grant Methodology*; (2) National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, DC: National Research Council, 2010); and (3) Homeland Security Studies and Analysis Institute, *FEMA GPD Risk Integration and Cost to Capability Analysis Final Report* (Arlington, VA: Homeland Security Studies and Analysis Institute, 2010).

[18] Government Accounting Office, *Port Security Grant Program*, 19.

[19] Ibid., 20.

[20] Ibid.

transit system, the new camera system would not reduce the system's vulnerability score as calculated by the risk analysis model. Thus, with this type of measure, a rail mass transit system could only reduce its vulnerability score by reducing the number of passengers utilizing the system.[21] The risk model's so-called robustness is thereby limited because activity counts do not reflect improvements made to security.[22]

When questioned, Federal Emergency Management Agency (FEMA) officials reported that capturing such data on all security improvements would be challenging due to the need to collect and validate data for all entities included in the risk model.[23] However, FEMA officials also acknowledged the importance of incorporating completed security projects as part of the vulnerability component of the risk model and stated that FEMA will continue to refine its vulnerability assessments.[24] Without accounting for the reductions in vulnerability achieved through new security measures implemented, including those funded through homeland security grants, the robustness of the risk model may be limited and not accurately reflect the relative risk of entities throughout the nation.[25] Instead, the risk model would likely continue to recognize the same entities as the highest risk, regardless of the security improvements made. In addition, by not accounting for security improvements resulting from homeland security grants, the security benefits of the grants are also not recognized.[26] Incorporating completed security projects into the vulnerability component of the risk model could help increase its robustness and more accurately direct allocations to the highest risk entities.[27]

3. FEMA Makes Little Progress Calculating Vulnerability

While FEMA officials said developing an improved vulnerability index that incorporates the effect of security improvements would be a challenging process, there are

---

[21] Ibid.

[22] Ibid.

[23] Government Accounting Office, *Port Security Grant Program*, 21.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Ibid.

interim measures FEMA could take to ensure the most precise data available are being used to populate the existing vulnerability index.[28] An example of how FEMA has progressed in this regard is the modification to the hazmat population data component calculation in the fiscal year 2011 Port Security Grant Program (PSGP) risk model.[29] The hazardous materials passing through a port are just as important to consider in calculating the vulnerability and threat of the port as the hazardous materials destined for that port. Rather than measuring only hazardous materials imports, as was done in the fiscal year 2010 and prior models, the modified measure would account for the transit of hazardous materials through a port that is not the final destination, providing added precision to the model.[30]

4. The Need to Refine Vulnerability

Another data component that needs to be considered within the vulnerability index for the PSGP risk model was foreign vessel calls.[31] Even though the PSGP risk model does consider foreign-flagged vessels with a foreign port as their last port of call arriving in U.S. ports,[32] this measure does not account for the variation in risk profiles of these vessels—as, according to the Coast Guard, not all foreign vessels are considered to be of equal risk.[33] Because the Coast Guard does not view all vessels to be of equal risk, it has developed a procedure to identify and target boarding those vessels that pose a high relative security risk to a port. This program, the High-Interest Vessel (HIV) Program, collects data that classifies arriving vessels according to risk, using multiple factors to establish the vessels' risk profiles.[34]

FEMA officials reported that they considered using HIV data in fiscal year 2011, but determined that, due to time constraints, it would be more straightforward to use a count

---

[28] Government Accounting Office, *Port Security Grant Program*, 22.

[29] The hazardous material (HAZMAT) population data component was part of the consequence index in the fiscal year 2010 model. It was moved to the vulnerability index in the fiscal year 2011 model.

[30] Government Accounting Office, *Port Security Grant Program*, 22.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Government Accounting Office, *Port Security Grant Program*, 22.

of foreign-flagged vessels during the first iteration of the vulnerability index.[35] However, FEMA officials reported that they will continue to research additional data elements for inclusion in future-year risk models.[36] Using data from the HIV Program (which the Coast Guard already collects) in future iterations of the risk model could position FEMA to better capture the vulnerability of port areas to vessels arriving from foreign ports and thereby improve the precision of allocations to high-risk port areas.[37]

E. ISSUES ASSOCIATED WITH RISK VARIABLES: THREAT AND CONSEQUENCE

DHS also has latitude to define how "threat" and "consequence" contribute to calculating risk. For most grant allocation programs, FEMA weighs threat as contributing 20 percent to overall risk, and consequence as contributing 80 percent.[38] For some programs that serve multi-hazard preparedness, those weights have been adjusted to 10 percent and 90 percent, respectively, in order to lessen the effect that the threat of terrorism has on the prioritizations.[39] Because threat has a small effect on FEMA's risk analysis, population is the dominant contributor to the consequence term. Therefore, the risk analysis formula used for grant making can be construed as one that, to a first approximation, merely uses population as a surrogate for risk.[40] FEMA indicated that it does not have the time or staff to perform more detailed or specialized consequence modeling, and it also stated to GAO that this coarse approximation is relatively acceptable to the entities supported by the grants programs.[41]

---

[35] Ibid. 23.

[36] Ibid.

[37] Ibid.

[38] National Research Council, *Review of the Department of Homeland Security's Approach*, 35.

[39] Ibid.

[40] Ibid., 35.

[41] Ibid.

1. The Need to Question Threat and Consequences

It is not clear whether FEMA has ever performed a sensitivity analysis of the weightings involved in these risk allocation formulas or evaluated the ramifications of the (apparently ad hoc) choices of weightings and parameters in the consequence formulas.[42] For these reasons, in 2010 the National Research Council of the National Academies recommended that FEMA should seek an external peer review by technical experts outside DHS of its risk-informed formulas for grant allocation to identify any logical flaws with the formulas, evaluate the ramifications of the choices of weightings and parameters in the consequence formulas, and determine if it could improve the transparency of these grant allocation risk models.[43] If population density is the primary determinant for grant allocations, FEMA's transparency can be improved by making that explicit.

2. Controversy of Risk Analysis Model

Such estimates of the variables that comprise DHS's risk analysis model have sparked controversy within the HSGP. In 2010, when DHS announced a reduction in the number of urban areas to be considered for funding under the UASI, the urban areas that were going to be cut organized campaigns around the concept of the unknown threat in order to maintain grant funds for maintenance and sustainability. Citizens of the urban areas slated to be cut were convinced there were significant threats to their areas, and that without funds, they would be left vulnerable to terrorist attacks. This was exemplified by the state of New Jersey and the commonwealth of Pennsylvania's protest over New York City receiving large sums of homeland security dollars in comparison to their own states. Moreover, this triggered equal and opposite reactions from the urban areas that continued to be considered for funding. Funded urban areas inferred that the risk analysis performed by DHS to allocate homeland security dollars was accurate.

[42] Ibid.

[43] Ibid

F. OTHER EXPERT OPINIONS

There have also been various other expert opinions regarding DHS risk assessment methodology and associated grant expenditures. John Mueller and Mark G. Stewart's book, *Terror, Security, and Money: Balancing the Risk, Benefits, and Costs of Homeland Security*, suggests that America needs to examine massive homeland security expenditures by applying analytical risk management approaches that emphasizes cost-benefit analysis and determinations of acceptable and unacceptable risks when developing regulations and future funding approaches.[44] Such an assessment is deemed critical, since the resulting decisions and actions affect the interests of multiple groups.[45]

Mueller and Stewart find homeland security expenditures since 9/11 have been excessive and not cost-effective.[46] In seeking to evaluate the effectiveness of the massive increases in homeland security expenditures since September 11, 2001, Congress' query has been, "Are we safe?" However, Mueller and Stewart believe this is the wrong question. Of course we are "safer"—the posting of a single security guard at one building's entrance enhances safety, however microscopically. The correct question is, "Are the gains in security worth the funds expended?" Or, as this absolutely central question was posed shortly after 9/11 by risk analyst Howard Kunreuther, "How much should we be willing to pay for a small reduction in probabilities that are already extremely low?"[47]

Gregory F. Treverton, in his book *Intelligence for the Age of Terror*, states, "Anyone's probability of being killed by a terrorist today is essentially zero and would be tomorrow, barring any major discontinuity. So, they (American citizens) should do nothing."[48] Such an approach deals up front with a key issue in risk assessment—evaluating the likelihood of a terrorist attack. But such an approach has scarcely ever been

---

[44] Mueller, and Stewart, *Terror, Security, and Money*, abstract.

[45] Ibid.

[46] Ibid.

[47] Howard Kunreuther, "Risk Analysis and Risk Management in an Uncertain World," *Risk Analysis*, 2222, no. 4 (2002): 66–63. See also John Mueller, *Some Reflections on What, if Anything, "Are We Safer?" Might Mean* (Washington, DC: Cato Institute, 2006).

[48] Gregory Treverton, *Intelligence for an Age of Terror* (Santa Monica, CA: Rand Corporation, 2009).

duplicated by politicians and officials in charge of providing public safety.[49] Treverton believes that the awkward problem of dealing with exceedingly low probabilities has been finessed by states and urban areas—and questionable expenditures accordingly justified.[50] He defines this phenomenon as probability neglect and discusses five techniques that are utilized to justify spending.

(1) Focus on Worst-Case Scenarios

Cass Sunstein assesses the worst-case phenomena, and he believes this scenario comes into being when emotions are intensely engaged. He argues that under such circumstances, people's attention is focused on the bad outcome; they are inattentive to the fact that it is unlikely to occur and hence mandate a substantial government response.[51] Sunstein explains that expenditures related to a low probability/high consequence can be emotionally justified. People want to ignore the conventional risk analysis and believe that the nightmare scenario is possible.

(2) Adding, Rather than Multiplying, the Probabilities

The second scenario for probability neglect focuses on the mathematics associated with calculating the probability of an attack. The author of a CRS from 2007 points out that DHS, within its calculation of risk, sums the probability of an attack with the losses from that attack. DHS then utilizes the results, within a rating scale, to distribute grant funds.[52] This procedure violates the principles espoused in accepted risk assessment techniques, such as those codified in international risk management standards supported by the International Organization for Standardization (ISO), which is backed by the U.S.[53]

---

[49] Mueller, and Stewart, *Terror, Security, and Money*, 5.

[50] Ibid., 5–6.

[51] Cass R. Sunstein, *Worst-Case Scenarios* (Harvard University Press, Cambridge, MA, 2007), 8–9.

[52] Ted Masses, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress* (Washington, DC: Congressional Research Service, 2007), 6.

[53] Ibid.

(3) Assess Relative, Rather than Absolute Risk

The third technique, as pointed out by CRS, is to rank relative risk, while neglecting to determine the actual magnitude of the risk.[54] Relative risk is a statistical term used to describe the risk of a certain event happening to one group verses another. Because DHS is assessing risk as a means to allocating resources to buy down risk, it is imperative, according to DHS, that its risk calculations be relative.[55] Risk experts appear to agree that all communities have some level of risk from terrorism, and, from a national perspective, it is necessary to identify the areas and entities across the country most at risk, and to work to reduce that risk. What is less clear, is the best way to evaluate *relative* homeland security risk and establish an acceptable level of risk while attempting to close the most dramatic gaps between risk and capabilities.[56]

This thesis points out that it may be true that New York is more likely to be struck by a terrorist than, say, Columbus, Ohio, and it is also more likely to be struck by a tsunami. Before spending a lot of money protecting New York from a tsunami, we need to get some sense of the likelihood of that event, not simply of how the risk compares to that borne by other cities. The same holds true for terrorism.

(4) Inflating the Importance of Potential Terrorist Targets

A fourth technique is to inflate the importance of potential terrorist targets. The Office of Management and Budget (OMB) defines "critical infrastructure" as "the assets, systems, and networks, whether physical or virtual, so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."[57] Yet vast sums of money are spent to protect elements of the infrastructure whose incapacitation would scarcely be "debilitating" and that would, at most, impose minor inconvenience and quite

[54] Ibid.

[55] Ibid., 15.

[56] Ibid., 6.

[57] Office of Management and Budget, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2011* (Washington, DC: Office of Management and Budget, 2011), 381.

limited costs. The terrorist attacks of 9/11 were by far the most damaging in history, yet, even though several major commercial buildings were demolished, both the economy and government continued to function within New York City and the U.S.[58]

(5) Inflating Terrorist Capacity

A final mistake is to massively inflate or to fail to assess the capacities of the terrorists, and therefore, by inference, both the likelihood that they will attack and the consequences of that attack.[59] All five techniques of probability neglect are considered within this thesis because, if realistic probabilities that a given target will be struck by terrorists were multiplied into the risk calculation, and if the costs of protection from unlikely threats were calculated following international risk management standards, it would be found that vast amounts of money have been misspent.

G. LACK OF AN ROI STRATEGY

Return on investment (ROI) is an important measure of risk assessment effectiveness, but DHS's current risk methodology, threat and hazard identification risk assessment (THIRA), does not incorporate ROI and lacks adequate rigor. If a threat or hazard can be mitigated and risk can be reduced, that reduction should be measurable. Capabilities-building may begin to reflect an ROI if FEMA begins to equate such capabilities to having the ability to respond to low-risk events (i.e., consequences associated with the incident are not considered significant) and potentially preventing the high-risk events from occurring. FEMA's ROI associated with the building of Boston-area capabilities obviously reduced the consequences associated with the marathon bombing. This has led to the conclusion that response capabilities, if activated and at the ready (unlike the previous NCR examples), can be used to calculate an ROI.

[58] Mueller, and Stewart, *Terror, Security, and Money*, 8.

[59] Ibid.

H. MAKING A HOMELAND SECURITY STRATEGY WORK, STARTING WITH THE END-CONSUMER—THE PUBLIC

Regardless of the risk methodology DHS utilizes to substantiate an ROI strategy, DHS may want to evaluate involving the public in decision making and homeland security efforts. In 2008, almost seven years after 9/11, survey data utilizing a nationally representative probability sample of several thousand American adults suggests the public has sustained desire for, and disappointment in the lack of, government-provided opportunities to serve a meaningful role in the country's response to terrorism.[60] The survey indicated that only 37 percent of American adults have ever made sacrifices on behalf of the "war on terror."[61] Moreover, nearly two-thirds of survey respondents felt that government had failed to provide, or clearly explain, ways for average citizens to play a role or participate in their country's defense against terrorism.[62] Americans continue to seek greater opportunities for political and social engagement following 9/11.[63]

I. FUTURE FUNDING STRATEGIES

Both government and nongovernment players have begun experimenting with collaborative dialogue on to how to afford homeland security needs.[64] These experiments range from public agencies pulling together stakeholders for joint discussions of issues, to full-fledged consensus-building efforts, to design proposals for action.[65] Some efforts are simply about the hope of finding a shared identity as a starting place for change and healing community rifts through building trust, transparency, and finding a shared homeland

---

[60] James N. Breckenridge, *The American Perceptions Study: Attitudes and Appraisals of Homeland Security* (Monterey, CA: The Center for Homeland Defense and Security, 2009).

[61] Fathali M. Moghaddam, and James M. Breckenridge, "The Post-Tragedy 'Opportunity-Bubble' and the Prospect of Citizen Engagement," *Homeland Security Affairs* 7, The 9/11 Essays (September 2011): 1–4.

[62] Ibid.

[63] Louis Penner et al., "Effects on Volunteering of the September 11, 2001 Attacks: An Archival Analysis," *Journal of Applied Social Psychology* 35, no. 7 (2005): 1333–1360.

[64] Judith E. Innes, and David E. Booher, *Planning with Complexity: An Introduction to Collaborative Rationality for Public Policy* (New York: Routledge, 2010), 4.

[65] Ibid.

security reality.[66] Crowdfunding[67] and bonding homeland security provides direct access to citizens and allow citizens to fulfill their desire for a meaningful role in the country's response to terrorism. It may also allow leadership to address the negative perception of discounting the average citizen in defense against terrorism and to convince citizens they have homeland security responsibilities. This thesis equates to an experiment in a collaborative form of public involvement beyond legally mandated forums.

J. THESIS STATEMENT

The cumulative increase in U.S. domestic homeland security expenditures over the decade since 9/11 exceeds $1 trillion.[68] The DHS risk methodology, which provides the basis for decisions about allocating these funds to urban areas and states, includes little understanding of the ROI. It is highly unlikely that the U.S. government will continue to spend trillions of dollars on protection, and therefore, an alternative source of funding is needed to sustain homeland security.

K. CLAIM AND RESEARCH QUESTION

DHS needs to develop a long-term, capital investment strategy that protects critical infrastructure, quantifies an ROI, and provides adequate funding. Can homeland security become sustainable by utilizing ROI strategies and a crowdfunding and municipal bonding program?

L. OVERVIEW OF REMAINING CHAPTERS

Chapter II discusses FEMA's approach to developing and justifying core capabilities utilizing the five-step THIRA process. The THIRA process is reviewed, and opinions are presented both regarding FEMA's strategic management and oversight and whether there are appropriate performance measures to gauge success. The response to two no-notice events (January, 2011 snow storm and August, 2011 earthquake) in the NCR are

---

[66] Ibid.

[67] Crowdfunding is by definition, the practice of funding a project or venture by raising many small amounts of money from a large number of people, typically via the Internet.

[68] Mueller, and Stewart, *Terror, Security, and Money*, executive summary.

reviewed to gauge if building response capabilities according to the THIRA process is effective and practical. The chapter concludes by claiming that an ROI strategy can be created around developing capabilities for planned special events.

Chapter III investigates how the city of Boston's response to the marathon bombing demonstrated that capabilities, if activated for planned special events, may allow for an ROI. The chapter also dissects the testimony of FEMA's former Deputy Administrator, Richard Serino, to Congress regarding FEMA's investment within the Boston UASI for the 10 years prior to the bombing. It is specifically evaluated with regard to the tangible and intangible benefits of homeland security grant funds and whether the THIRA process was beneficial in presenting potential threats and risks. An alternative ROI calculation supports Boston's investment strategy in capabilities-building as an appropriate approach for planned special events.

Chapter IV presents Lewis's five-step method of vulnerability and risk assessment. His approach is based on network theory and fault tree technology that uses estimates of cost and the probability of an attack to compute an investment strategy aimed at reducing risk and producing ROI. This method, entitled model based risk assessment (MBRA), is reviewed along with the pros and cons of utilizing such a strategy. Step 2 of this process, development of fault trees, is utilized to show how the city of Boston may have been able to identify the potential threat of an improvised explosive device (IED) triggered during a large-scale event and how the city may have minimize its vulnerabilities and associated consequences by adding preventative measures. A second example of how MBRA could be utilized to evaluate long-term investment is also presented: the New Jersey decision-making process associated with burying power lines verses building overhead power lines in the aftermath of Hurricane Sandy. Finally, questions of resiliency and cost are presented, as well as a discussion of the impact of local jurisdictions when protecting critical infrastructure for long-term security investment.

Chapter VII investigates crowdfunding and bonding at the individual and local jurisdictional levels as alternative methods for funding homeland security investments. The processes involved in these methods also engage citizens so they can become homeland security decision makers. The answer to the future of homeland security funding lies in the

hands of the citizens, and public safety officials must have a means to engage them, to tap the ability, desire, and support of the masses.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FEMA'S NEW MEASURE OF SUCCESS—BUILDING CAPABILITIES

With the introduction of *Presidential Policy Directive 8* (PPD-8) on March 30, 2011, FEMA began equating gains in security and a reduction in risk to building core capabilities[69] and the capability targets—the performance thresholds for each of the core capabilities. FEMA now allocates grant resources to support developing core capabilities for preparedness.[70] Table 1 outlines the core capabilities by mission area: prevention, protection, mitigation, response, or recovery. Such a model replaces "vulnerability" with "capability," in a sense replacing a measure of gaps with a measure of the ability of a system or community to withstand an attack or disaster, or to respond to it.[71] These measures of capabilities can more readily be aggregated to produce regional and national measures of security—a macro measure of national "hardness" against homeland security hazards.[72]

Table 1. Core Capabilities by Mission Area

Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public Information and Warning				
Operational Coordination				
Forensics and Attribution	Access Control and Identity Verification	Community Resilience	Critical Transportation	Economic Recovery Housing
Intelligence and Information Sharing	Cybersecurity Intelligence and Information Sharing	Long-term Vulnerability Reduction	Environmental Response/Health and Safety	Health and Social Services
Interdiction and Disruption	Interdiction and Disruption	Risk and Disaster Resilience Assessment	Fatality Management Services	Infrastructure Systems

[69] Federal Emergency Management Agency, *National Preparedness Goal*, 1st ed. (Washington, DC: Federal Emergency Management Agency, 2011), 1.

[70] Ibid.

[71] National Research Council, *Review of the Department of Homeland Security's Approach*, 35.

[72] Ibid.

Prevention	Protection	Mitigation	Response	Recovery
Screening, Search, and Detection	Physical Protective Measures	Threats and Hazard Identification	Infrastructure Systems	Natural and Cultural Resources
	Risk Management for Protection Programs and Activities		Mass Care Services	
	Screening, Search, and Detection		Mass Search and Rescue Operations	
	Supply Chain Integrity and Security		On-scene Security and Protection	
			Operational Communications	
			Public and Private Services and Resources	
			Public Health and Medical Services	
			Situational Assessment	

A. JUSTIFYING CAPABILITIES SPENDING THROUGH THIRA

So how does DHS establish informed and defensible capability targets and commit appropriate resources to closing the gap between a target and a current capability or sustaining existing capabilities? FEMA's response can be found in the THIRA guidance. FEMA believes that THIRA allows a jurisdiction to understand threats and hazards and how impacts may vary according to time of occurrence, season, location, or community factors.[73] The results of THIRA should be used by jurisdictions to make informed decisions about how to allocate resources.[74] Additionally, THIRA provides each jurisdiction a framework to establish capability targets and monitor progress toward building, sustaining, and delivering capabilities, as well as manage the risk it faces.[75]

[73] Federal Emergency Management Agency, *Use of Threat and Hazard Identification and Risk Assessment for Preparedness Grants: An Addendum to the THIRA* (Washington, DC: Federal Emergency Management Agency, 2012), 1.

[74] Ibid.

[75] Ibid.

The THIRA process consists of five basic steps outlined in Figure 1 and explained below.

Figure 1. The Five-Step THIRA Process

(1) Identify the Threats and Hazards of Concern

A community should identify a list of the threats and hazards of concern to the community based on past experience, forecasting, expert judgment, and available resources. FEMA suggests reviewing a list of the types of threats/hazards contained within the THIRA guidance to determine potential examples of natural, technological, and/or human-caused threats.[76] Table 2 shows the threats and hazards that should be considered during this identification step.

Table 2. List of Threats and Hazards[77]

Natural	Technological	Human-Caused
Avalanche	Airplane crash	Biological attack
Animal disease outbreak	Dam failure	Chemical attack
Drought	Levee failure	Cyber incident
Earthquake	Mine accident	Explosive attack
Epidemic	Hazardous materials release	Radiological attack
Flood	Power failure	Sabotage
Hurricane	Radiological release	

[76] Department of Homeland Security, *Threat and Hazard Identification*, 3.

[77] Ibid., 6.

Natural	Technological	Human-Caused
Landslide	Train derailment	
Pandemic	Urban conflagration	
Tornado		
Tsunami		
Volcanic eruption		
Wildfire		School and workplace violence
Winter storm		

(2) Give Threats and Hazards Context

Using the list of threats and hazards, develop context that shows how those threats and hazards may affect a community.[78] This step is concerned with the "when" and "where" for each of the threats and hazards identified in Step 1.

(3) Examine the Core Capabilities Using the Threats and Hazards

Using the threat and hazard context, identify impacts to the community through the lens of the core capabilities described in the *National Preparedness Goal* (GOAL).[79] This step requires the community to identify the desired outcomes against the predefined core capabilities.

(4) Set Capability Targets

Looking across the estimated impacts to the community, in the context of each core capability and coupled with a jurisdiction's desired outcomes, set capability targets.[80]

[78] Ibid., 2.

[79] Ibid., 3

[80] Ibid.

(5) Apply the Results

Build the resources to deliver the targeted level of capability with either community assets or through mutual aid, identify mitigation opportunities, and drive preparedness activities.[81]

The THIRA guidance illustrates this five-step process:

> A jurisdiction identifies tornadoes as a hazard and assesses its vulnerabilities if a tornado strikes at different times, seasons, and locations. Using the core capabilities identified in the National Preparedness Goal (GOAL), the jurisdiction assesses the impacts and identifies the highest potential capability target level for Fatality Management Services. Preparing for response, the jurisdiction develops typed resources using the National Incident Management System to accomplish the required Fatality Management Services target. These resources are either built or sustained through collaboration with non-traditional partners, mutual aid planning, or direct investment by the jurisdiction. The jurisdiction may also undertake mitigation planning and projects such as safe rooms and warning systems that have been proven to lessen fatalities. Taking these actions reduces vulnerability, lowering the Fatality Management Services capability target in future THIRAs.

To be effective, FEMA believes the THIRA process requires the participation of the whole community in sharing information, accounting for population-specific factors, and understanding the initial and cascading effects of a threat or hazard. Analysis of the THIRA results should guide future preparedness efforts across all mission areas, allowing a jurisdiction to develop a strategy to allocate resources effectively, achieve capability targets, and reduce risk.[82] Such a strategy should consider finding, connecting to, and strengthening community resources by leveraging the expertise and capabilities of individuals, communities, the private and nonprofit sectors, faith-based organizations, and all levels of government;[83] ultimately, a jurisdiction may find that it must fill gaps in order to build and sustain capabilities. Finally, the analysis can also be used to educate

[81] Ibid., 2.

[82] Ibid.

[83] Ibid.

individuals, families, businesses, organizations, and executive leaders on the risks facing their community and on their roles in preparedness.

FEMA trusts that the THIRA process ensures a shared understanding of capabilities and requirements across the nation by reviewing local and state THIRAs through a review process that includes all regional partners in a collaborative effort with the states.[84] This review ensures that each submitted THIRA is developed in alignment with the *Comprehensive Preparedness Guide (CPG) 201* and answers the following questions:

1. Did the jurisdiction provide description statements of the threats and hazards of concern?
2. Did the jurisdiction provide outcome statements for all 31 Core Capabilities from the GOAL?
3. Did the jurisdiction provide estimated impacts for all threats and hazards of concern in relation to the 31 Core Capabilities?
4. Did the jurisdiction provide capability targets for all 31 Core Capabilities?
5. Did the jurisdiction provide an affirmation that their submittal is in compliance with CPG 201?[85]

The FEMA regions will engage with their partners across the whole community (including other federal agencies) to develop Regional THIRAs.[86] This process will leverage information contained in the strategic national risk assessment (SNRA) as well as inform its future revision to ensure it accurately reflects regional variation in threats and hazards.[87]

B. THIRA'S ROI QUESTIONED

On March 20, 2012, the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications, questioned FEMA's new approach during a hearing entitled *Ensuring the Transparency, Efficiency, and Effectiveness of Homeland Security Grants*. Testimony was presented by

---

[84] Federal Emergency Management Agency, *Use of Threat and Hazard Identification*, 2.

[85] Federal Emergency Management Agency, *Threat and Hazard Identification and Risk Assessment Information Sheet* (Washington, DC: Federal Emergency Management Agency, 2013).

[86] Federal Emergency Management Agency, *Use of Threat and Hazard Identification*, 2.

[87] Ibid.

the Assistant Inspector General for Audits of DHS' Office of Inspector General (OIG), Ann L. Richards, who discussed FEMA's need to make improvements in strategic management, performance measurement, and oversight, to ensure the transparency, efficiency, and effectiveness of the grant process.[88] Specifically, the Inspector General pointed out that strategic planning, performance measurement, and oversight—including tracking states' milestones and accomplishments for HSGP-funded programs—are important management controls, ensuring federal funds are utilized for their intended purpose and preparedness capabilities are enhanced.[89]

Building capabilities enhances public safety officials' understanding of the potential threats they face and the capabilities they will need to prevent, protect, mitigate, respond, and recover from a potential disaster. However, except for in instances of planned events, difficulties arise when operating and implementing prevention and protection capabilities. This indicates that prevention and protection capabilities only work well during such planned events in which operating centers are activated.

The Honorable Michael A. Nutter, Mayor of Philadelphia and Vice President of the U.S. Conference of Mayors, also submitted testimony that questioned if local government officials, emergency managers, and first responders have a role in the THIRA process so that local (i.e., major cities within large states) concerns are taken into consideration when assessing capability gaps. Mayor Nutter explained his firsthand experience of the risks associated with the city of Philadelphia, which were dismissed from homeland security grant fund consideration at the state level. He also questioned if FEMA can ensure federal funding is utilized to improve preparedness in high-risk areas, as recommended by the 9/11 Commission.[90] Mayor Nutter's statements point to the issue that FEMA guidance

---

[88] *Hearing before Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications, U.S. House of Representatives, Ensuring the Transparency, Efficiency, and Effectiveness of Homeland Security Grants*, 112th Cong. (2012) (testimony of Ann L. Richards, Office of Inspector General).

[89] Ibid.

[90] *Hearing before Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications, U.S. House of Representatives, Ensuring the Transparency, Efficiency, and Effectiveness of Homeland Security Grants*, 112th Cong. (2012) (testimony of Michael Nutter, Mayor of the City of Philadelphia)

directs authority for the development of the THIRA and the distribution of homeland security grant dollars to the individual states. The state may not, and does not have to, agree with the THIRA analysis performed by the metropolitan areas within the state. For example, Philadelphia may have determined that acts of terrorism are the leading threat for the commonwealth of Pennsylvania. The commonwealth may not agree, and instead believe the largest threat is flooding due to large storms.

C. THE PRACTICALITY OF CAPABILITIES-BUILDING

Conceptually, it makes sense to think of building up capabilities in order to add to local jurisdictions' and states' collective homeland security. But is it practical? This question was the basis of a 2012 GAO evaluation of the NCR's management of grant resources, under the supervision of FEMA, to build capabilities.[91] The NCR is an urban area that includes the District of Columbia and local jurisdictions in the state of Maryland and the commonwealth of Virginia.[92] A network of committees—composed of senior federal, state, and local officials and subject matter experts—work together to allocate homeland security grant funds to build the core capabilities needed to achieve the GOAL.[93] Since 2003, DHS has allocated over $560 million through the UASI grant program to the NCR.[94] To help facilitate operational communications and information sharing across local, state, and federal government entities within the NCR during an emergency, over $24 million of UASI funds were utilized to purchase communication tools and programs, including

(1) Web Emergency Operations Center

---

[91] Government Accounting Office, *Performance Measures and Comprehensive Funding Data Could Enhance Management of the National Capital Region Preparedness Resources* (GAO-13-116R), (Washington, DC: Government Accounting Office, 2013), 1.

[92] 10 U.S.C. 2674(f)(2).

[93] UASI grant recipients must create a working group with representation from the region that will be responsible for coordinating development and implementation of program elements. Before funding can be distributed, DHS also requires each UASI recipient to develop and submit a strategic plan that outlines the region's common goals, objectives, and steps for implementation. The strategy is intended to provide each recipient with direction for enhancing regional capability and capacity to prevent and reduce vulnerability.

[94] Government Accounting Office, *Performance Measures and Comprehensive Funding Data*, 1.

A web emergency operations center is a web-enabled, user-friendly, and locally-configurable incident and event management system. With access to the Internet, authorized emergency managers and first responders, regardless of location, can enter and view incident information on WebEOC status boards. WebEOC enables users to manage multiple incidents and daily events, assign and track missions and tasks, provide situation reports, manage resources, and prepare reports.[95]

(2) Regional Incident Communication and Coordination System

Regional Incident Communication and Coordination System (RICCS) consists of two securely-hosted servers and software with capabilities for conference calling, short text messages to cell phones or pagers, and longer messages to email accounts. RICCS is utilized by public safety officials and the NCR leadership to rapidly communicate emergency information to area officials, and to convene conference calls or other meetings for decision-making.[96]

(3) The Emergency Management Network

The Emergency Management Network (EMNet) is a secure, satellite-based messaging system allowing emergency operations centers (EOCs) to coordinate response, recovery, and requests for assistance if other commercially-based systems fail.[97]

(4) Washington Area Warning System

The Washington Area Warning System (WAWAS) is a FEMA-owned system utilized by NCR partners, which is the primary audio alert and information-sharing system among EOCs during an incident. The NCR has built a system of **communication and collaboration tools** between all jurisdictions' EOCs that includes **videoconferencing** and

[95] WebEOC [product sheet], accessed December 12, 2014, http://www.esi911.com/esi/index.php?option=com_content&task=view&id=14&Itemid=30

[96] The RICCS system sends notices to email, pagers, and mobile phones and continues to operate if mobile voice bandwidth becomes jammed. It currently serves about 1,500 users in more than 50 groups, which include top local, state, and federal officials in each homeland security and emergency management discipline. RICCS is owned by the Metropolitan Washington MWCOG and is independent of the citizen alerting systems operated by local governments with UASI funds.

[97] Currently the systems receive all messages sent out by the National Weather Service and other authorized senders.

satellite phone communications dispatch service. The videoconferening system, installed in 2007, allows EOCs and other government agencies to communicate with each other via video bridge. The satellite phones are used for regional emergency management communications when primary and secondary communications fail during an event.

(5) NCRnet

The National Captial Region Net (NCRnet) is a UASI-funded, private, fiber optic communications network that interconects the NCR jurisdictions and provides the primary underlying communications interconnectivity for video conferencing capabilities. Despite multiple communications tools and systems put in place since 9/11, none were activated during a fast-moving snowstorm on January 26, 2011 or the earthquake on August 23, 2011.[98] This resulted in a lack of real-time, situational awareness, and minimal regional communication and coordination, causing emergency management officials and first responders to react to each of the incidents, rather than act proactively before the impact occurred. Regional situational awareness, one of the 31 core capabilities, was not present for either event.

During the January 26, 2011, snowstorm conditions deteriorated rapidly in the NCR as heavy precipitation overspread the region at the start of the late afternoon rush hour. Colder air moved into the area during this time, which caused the precipitation to change quickly to sleet and then to heavy snow. Heavy snow continued through the evening hours with snowfall rates around two to three inches per hour during the height of the event.[99] Many commuters experienced eight to 12 hour commutes due to snow and ice covered roads; abandoned and disabled cars, trucks, and buses; and outages of traffic signals lacking backup power.[100] A November 2011 report by regional officials found that some of the problems cited during the snowstorm were caused by early dismissal of many of the

[98] Metropolitan Washington Council of Governments, *Report of the Steering Committee on Incident Management and Response: A Proposal for a Regional Incident Coordination Program and over a Dozen Other Improvements to Enhance Incident Management and Response in the National Capital Region* (Washington, DC: Metropolitan Washington Council of Governments, 2011).

[99] National Oceanic and Atmospheric Administration, "Snowfall Totals," National Weather Service Forecast, January 26, 2011, http://www.erh.noaa.gov/lwx/events/snow_20110126/

[100] Government Accounting Office, *Performance Measures and Comprehensive Funding,* 5.

region's employees, which resulted in a compressed rush hour just as weather and traffic conditions were deteriorating.[101] Despite the worsening traffic, no regional officials initiated a conference call to exchange information and coordinate a phased release of workers or to consider a region-wide message to the public, even though they had purchased the capabilities to do so utilizing homeland security grant funds.[102]

Later in the year on August 23, 2011, the largest earthquake to hit the mid-Atlantic states of the U.S. in more than a century jolted the NCR, prompting widespread building evacuations, snarling traffic, and sending emergency crews scrambling after reports of superficial damage and minor injuries. The quake rumbled across the D.C. region at 1:51 p.m., bewildering tourists, residents, and workers who spilled onto city streets while offices, schools, and attractions were inspected for structural damage. The U.S. Geological Survey estimated the magnitude of the earthquake at 5.8.[103] Once again, emergency decision makers turned inward and focused on the immediate concerns of their individual jurisdiction or state; there was minimal regional communication about evacuating the downtown core of Washington, D.C., This was exemplified in the abrupt release of federal government workers, who make up approximately 40 percent of the workforce in Washington, D.C., Federal workers flooded the transportation networks in a simultaneous race to get home.

Examining the history of numerous previous events, it is a known fact that the transportation networks in the NCR cannot support the mass evacuation of downtown Washington, D.C., without a phased release of the federal government workforce. Streets in the downtown core immediately become congested and the congestion spreads in concentric rings from downtown to the outer suburbs. It was again obvious that the release of the federal workforce was neither communicated nor coordinated. Situational awareness, regional coordination, and public alerts and warnings were cited by regional

---

[101] Metropolitan Washington Council of Governments, *Report of the Steering Committee*.

[102] Ibid.

[103] Dave Boyer, Tom Howell, and Shaun Waterman, "5.8 Magnitude Quake Jolts Eastern US," *Washington Times*, August 23, 2011, http://www.washingtontimes.com/news/2011/aug/23/earthquake-jolts-dc-area/?page=all

officials as capabilities needing enhancement in the region's assessment of the response to the January 26, 2011, snowstorm and the August 23, 2011, earthquake.[104] The NCR had spent $24 million dollars for six separate communication tools to have regional situational awareness during an emergency, but none of the tools were utilized during fairly minor natural emergencies.

D. ROI ANALYSIS—THREAT, VULNERABILITY, AND CONSEQUENCE

If one applies the five THIRA steps to winter storms and other natural disasters, it is apparent that the NCR adhered to the process by purchasing communications capabilities to assist in preventing gridlock and responding to such incidents. However, the capabilities were not activated during either of the above no-notice events, with negative consequences. Based on the risk calculations, the NCR purchased communications equipment to coordinate the federal government and notify the public, but the capabilities were not utilized. There was no reduction in risk from the communications equipment, so the ROI for purchasing the capabilities is zero in both cases; the expenditures are not cost-effective. It is challenging to quantify the ROI associated with building capabilities. Even if the communications tools were activated the day of each event, it is difficult to see a way or a means of quantifying how many lives were saved, how many injuries prevented, or how much less road congestion existed due to a coordinated release. It also cannot be determined how many terrorist incidents have been thwarted due to increased capabilities. For example, what if three individuals were stopped in Logan airport today because of small pocket knives in their carry-on luggage? The individuals would be asked to discard the knives prior to entering the terminal and would be able to continue on with their trip. Has the increase in screening capabilities at airports thwarted terrorism attempts? The answer is that we do not know, nor will we ever know. These unknowables are the type of quantifiable data government officials and the public want to justify homeland security grant expenditures.

Rather than search for the illusive answers surrounding natural disasters or thwarted terrorist activities, FEMA should focus on calculating the ROI of grant expenditures for

[104] Government Accounting Office, *Performance Measures and Comprehensive Funding,* 4.

special events, such as the Boston Marathon. During such special events, the capabilities that have been purchased are activated to prevent incidents from occurring or prevent severe consequences if an incident does occur. The event itself allows for additional parameters to be established such as a specified amount of time and space, and approximate number of individuals associated with the event. The parameters allow for pre- and post-measurements to be established, which in turn allows for ROI calculations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. HOW TO CALCULATE DHS' ROI IN RESPONSE TO THE BOSTON MARATHON BOMBINGS

DHS said during the response to the April 15, 2013, Boston Marathon incident, the City of Boston's preparedness systems worked as they should, unlike the NCR's preparedness systems in the previous examples. DHS attests that, because of the investment in local and state resources, the city of Boston was not overwhelmed the day of the event but instead was able to effectively respond.[105] The city's response demonstrates an ROI and shows significant progress over the previous 10 years.[106] But some believe that the success of the response was due to a number of fortunate (and unrepeatable) circumstances, and there are still significant concerns that FEMA's grant programs do too little to ensure that grant funding is spent addressing the highest threats and risks.[107]

This chapter investigates how the city of Boston's response demonstrates that capabilities, if activated for planned special events, allow for an alternative ROI calculation by evaluating the number of lives saved against the total UASI funds spent by the city. Such a calculation indicates that capabilities-building can work as an investment strategy.

A. DHS'S ROI

In his testimony before the Homeland Security Government Affairs Committee on July 10, 2013, FEMA's Deputy Administrator Serino stated,

> Quite simply, our preparedness system worked that day like it should: we invested in local and state resources, those resources were not overwhelmed the day of the event, and local and state responders were able to effectively respond. This shows the efficacy of our programs and demonstrates our return on investment.

This statement shows that FEMA has begun to equate the successful response to the increased capabilities in the Boston UASI. But the consequences associated with the

---

[105] *Lessons Learned from the Boston Marathon Bombings* (testimony of Richard Serino), 5.

[106] Ibid.

[107] *Lessons Learned from the Boston Marathon Bombings: Preparing For and Responding to the Attack, Hearing before the Committee on Homeland Security and Governmental Affairs,* 113th Cong., (2013) (remarks by Tom Coburn).

Boston Marathon bombings were not considered significant from a terrorist-event prospective. Four lives were lost during the bombing incident, including one law enforcement official associated with the apprehension of the terrorists. Simply, the consequences associated with this event were not considered significant. It is questionable whether FEMA can measure if the increased capabilities purchased with homeland security grant funds actually saved lives that day.

To support the claim that FEMA reaped an ROI, four critical points are made (1) FEMA's guidance served as the basis for the collective response;[108] (2) FEMA's grant funds provided commodities and training that were essential in response to the explosion;[109] (3) Boston's 2012 THIRA accurately identified complex attacks (such as a mass casualty or active shooter) as one of the top threats and hazards, allowing grant dollars to be spent appropriately;[110] and (4) with FEMA's assistance, state and local public safety officials demonstrated proper incident response.

1. FEMA's ROI: A Collective Response

FEMA defines "whole community" as an approach to emergency management that reinforces the notion that we must leverage the resources of our collective team at every level of government to prevent, prepare for, protect against, respond to, and recover from, all hazards, and that collectively we must meet the needs of the entire community in each of these areas.[111] This larger collective emergency management team includes state, local, tribal, and territorial partners as well as non-governmental organizations like faith-based and non-profit groups, the private sector, individuals, families, and communities, who continue to be the nation's most important assets as first responders during a disaster.[112] But FEMA continues to search for innovative ways to involve the private sector, individuals, families, and communities within homeland security strategies.

---

[108] *Lessons Learned from the Boston Marathon Bombings* (testimony of Richard Serino), 5.

[109] Ibid.

[110] Ibid., 9.

[111] Federal Emergency Management Agency, *National Preparedness Goal*, A-2.

[112] Ibid.

FEMA provides proof that the collective guidance assisted in developing the whole community response. Deputy Administrator Serino testified that on April 15, 2013, Americans witnessed the strength of the whole community—people coming together to help each other and making America's collective response that much more effective and efficient.[113] FEMA supports such a statement by accepting that the approach to national preparedness helped to empower and strengthen the whole community, by giving its members the right tools and information they needed to be prepared[114] through its preparedness programs: training and exercises, technical assistance, and community preparedness.

FEMA considers the National Preparedness System (NPS) as the instrument that the nation employs to build, sustain, and deliver the core capabilities that work toward the GOAL. FEMA requires grantees, including both the commonwealth of Massachusetts and the city of Boston, to implement the NPS and establish a whole-community approach to homeland security and emergency management.[115] FEMA concluded that because of the NPS implementation, the whole Boston community was better planned, organized, equipped, trained, and exercised, resulting in improved preparedness and resilience.

FEMA's guidance also served as the basis for the collective response. First responders in Boston used the National Incident Management System (NIMS) and the National Response Framework (NRF) as the basis for developing and conducting exercises before the event.[116] Agencies and organizations involved adopted the Incident Command System (ICS), conducted planning and operations using unified command, and integrated aspects of the region's disaster plans into the event's operations plan.[117]

---

[113] *Lessons Learned from the Boston Marathon Bombings* (testimony of Richard Serino), 3.

[114] Ibid.

[115] Ibid.

[116] Ibid., 4.

[117] Ibid.

2. FEMA's ROI: Sources of HSGPs

The second of four areas where FEMA experienced an ROI was within its HSGP. Many of the capabilities demonstrated in Boston and in the immediate aftermath of the bombings were built or enhanced, and have been sustained, through the preparedness suite of HSGPs, including the UASI Grant Program and the SHSP.[118] Since 2002, the commonwealth of Massachusetts has received more than $943 million in FEMA preparedness grant funds.[119] Since 2003, Boston itself has received more than $369 million through eight grant programs, including $179 million through UASI grants.[120] Both Massachusetts and Boston invested state, local, and federal grant funds in systems that were considered critical during the response.[121] FEMA believes that the grant funds provided resources and training that were essential in response to the explosions.

a. Resources

- Boston implemented the Emergency Patient Tracking System, a secure, web-based application that facilitates incident management, family reunification, and overall accountability for patients during emergency incidents. The system ensured patients were triaged and transported in an orderly manner to the appropriate hospital based on their needs.[122]
- The Boston Public Health Commission (BPHC) invested $200,000 in Mass Casualty Incident (MCI) medical supplies and equipment to stock the special operations vehicles at the marathon, which proved crucial in responding to victims of the bombings.[123]
- BPHC also used more than $920,000 in grant funds for first responder safety, including purchasing equipment and supplies such as personal protective equipment and radiation dosimeters for first responders.[124] Both the protective equipment and the radiation dosimeters were used in the immediate aftermath of the bombings.

---

[118] Ibid.

[119] Ibid.

[120] Ibid.

[121] Ibid.

[122] Ibid.

[123] Ibid., 5.

[124] *Lessons Learned from the Boston Marathon Bombings* (testimony of Richard Serino), 5.

- The grant funds also supported planning and coordination, authorizing staff salaries for medical surge planning projects (such as patient tracking), and coordinating health and medical services. These capabilities were particularly essential in ensuring a coordinated and successful response and recovery operation following the blasts.[125]
- HSGP grants provided more than $3 million for screening, search, and detection equipment, such as a forward-looking, infrared imaging unit used by the Massachusetts State Police to search for, locate, and apprehend the surviving bombing suspect, and the camera systems that were used during the post-incident investigation.[126]
- More than $7 million in UASI grants were leveraged for on-site security and protection, including much of the equipment used during the event, such as bomb robots, x-ray equipment, and ballistic helmets and vests.[127]
- Operational communications were bolstered, with nearly $15 million in funding through UASI grants going toward such enhancements as the addition of frequencies to support the regional mutual aid radio systems, which include law enforcement, fire services, and EMS.[128]

b. Training, Exercises, and Technical Assistance

First responders of the commonwealth and Boston UASI also trained and exercised through support from FEMA, making them more equipped to serve their communities during real-world incidents. Training examples include:

- Since 2000, more than 5,500 Boston area responders received training through FEMA partners, including the National Domestic Preparedness Consortium (NDPC) and Continuing Training Grantees. During that same period, FEMA's Center for Domestic Preparedness (CDP) provided chemical/biological and mass casualty training to more than 500 Boston responders and providers.[129]
- FEMA supported 12 exercises directly involving the City of Boston, including topics as diverse as chemical and biological attacks, hurricane preparedness, hazardous materials events, cyber threats, and IEDs.[130] In 2011, DHS, in conjunction with the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center, hosted a Joint Counterterrorism

[125] Ibid.

[126] Ibid., 6.

[127] Ibid.

[128] Ibid.

[129] Ibid.

[130] *Lessons Learned from the Boston Marathon Bombings* (testimony of Richard Serino), 6.

Awareness Workshop that focused on integrating response operations to a complex attack in the Boston metropolitan area. More than 200 participants from the local, state, and federal communities participated in the workshop.[131]

- In 2012, as part of FEMA's Regional Catastrophic Preparedness Grant Program, the Metro Boston Homeland Security Region (MBHSR) exercised the Regional Catastrophic Coordination Plan (RCCP) designed to augment existing operations plans by facilitating communication, situational awareness, and functional area coordination across the region in a catastrophic event.[132]
- More than $275,000 was used to fund MCI training, education, and exercises for first responders. In 2003, Boston Emergency Medical Services (EMS) utilized funding to pilot a training and exercise program, which later became the DelValle Institute for Emergency Preparedness, and that has since trained tens of thousands of first responders.[133]
- In March 2013, grant funds were used to coordinate a psychological first-aid course for first responders providing pre-hospital medical care.[134]
- Boston also used UASI funds to train SWAT teams to better integrate bomb technicians into tactical operations, a crucial capability that was demonstrated in the aftermath of the marathon bombings.[135]
- DHS technical assistance and funding enabled the City of Boston to codify its emergency response plans and protocols through planning support initiatives including assistance with IED awareness, fusion centers, equipment, anti-terrorism training, and interoperable communications. Further, the National Protection and Programs Directorate (NPPD) Office of Emergency Communications (OEC) worked closely with jurisdictions in the MBHSR to improve coordination, training, and tactical planning for emergency communications.

FEMA asserts that the ROI for training, exercising, and planning is the development of new skills, the promotion of continuous improvement, and the development of relationships before they must be relied upon in a crisis,[136] which allows for a reduction in consequences associated with an event and a reduction in overall risk.

---

[131] Ibid.

[132] Ibid.

[133] Ibid., 5.

[134] Ibid.

[135] Ibid., 7.

[136] Ibid., 6.

c. FEMA's ROI: Boston's 2012 THIRA Identified the Potential Threat

To provide a common, consistent approach for identifying and assessing risks and associated impacts, the City of Boston developed its 2012 THIRA. The THIRA expanded on existing state, territorial, tribal, and local hazard identification and risk assessments. The results guided preparedness efforts across all mission areas and educated individuals, families, businesses, organizations, and executive leaders on the risks facing the city and on their roles in preparedness. FEMA testified that Boston's 2012 THIRA identified complex attacks, such as the Boston Marathon bombing, as one of the top threats/ hazards.[137] This assessment assisted the commonwealth of Massachusetts and the Boston urban area in planning and preparing for such a scenario and prioritizing the development of capabilities to address known and evolving threats.

d. FEMA's ROI: Appropriate Incident Response

Finally, the Boston Marathon was evaluated by the interagency Special Events Working Group (SEWG), managed by the DHS Office of Operations Coordination and Planning, and was determined to be a high-risk event, which resulted in enhanced attention across federal agencies and assured a greater level of situational awareness and coordination of dedicated federal resources.[138] Through its interagency relationships and established special event processes, DHS was positioned to respond very quickly to the needs of state and local partners.[139] This preparation was instrumental to the rapid federal response to the Boston Marathon bombing in several ways:

- FEMA participated in Boston Marathon security coordination meetings with other federal, state, and local partners including: DHS NPPD Federal Protective Service (FPS), the Massachusetts Homeland Security Advisor, the Commonwealth Fusion Center/Massachusetts State Police Counter-Intelligence Unit; the Boston Regional Intelligence Center (BRIC), and the FBI/Joint Terrorism Task Force (JTTF).[140]

---

[137] Ibid.

[138] Ibid.. 7.

[139] Ibid.

[140] *Lessons Learned from the Boston Marathon Bombings* (testimony of Richard Serino), 7.

- While intelligence reporting indicated no credible threat to the event, its designation as a Special Events Assessment Rating (SEAR) by the SEWG meant there were federal, state, and local security and logistical support resources on hand.[141] The FBI was designated the event's lead federal law enforcement agency and the Massachusetts State Police was the designated lead local law enforcement and public safety organization.[142] The Massachusetts EOC was the designated operations center for the event.
- The DHS Massachusetts Protective Security Advisor (PSA) participated in Boston Marathon security coordination meetings and worked directly with owners and operators of critical infrastructure to identify facilities in proximity to the event. Engagement included documenting protective measures, reviewing past assessments, providing local and state partners with map books of all critical infrastructure and chemical facilities in close proximity to the marathon route, and monitoring infrastructure on a real-time basis.[143]
- FEMA activated Region I's Regional Response Coordination Center (RRCC) and the Region's Incident Management Assistance Team (IMAT).[144]
- FEMA monitored the situation from headquarters in Washington, D.C., coordinating with other agencies at the National Watch Center (NWC), which coordinates closely with the DHS National Operations Center for national-level information sharing, situational awareness, and common operating picture.[145] The NWC was activated to Enhanced Watch to include the NWC Threat Monitoring Team, and additional personnel were advised of the potential for a deployment.

FEMA believes that an ROI was demonstrated by the effective response to the Boston Marathon bombing. The bombing scenario was identified as a possibility utilizing THIRA, capabilities were purchased accordingly, and FEMA guidance ensured a coordinated and managed response.

---

[141] Ibid.

[142] Ibid., 8.

[143] Ibid.

[144] Ibid.

[145] Ibid., 7.

B. CAPABILITIES-BUILDING—AN ROI CALCULATION

Capabilities-building may begin to reflect an ROI if FEMA equates such capabilities to responding to low-risk events (i.e., consequences associated with the incident are not considered significant) and potentially preventing the high-risk events from occurring. FEMA's ROI associated with building capabilities within the Boston area obviously reduced the consequences associated with the marathon bombing. For example, assume, as the current administration has for spending calculation purposes, that a human life is worth $6 million.[146] A FEMA lesson-learned memo indicates that more than 140 lives were saved[147] due to the response capabilities in place the day of the bombing. This would equate to an ROI of over 469 percent if one utilizes the $179 million in UASI funds given to Boston as a direct investment in building capabilities; FEMA can confidently say that the homeland security investment in the city of Boston has a tangible ROI.

As previously mentioned, this has led to the conclusion that response capabilities, if activated and at the ready, (unlike the previous NCR examples) can be used to calculate an ROI. Response capabilities can also assist in calculating ROIs for natural disasters in which public safety officials have time to activate the purchased capabilities. For example, the numerous communication and warning tools in tornado- prone areas of America have given individuals adequate time to find shelter prior to the arrival of the tornado, saving lives. Even though the January 26, 2011 snowstorm in the NCR was predicted, the rate of snowfall was not, and public safety officials did not activate capabilities to assist in preventing the transportation consequences.

Deputy Administrator Serino summed up FEMA's position regarding the Boston Marathon bombing:

> Although we will never forget those whose lives were lost, as a community we can take some solace that our preparedness efforts helped saved lives. At FEMA, we often stress that there is no one agency or entity responsible

[146] Binyamin Appelbaum, "As the U.S. Agencies Put More Value on Life, Business Fret," *New York Times*, February 16, 2011, http://www.nytimes.com/2011/02/17/business/economy/17regulation.html

[147] Federal Emergency Management Agency, *Boston Marathon Bombing, Hospital Readiness and Response, Lessons Learned Information Sharing*, accessed December 12, 2014, https://www.llis.dhs.gov/sites/default/files/Boston%20Marathon%20Bombings%20Hospital%20Readiness%20and%20Response.pdf

> for emergency response. It takes a whole community of emergency responders to prepare for disasters and save lives. I have never been so proud to be a part of the Boston community as I was on April 15. We owe it to those whom we lost and to those who were injured that day to keep improving—and we will work with all of our partners across this great country to honor that moving forward.[148]

The city of Boston also supports that FEMA's investment produced a significant ROI and was exemplified in the response to the Boston Marathon bombings. Kurt N. Schwartz, Undersecretary for Homeland Security, Homeland Security Advisor, and Director of the Massachusetts Emergency Management Agency testified at the same hearing as Serino. Undersecretary Schwartz stated that the response to the events surrounding the Boston Marathon demonstrated the value of the money, time, and resources invested in local, state, and federal homeland security since 2001. Within seconds of the bomb blasts at the finish line, an array of personnel, resources, and capabilities, many funded with federal homeland security grant dollars, were ready to triage and care for the wounded, communicate with the public, provide situational awareness for decision makers, ensure the safety and security of the public and critical infrastructure, set up a joint command center, and ultimately identify and apprehend the suspected terrorists. Schwarz insists there is a clear correlation between the effectiveness of response operations in and around Boston in the aftermath of the bombings, and the local, regional, and state investments in building and sustaining capabilities.[149]

1. Measuring an ROI Alongside Boston's Luck-Factor

Doctor Arthur L. Kellermann, the Paul O'Neill-Alcoa Chair of Policy Analysis at the Rand Corporation, in his testimony entitled "What Should We Learn From Boston?," expressed concern about how DHS measures ROI and that the federal government's grant monitoring effort has focused more on structure (e.g., facilities, equipment, and supplies) and process (e.g., the number and type of people hired, trainings held) than on desired

---

[148] *Lessons Learned from the Boston Marathon Bombings* (testimony of Richard Serino).

[149] *Attacks on the Homeland, Hearing before the Committee on Homeland Security*, 113th Cong., (2013) (Kurt N. Schwarz, Undersecretary, Executive Office of Public Safety and Security, Commonwealth of Massachusetts), www.gpo.gov/fdsys/pkg/CHRG-113hhrg82590/html/CHRG-113hhrg82590.htm

outcomes—the capabilities local and state governments must have to successfully manage a disaster or terrorist attack.[150] He questioned whether or not FEMA's grant programs are employing adequate measures to assess grantee activities and performance.[151] Regardless of whether FEMA's current approach to grants is altered or retained, FEMA faces the difficult task of identifying a manageable number of straightforward standards, focusing less on the process of grant management and more on achieving desired *capabilities* and *outcomes*.

To prove his point, Kellermann focused on the medical response to the Boston Marathon bombing. He specifically points out the reason so many victims of the Boston Marathon bombing survived that day: because Boston first responders were both prepared and lucky. To explain how "luck" played a role, Kellerman speaks to six factors that worked in the rescuers' favor the day of the bombing:

1. The bombers targeted a major event where large numbers of police, security, and EMS personnel were pre-deployed. This dramatically shortened response times.[152] Senator Tom Coburn of Oklahoma, in his opening remarks during the hearing, supported this statement by pointing out,

> The Boston bombing first responders were heroic in minimizing the loss of life, but a number of fortunate (and unrepeatable) circumstances contributed to the successful response. The state, city, and first responder community engaged in extensive planning to support the marathon every year. This included preparing for mass casualties among the runners; maintaining a heavy police, EMS, first responder, and volunteer presence; and running a table-top exercise each year prior to the event to practice responding to different types of scenarios.[153]

---

[150] David Dausey, Nicole Lurie, and Alex Diamond, "Public Health Response to Urgent Case Reports," Data Watch, August 30, 2005, 10.1377/hlthaff.w5.412

[151] Tom Coburn, *Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities*, 2012, http://www.coburn.senate.gov/public/index.cfm?a=Files.Serve&File_id=b86fdaeb-86ff-4d19-a112-415ec85aa9b6

[152] *What Should We Learn From Boston? Testimony before the Committee on Homeland Security and Governmental Affairs*, 113th Cong., 1 (2013) (testimony of Arthur L. Kellermann).

[153] Ibid.

2. The day of the Boston Marathon is a state holiday for the commonwealth, so the city's streets were not choked with traffic.[154]

3. Hospitals were operating at slightly less than maximal capacity. The attack happened shortly before the 3 p.m. shift change, which means that, because day-shift staff remained on duty, double the normal complement of health care providers was on-site at every facility.[155]

4. The bombs exploded in the heart of a city that is home to seven trauma centers and several world-class hospitals. Senator Coburn referred to Boston's medical infrastructure as some of the best in the world. Because Boston EMS took care to evenly distribute the casualties, each trauma center received a manageable number of victims.

5. The two relatively low-yield bombs exploded out-of-doors. Typically, closed-space bombings are more severe because surrounding walls concentrate blast waves.[156] Lack of any structural collapse facilitated the rapid extrication of and medical attention to victims.[157]

6. U.S. military healthcare providers in Iraq and Afghanistan had gained extensive experience in responding to IED injuries, with explosive devices accounting for three-quarters of injuries to American personnel. Their lessons learned have spread through the U.S. trauma care community,[158] and almost every hospital has a surgeon, nurse, or medic with battlefield experience, as well as trauma personnel who have deployed internationally for disaster response efforts.[159]

Kellermann also points to three factors that explain why Boston first responders are considered, in his words, "good" and why possessing that quality was a significant factor in the medical response: bystander response, preparation of EMS, fire, and police, and the hospitals were prepared to do a good job.

Rather than flee the scene, runners tore off their shirts and used them as tourniquets, or applied direct pressure to slow bleeding. Bystanders pulled barriers aside to create access

---

154 City of Boston, "Traffic and Parking Advisory, Marathon Weekend," April 10, 2013, http://www.cityofboston.gov/news/Default.aspx?id=6076

155 *What Should We Learn From Boston?* (testimony of Arthur L. Kellermann), 1.

156 Ron Golan, Dror Soffer, Adi Givon, and Kobi Peleg, "The Ins and Outs of Terrorist Bus Explosions: Injury Profiles of Onboard Explosions Versus Explosions Occurring Adjacent to a Bus," *Injury* 45, no. (2013): 39–43.

157 *What Should We Learn From Boston?* (testimony of Arthur L. Kellermann), 2.

158 Ibid., 2.

159 Atul Gawande, "Why Boston's Hospitals Were Ready," *The New Yorker*, April 17, 2013, www.newyorker.com/news/news-desk/why-bostons-hospitals-were-ready

for emergency vehicles, while those with medical training began triaging victims.[160] Kellermann considered these courageous civilians the true first responders.

A few years before the marathon bombings occurred, more than 700 of the city's pre-hospital and hospital-based responders learned the basics of blast-injury care at a city-wide "Tales of Our Cities" anti-terrorism conference hosted by (then) Boston EMS director Rich Serino and sponsored by the Center for Disease Control (CDC).[161] Speakers from Madrid, London, Mumbai, and other global cities that have been targets of terrorism described how each specific incident unfolded, how they managed the response, and what they would do differently.[162] Lessons learned from the conference were subsequently woven into the city's response plan. Every hospital that received casualties had a well-crafted disaster plan that had been exercised prior to the event and was ready to put into action the day of the event.[163]

Kellermann maintains that FEMA needs to develop and maintain a set of valid and reliable performance measures that can be used to track progress made, identify areas for improvement, and assist in the development of appropriate accountability systems.[164] In addition, FEMA needs to develop a representation of ROI that can be understood and accepted by Congress and the public. In this vein, Kellermann makes three recommendations that focus on strengthening preparedness research, grant-making, and partnerships.

Kellermann suggests (a) employing a risk-based approach to setting priorities, (b) enhancing coordination by forming an interagency working group, and (c) implementing a simple process to categorize and track current and future preparedness research projects so officials can easily determine which agency is funding what, and quickly disseminate key findings.[165] This will assist with the translation of research to the front lines and shorten

---

[160] *What Should We Learn From Boston?* (testimony of Arthur L. Kellermann), 2

[161] Smith JF Doctors Share Expertise on Handling Terror Attacks, The Boston Globe, June 15,

[162] *What Should We Learn From Boston?* (testimony of Arthur L. Kellermann), 2.

[163] Ibid.

[164] Ibid., 7.

[165] Ibid., 8.

the feedback loop to the research community. An example of the process would be the development of a standardized, searchable format for "after-action" reports.[166]

Going forward, grant-making should be more focused on results and should specify the desired capabilities and outcomes.[167] To compare the current state of grant-making with a desired state, Kellermann uses the analogy of monitoring every test or therapy a doctor orders against the outcomes he or she achieves.

Finally, Kellermann strongly suggests strengthening partnerships with industry regulators who can assist in the development and implementation of preparedness capabilities.[168] Such preparedness capabilities could then be aligned with industry performance measures.

Senator Coburn reinforced Kellermann's perspective by pointing out that Congress has the responsibility to look not just at a few good examples but at the grant programs as a whole.[169] At a time when grant dollars are shrinking, Senator Coburn begs an important question: do Congress and FEMA need to do more to align grant funds with concrete activities that work, such as using models to ensure objective decisions are made when allocating resources for risk/vulnerability reduction.

It is important to note at this point that while capabilities-building for preplanned special events and predictable, naturally-occurring events can be a critical factor in a successful response, it is a short-term investment strategy and does little to prepare the country for large-scale terrorist events that can have wide-ranging effects across our vast network of critical assets. An attack on America's key infrastructure networks could have devastating, long-term consequences; accordingly, a long-term funding strategy needs to be developed to protect such assets.

---

166 Ibid.

167 Brian Jackson, Kay Sullivan Faith, and Henry Willis, *Are We Prepared? Using Reliability Analysis to Evaluate Emergency Response Systems* (Santa Monica, CA. RAND Corp., 2011), http://www.rand.org/pubs/external_publications/EP201100141.html

168 *What Should We Learn From Boston?* (testimony of Arthur L. Kellermann), 8.

169 Coburn, *Safety at Any Price*.

IV. AN ALTERNATIVE ROI STRATEGY: MODEL-BASED RISK ASSESSMENT

The exclusivity in DHS' risk methodology and management may enable DHS to prove that, by building capabilities, an urban area or state can reduce its risk for predictable, natural events and/or preplanned special events, and calculate an ROI for short-term investing. An in-depth, holistic MBRA with limited generalities may assist in developing an ROI strategy; the purpose of the MBRA methodology is to support objective decision-making regarding allocating resources for reducing risk and/or vulnerabilities.[170] The network analysis tool uses an engineering modeling technique to represent all possible faults to related parts of a system, and then determines how to best allocate resources to those parts to minimize overall risk.[171] This differs from DHS' analysis, which is goal-based according to a theory of action, beginning with a pre-specified set of capabilities aligned to program goals.

A. DEFINITION OF ROI

If a threat or hazard can be mitigated and risk can be reduced, that reduction should be measurable. Suppose the cost of reducing or eliminating risk (E) is known. The effectiveness of investing E can be calculated as an ROI. ROI is simply the difference in risk before and after investing E, divided by investment E. This is written in Eq. 5:

$$ROI = \Delta R/E \qquad \text{Eq. 5}$$

representing the benefits derived as a reduction in risk or the "biggest bang for the buck."

Risk reduction can be achieved by reducing threat (T), vulnerability (V), consequence (C), or all three, and through a variety of methods. Politics, layered defense, or improved intelligence may reduce intent, which in turn reduces threat. Target hardening, redundancy, and resiliency all reduce vulnerability. Faster and more capable rescue, response, and planning all reduce consequence.

---

[170] Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security, Defending a Networked Nation* (Hoboken, NJ: John Wiley & Sons, Inc., 2006), 107.

[171] Ibid., 146–147.

When funds are limited, ROI analysis can be utilized to make decisions. DHS refers to this as risk-informed decision making, and the resulting strategy as a risk-informed strategy. But how does one reduce risk when resources are limited? Risk-informed strategy requires that one estimate risk for all assets threatened by human-caused or natural disasters, rank the assets from highest to lowest level of risk, and invest in the highest-risk asset first. One must then work down the list, and when money runs out, stop. This strategy can apply to both prevention and response. However, risk-ranking is not optimal because it does not guarantee the best ROI.

This chapter presents Lewis's MBRA method of vulnerability and risk assessment. His approach is based on network theory and fault tree technology that uses estimates of cost and the probability of an attack to compute an investment strategy aimed at reducing risk. Lewis's concept is to allocate resources in an optimal ROI fashion such that the overall risk is minimized. The argument is that the objective for reducing risk (to eliminate vulnerabilities or simply prevent the worst thing from happening) will present itself.

This method of assessment is based on sound principles of logic, probability, and cost minimization.[172] MBRA provides the policy maker with a scientific answer to the question "what is worthwhile protecting, and for how much?" MBRA combines asset identification with quantitative analysis to reach a policy decision.[173] It tells the decision maker how much money to spend on protecting the most critical components of the infrastructure. By securing the most critical components of the infrastructure, communities are assuring that they can reduce risk and become more resilient to all hazards.

This thesis assumes that critical infrastructure can be understood, analyzed, and protected using a network theory approach. For example, to secure the Washington Metropolitan Area Transit Authority (WMATA) commuter rail system of Washington, D.C., one must secure the metro stations in which a majority of the rail lines converge (i.e., Metro Center as represented by the rail map). Networks can also be represented as mathematical graphs containing nodes and links and depicting which nodes are

[172] Ibid., ix.

[173] Ibid., 107.

connected.[174] Infrastructure such as electrical power, telecommunications, transportation, and water (what some consider the life sectors) can be modeled as networks as depicted in Figure 2. Then these networks can be analyzed rigorously to identify assets that may be at risk.[175] Lewis's five-step process is discussed in more detail below.

Figure 2. WMATA Rail Map[176]

[174] Ibid., 77.

[175] Ibid.

[176] "WMATA Rail Map," accessed December 12, 2014, https://search.yahoo.com/search?fr=mcafee&type=B211US756D20110304&p=WMATA+Rail+map

B. UTILIZING FAULT TREE ANALYSIS WITHIN MBRA

To begin to understand the how a sector can be evaluated for funding strategies, MBRA utilizes the development of a fault tree, which is a model of what happens to the sector when a *threat* turns into a *fault*.[177] A *threat* is an entity that wants to attack a sector component;[178] a *fault* is a failure or failure mode caused by a malfunction, or natural or manmade event; and *vulnerability* is a measure of the likelihood that a fault will occur. A *vulnerability* is defined as the probability of a *threat-induced fault* making *vulnerability* equal to *fault probability* or

V(i) = Probability (i) = Probability that an attack by threat (i) will succeed[179]

So *vulnerability* is a probability that measures the susceptibility of a component to a threat.[180]

A fault tree is simply a model of the components of a critical node or sector, organized as a hierarchy or tree-structured graph.[181] The nodes of the tree are called components, logic gates, and threats. A component is any major asset of the sector, such as a water treatment plant, electrical power transformer, and telecommunication hotel.[182] The root of the fault tree is a special component that represents the entire sector. A threat is any physical or cyber-threat to a sector component. A fault occurs when a threat is activated and successfully damages one or more components of the sector.[183] So, the purpose of the fault tree is to model what happens to the sector when a threat turns into a fault.[184] Also, the logical relationships among threats and the vulnerabilities of components in a sector can all be captured using a fault tree. The output from the fault tree is a list of vulnerabilities that will occur, potentially allowing for the mapping of future long-term

---

[177] Lewis, *Critical Infrastructure Protection in Homeland Security*, 112.

[178] Ibid.

[179] Ibid.

[180] Ibid.

[181] Ibid., 113.

[182] Ibid.

[183] Ibid.

[184] Ibid.

funding strategies. To prove that a fault tree can begin to identify potential short-term funding strategies, the Boston Marathon incident is reviewed. In the next section, the marathon route is evaluated against the IED attack.

C. SHORT-TERM STRATEGY EXAMPLE: PREVENTATIVE SECURITY AND PLANNED SPECIAL EVENTS

An IED is the detonation of an explosive device on or near a target and can be produced in varying sizes, functioning methods, containers, and delivery methods (e.g., person, vehicle, or projectile). IEDs are particularly effective against unarmored civilian targets. For this reason, they are often employed at locations where large populations gather, such as the starting and/or finish line of the Boston Marathon, a crowded special event. Furthermore, IEDs are designed to destroy, incapacitate, harass, or distract. The extent of the damage is determined by the type and quantity of explosive. Effects are generally static, other than cascading consequences (unintended effects), such as incremental structural failure. Exacerbating conditions include ease of access to the target, lack of barriers/shielding, poor construction, and ease of concealment of the device (see Figure 3).[185]

The preponderance of assessment indicates that IED attacks against crowds during special events, such as the Boston Marathon, are the most likely threat. Such attacks require relatively little sophistication in terms of material acquisition and coordinated planning. In addition, the knowledge and methodologies of specific IED attacks are widely available via the Internet to a variety of potential aggressors. Though ultimately less significant than many other forms of attack, repeated or strategically timed IED attacks could well create significant and persistent disruptions in normative operations.

[185] Global Security, "Improvised Explosive Device (IEDs)/ Booby Traps," accessed November 28, 2014, http://www.globalsecurity.org/military/intro/ied.htm

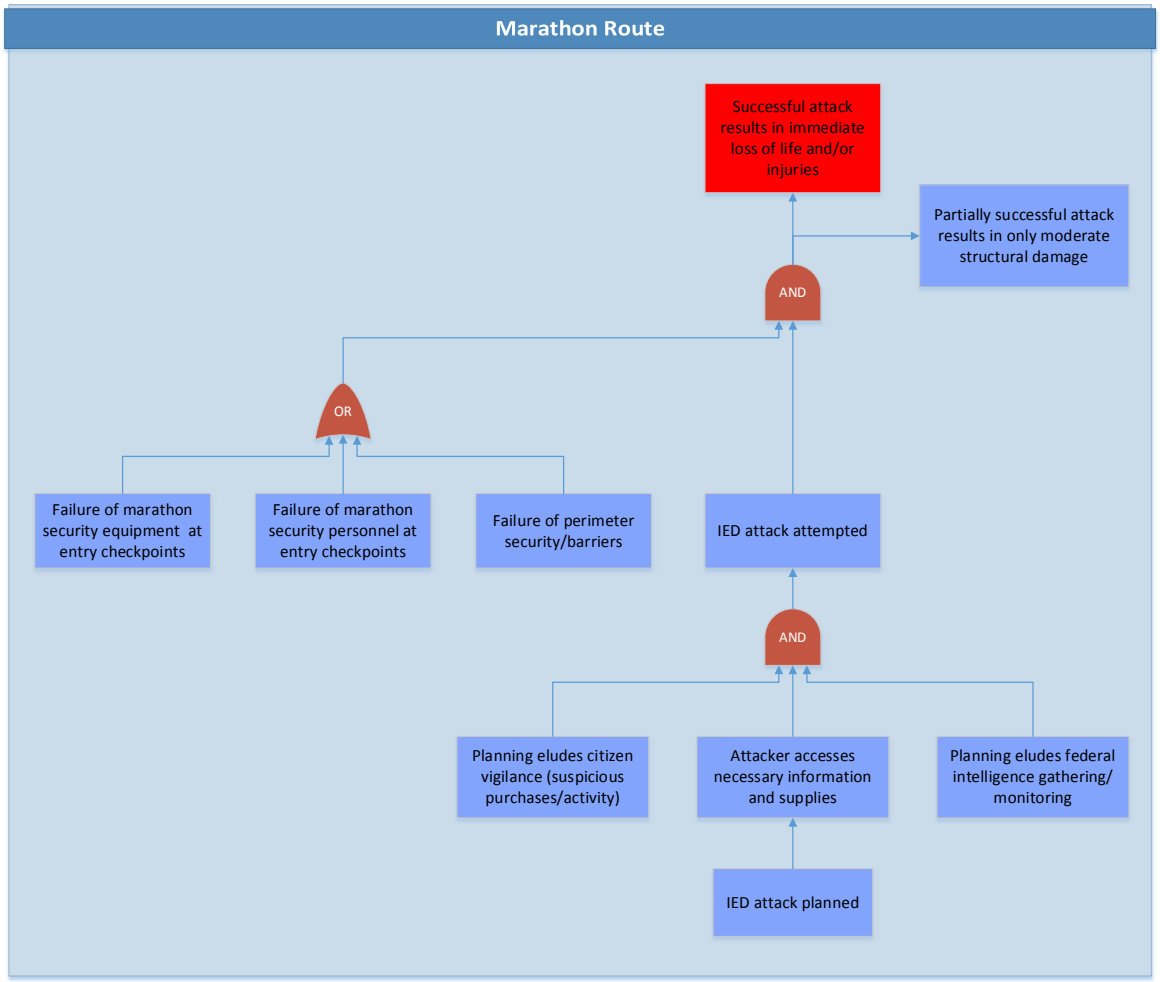

Figure 3. Boston Marathon Route Fault Tree

The fault tree represented in Figure 3 depicts the Boston Marathon route itself as the sector and utilizes an IED scenario as the threat. The vulnerabilities associated with the infrastructure (the marathon route itself) indicate that preventative measures in the form of a layered defense, such as ticketing and screening guests at areas where crowds form (start and finish lines), establishing security screenings for parade-route entry points, and prohibiting items such as backpacks could have reduced the probability that the threat would succeed, or mitigated the resulting damage. Note that it is irrelevant whether the attack is by a participant in the marathon (e.g., suicide belt, backpack, or remote detonation) or a bystander; while the threat itself may be slightly different, the affected components and outcomes are identical.

D. ROI ASSESSMENT FOR PREVENTATIVE SECURITY

Fault tree analysis requires the analyst to estimate four inputs for each threat/asset pair (leaves of the tree): threat, vulnerability, consequence, and cost of preventative measures. The cost associated with such preventative measures can be calculated by estimating the costs associated with the establishment of checkpoints with metal detectors at both the start and finish lines and the additional law enforcement personal needed for such checkpoints. In order to screen approximately 10,000 spectators at both the start and finish lines, approximately seven check points with three individual stations each (one station equates to one metal detector and two law enforcement professionals) would be able to screen all individuals in under two hours. This is based on the assumption that 240 individuals could be screened per station per hour.[186] A total of 42 law enforcement professionals (two for each of the 21 stations) would be needed for a 12-hour shift. The mean average hourly rate for a law enforcement official in the Boston area is $28.45.[187] Since the marathon occurred on a holiday, law enforcement professionals would have received time-and-half, equating to $42.68 per hour. The total cost for additional law enforcement professionals would be approximately $21,511, or $2.15 per individual entering the areas near the start and finish lines. If walk-through metal detectors would need to be purchased (at approximately $4,000 per detector[188]), this would add $84,000 to the screening costs (for one detector at each of the 21 stations) for a total cost of $105,521, or $10.50 per individual entering the areas near the start and finish lines. This equates to an ROI of 796,050 percent if 140 lives were not seriously injured. This is a significant increase in a ROI compared to the 469 percent ROI associated with FEMA's capabilities building. Risk will decrease significantly with the utilization of preventative measures due to the decrease in vulnerability associated with the targets (start and finish lines).

---

[186] Dallas Fort Worth International Airport Planning Department, *Security Checkpoints Tiger Team 2005, Improving Throughput*, rev. (Dallas Fort Worth, TX: Dallas Fort Worth International Airport Planning Department, 2006), 3.

[187] Bureau of Labor Statistics, "Occupational Employment and Wages," May 2013, http://www.bls.gov/OES/current/oes333051.htm

[188] U.S. Department of Justice, "Walk-Through Metal Detectors for Personnel," September 1999, https://www.ncjrs.gov/school/ch3a_5.html

In comparison, the security and preparedness costs for President Obama's 2009 inauguration were approximately $38.825 million for the District of Columbia,[189] for an estimated crowd of 1.8 million spectators. This equates to $26.11 per spectator. More specifically, the costs associated with the Washington, D.C., Metropolitan Police Department (MPD) and other law enforcement brought in to assist the day of the inauguration was approximately $20,907,354.[190] This equates to approximately $11.62 per-individual. All preventative measures, including ticketing of individuals associated with certain vulnerable areas, restricting backpacks, and the screening of individuals, were incorporated into the security plan.[191]

E. LONG-TERM STRATEGY EXAMPLE: POWER LINES AND NATURAL DISASTERS

An understanding of long-term investment in networks and associated vulnerabilities would have been extremely effective for the electric and gas subsector prior to super storm Sandy. According to Atlantic City Electric (ACE), more than 8 million customers across the northeastern U.S. lost power as a result of Sandy. In their initial reports to the New Jersey Bureau of Public Utilities (BPU), companies in the electric and gas subsector described the profound impact of the storm. Statements from Public Service Electric and Gas (PSE&G) and Jersey Central Power and Light (JCP&L) sum up the challenges faced by the entire subsector. PSE&G's statement read, in part:

> This weather event will rank as the worst in PSE&G's history in terms of the number of customers without service, with a preliminary estimate indicating that 1.98 million or 90% of the company's 2.2 million electric customers experienced an extended interruption of service. Sandy interrupted power to one-third of PSE&G's transmission circuits, damaged 2,400 utility poles, and 48,000 [downed] trees.

---

[189] Government of the District of Columbia, *Proposed Budget and Financial Plan, Volume 1, Executive Summary, FY 2010 Meeting the Challenge* (Washington, DC: Government of the District of Columbia, 2008), F-5.

[190] The author of this thesis developed the overall District budget associated with President Obama's 2009 inauguration.

[191] The author of this thesis was part of the Inaugural Planning Committee for the District of Columbia that assisted in the development of the security plan for the 2009 Presidential Inauguration.

JCP&L's statement discussed the challenges of restoration, given the breadth of damage to its infrastructure:

> Due to the extreme force of Sandy, 1,100 of JCP&L's 1200 circuits were damaged, and ultimately, 786 of those circuits were quarantined. In many areas, line workers rebuilt the electrical system. For example, JCP&L serves over 230 municipalities and in some of those towns over 300 poles needed to be replaced. Restoration efforts were challenged by thousands of downed trees, fallen branches and other debris as well as flooding from heavy rain. Also, the Nor'easter brought additional challenges in the form of 12 inches of heavy wet snow to some areas. Damage was so severe that approximately 65,000 trees were cut and cleared to restore power, 34,000 hazard locations were identified and over 19,000 cross-arms, 6,700 poles, 3,600 transformers and 400 miles of wire were damaged.

Rockland Electric Company's (RECO) statement revealed the impact Sandy had on its customer base:

> There were 1,239 'no power incidents' affecting 75,122 customers throughout the RECO Service Territory over the course of the storm. Many customers were affected more than once during the event due to switching and for safety reasons while making permanent repairs to the system….The preliminary data indicates these outages break down by cause and customers affected, as follows:
>
> - Tree Contact—614 interruptions, affecting 53,230 customers;
> - Equipment Failure—34 interruptions, affecting 3,909 customers;
> - No Cause Found—341 interruptions, affecting 11,103 customers;
> - Non-Company Accidents—one interruption, affecting two customers;
> - Unknown—249 Interruptions, affecting 6,878 customers.

The electric and gas subsectors said they faced challenges in working with the various layers and units of government during the response and recovery phase of the emergency. Coordination and communication with municipal and county offices of emergency management proved challenging. Although electric and gas utilities are required to provide a representative to county OEMs, this requirement does not extend to municipal OEMs. This gap in coverage impeded coordination of the overall response. The utilities were confident in the knowledge level and professionalism of their representatives,

but breakdowns in coordination and communication occurred at the county level nevertheless.

Participants also reported that the management of local government expectations was challenging. Specifically, at the municipal level—where, in some cases, the entire infrastructure had to be replaced—a lack of understanding about the restoration of service created unrealistic expectations about how quickly service could be restored. One major theme expressed was the importance of educating government officials at all levels about electric and gas infrastructure and the complexity of restoring power after a disaster.

It was also noted that the storm had greater impact on equipment and industrial control systems when there were single points of failure. Pre-identifying single points of failure before a disaster event could potentially prevent cascading problems. This was particularly true for the Sewaren electrical substation. This particular substation distributed power to all oil refineries in New Jersey. Due to the storm surge, the substation was flooded, and New Jersey and New York City lost all capability to refine and pump petroleum. However, PSE&G noted that the switch was not in the 100-year flood zone and had therefore not been considered as vulnerable as it ultimately proved to be.

The U.S. must begin to investigate the development of long-term investment strategies for critical infrastructure, such as replacing the above-ground electrical distribution systems with below-ground systems. With the increased number of severe storms affecting the U.S., such as Hurricane Sandy, evaluating ROI utilizing Lewis's MBRA will be critical if the electrical companies and the consumer are to support such an investment.

F. CONCLUSION

The following question needs to be answered, "Given the limited budget for protecting networks and building capabilities, how best should the money be spent?" This step will require the derivation of an investment strategy that removes or diminishes the likelihood of faults occurring in the networks if hazardous events occur and determines the capabilities needed for the jurisdiction to respond adequately and become more resilient.

If a jurisdiction decides not to diminish a fault or build a capability, the reasoning associated with this decision needs to be documented and reevaluated on an annual basis.

Due to the cost limitation associated with securing America's infrastructure, this thesis supports the utilization of MBRA as a short- and long-term homeland security strategy. America must begin to analyze its infrastructure, understand its vulnerabilities, and develop infrastructure that is hardened. But for such a strategy to be successful, the investors (i.e., the American public) need to understand the ROI. The success of such a strategy lies in making homeland security part of the American culture and not just a government funding program.

THIS PAGE INTENTIONALLY LEFT BLANK

V. THE FUTURE OF HOMELAND SECURITY INVESTMENT: INFORMED DECISION-MAKING BY THE PUBLIC

Since 2003, DHS has awarded more than $16.3 billion through SHSP and UASI grants to enhance the capabilities within states and urban areas.[192] The cost of maintaining these additional or enhanced capabilities must be absorbed by local operating budgets, but when facing difficult fiscal conditions, state and local governments may reduce their level of contribution towards public safety and, consequently, homeland security preparedness, to address competing priorities. States, urban areas, and jurisdictions need to find alternative means to raise capital to maintain current capabilities and manage risk.

Both governmental and nongovernmental players have begun experimenting with collaborative dialogue on how to afford homeland security needs.[193] These experiments range from public agencies pulling together stakeholders for joint discussions of issues, to full-fledged consensus-building efforts, to design funding proposals for action.[194] These efforts are hoping to build a shared identity as a starting place for change and heal community rifts through building trust and finding a shared homeland security reality.[195] Crowdfunding and bonding homeland security needs can produce informed homeland security ROI strategies and support citizens' desires for meaningful roles in the country's response to terrorism. Such ROI strategies may also allow leadership to solve some negative perception issues and convince citizens that they have homeland security responsibilities. This thesis suggests crowdfunding and bonding, as an experiment in public collaboration for homeland security initiatives beyond legally mandated forums.

---

[192] *Hearing before Committee on Homeland Security, Subcommittee on Emergency Preparedness* (testimony of Ann L. Richards).

[193] Innes, and Booher, *Planning with Complexity*.

[194] Ibid.

[195] Ibid.

A. CROWDFUNDING

Crowdsourcing and crowdfunding are collective efforts of individuals who network and pool their resources, usually via the Internet, to support efforts initiated by other people or organizations.[196] It can involve collecting intellectual support, data, opinions, financial capital, or other forms of assistance. Working within a multitude allows each individual member the benefits of being contributor, but makes it easy by requiring only a small contribution from each person. A small contribution may mean a few minutes of one's time to forward emails or provide an opinion, a minor effort such as dropping off donations, or a small financial donation (according to Crowd Fund Capital Advisors, a group that provides strategy and technology expertise to investors, the average crowdfunding donation is $80[197]). Crowdfunding can also refer to the funding of a company by selling small amounts of equity to many investors. Moreover, crowdfunding investment ideas have been drawing buzz around the nation since Congress passed the Jumpstart Our Business Startups (JOBS) Act and the bill was signed into law by President Obama in April 2012.[198] The new legislation was developed to help entrepreneurs and small businesses raise capital directly from individuals online. Crowdfunding companies, such as RocketHub, Kickstarter, and Indiegogo, have drawn media attention to the idea of donation/reward-style fundraising campaigns. Crowdsourcing and crowdfunding offer strong elements of social networking by opening the discussion, feedback, and funding processes to the general public, which builds in transparency and trust—two of the key factors missing within today's homeland security construct.

---

196 *Wikipedia*, s.v., "Crowdfunding, accessed July 23, 2014, http://en.wikipedia.org/wiki/Crowd_funding. *Merriam Webster Dictionary* defines crowdfunding as "the practice of soliciting financial contributions from a large number of people especially from the online community." *Merriam Webster Dictionary*, s.v., "Crowdfunding," accessed July 23, 2014, http://www.merriam-webster.com/dictionary/crowdfunding

197 Jason Best, and Sherwood Neiss, "Crowdfund Investing—Trick or Treat? Crowdfund Capital Investors Isn't the Bogeyman Some Would Have to Believe," October 29, 2012, http://www.crowdfundcapitaladvisors.com/blog/crowdfund-investment/108-crowdfund-investing-trick-or-treat-cfi-isn-t-the-bogeyman-some-would-have-you-believe.html

198 Securities and Exchange Commission, *Eliminating the Prohibition Against General Solicitation and General Advertising in Rule 506 and Rule 144A Offerings*, http://www.sec.gov/rules/proposed/2012/33-9354.pdf

Sherwood Neiss, entrepreneur, in testimony before the subcommittee on the Threat Awareness and Reporting Program (TARP), Financial Services, and Bailouts of Public and Private Programs in the U.S. House of Representatives on September 15, 2011, equated crowdfunding with a college football team. He stated, "The team is not in the majors, and it takes a good team and a solid fan base to propel the team to the championship. In crowdfunding, the fans are the investors that, more likely than not, know the players and rally around them, providing strategies, experience, and money, not so they can pay their way to the big game but so they can launch a company that will benefit the entire community."[199]

Such opportunities to engage knowledgeable stakeholders and benefit the whole community present themselves when proposing new and innovative homeland security initiatives for the local community.

In August 2012, AppsBlogger looked at a total of 45,815 Kickstarter projects and nearly $215 million in pledged funds. The study found that only 54 percent of completed projects had succeeded.[200] If only about half of these crowdfunding projects succeed, why are people not raising concerns, but instead pledging more via platforms like Kickstarter than ever before? The answer is simple—people inherently want to be part of a community, and they want recognition for it. People are drawn to crowdfunding because they are capitalists at heart. According to the Sustainable Economies Law Center, the success of crowdfunding sites demonstrates the desire of members of the public to support projects they believe in; the possibility of financial return only reinforces this economically healthy impulse.[201] Crowdfunding is more than just money; it is facilitation, dedication, team building, and valuation. These are the ingredients needed to make a new homeland security

[199] Best, and Neiss, "Crowdfund Investing—Trick or Treat?"

[200] "News on Kickstarter—About 41% of the Projects Fail," August 3, 2012, http://edithosb.wordpress.com/2012/08/03/kickstarter/

[201] Elizabeth M. Murphy, "Petition for Rulemaking, Exempt Security Offerings up to $100,000 with $100 Maximum per Investor from Registration," Sustainable Economics Law Center, July 1, 2011, http://www.crowdsourcing.org/document/sustainable-economies-law-centers-selc-petition-for-rulemaking-exempt-securities-offerings-up-to-100000-with-100-maximum-per-investor-from-registration/3618

reality that is relevant to the current global fiscal scenario and meets the consumer's need for involvement.

The AppsBlogger review of Kickstarter also defined some potential measures for successful funding; one is the lower the cost, the more likely the project is to succeed. In 2012, the average funded Kickstarter project cost was $10,000, although 17 of the projects funded on this platform alone were over $1 million.[202] Today, $10,000 remains a reasonable goal for successful Kickstarter projects, and to-date, 82 of their projects have reached six or seven figures.[203] Forbes also supports the claim that successful crowdfunding projects set a reasonable financial goal, and meet that goal within the first 30 to 40 days.[204] This bodes well for projects on smaller, neighborhood and municipal scales, and suggests that breaking large projects into smaller, manageable goals may be prudent in order to obtain funding in a timely manner.

It is also notable that a surprising percentage of funded projects on Kickstarter (8.5 percent) received more than double their financial goal, reaching over 200 percent of requested funding.[205] On Indiegogo, 87 percent of funded projects exceed their goal, by an average of 31 percent.[206] Because the public can see that a project has already reached its goal, and yet continues to pledge, this suggests again that people are more than willing to support efforts they see as necessary or good.

---

[202] "News on Kickstarter—About 41% of the Projects Fail."

[203] Ibid.

[204] Chance Barnett, "Donation-based Crowdfunding Sites: Kickstarter vs. Indiegogo," *Forbes*, September 9, 2013, http://www.forbes.com/sites/chancebarnett/2013/09/09/donation-based-crowdfunding-sites-kickstarter-vs-indiegogo/

[205] "News on Kickstarter—About 41% of the Projects Fail."

[206] "Indiegogo Insight: 87% of Campaigns that Reach Their Goal Exceed It," December 8, 2011, *Indiegogo Blog*, http://go.indiegogo.com/blog/2011/12/indiegogo-insight-87-of-campaigns-which-reach-their-goal-exceed-it.html

1. Examples in Homeland Security

Currently, the avenues for public involvement are limited. Immediately after large-scale disasters, many individuals, looking for a way to be part of the solution, donate items to the victims. Donations are so numerous, in fact, that donations management has become its own emergency support function in many city and state disaster response plans. In particular, people feel a need, or prefer, to donate their used clothing. Unfortunately, most clothing is not utilized and instead becomes trash. This results in more work for the local first-responding agencies, which now have to manage the resulting trash as well. But what if someone developed a business plan to process clothing donations for consignment? The proceeds from the clothing sales could then be given directly to the disaster victims. If the business plan was posted on a crowdfunding website immediately after the disaster, it would maximize the number of potential investors to fund the start-up, capitalizing on press and social media coverage of the incident, and the resulting public urge for involvement. Funds could even be pledged by the victims themselves, who would receive an ROI for their financial contribution through the return of gained profits. This would allow not only those unaffected by the disaster to contribute and assist, but it also would allow the victims of the disaster to "help themselves," to be active participants in their own recovery. A victim puts money into funding the start-up, unaffected citizens provide donations of material goods for sale, victims buy needed items (perhaps at deep discounts, while others buy at consignment prices), and victims receive the proceeds/profits from the remaining sales.

Another hypothetical example of homeland security crowdfunding could be an additional security fee added to the ticket of a large event such as the Boston Marathon or the Presidential Inauguration. Such a fee (comparable to the size and magnitude of the event) could allow for preventative measures to be put in place so that the threat and vulnerabilities are reduced; ultimately, this would reduce the overall risk to the individual spectator. Large cities around the country have begun to re-evaluate the cost of a permit for special events to be inclusive of preventative measures. Such cost is then redirected to the individual spectator or participant as an additional fee (a form of crowdfunding).

The significant capabilities and benefits of crowdsourcing were exemplified in December 2009 by a Defense Advanced Research Projects Agency (DARPA) competition.[207] To mark the fortieth anniversary of the ARPANet, precursor to today's Internet, DARPA announced the DARPA Network Challenge. The challenge was to be the first to submit the locations (i.e., latitude and longitude coordinates) of 10 moored, 8-foot, red, weather balloons at separate, previously undisclosed, fixed locations in the continental U.S. The balloons would be in readily accessible locations (e.g., parks or public squares) and visible from nearby roads. Because of the potentially wide geographic distribution of the balloons (actual locations were: two in California, and one each in Arizona, Delaware, Florida, Georgia, Oregon, Tennessee, Texas, and Virginia) and short preparation time (DARPA announced the challenge one month before the contest start), any strategy necessitated use of the Internet for mobilization and intelligence gathering. The focus of the competition was to explore how broad problems can be tackled using Internet tools, specifically, and most importantly to this discussion, what role social networking can play in the team building and urgent mobilization required for time-critical needs. Researchers hoped to gain insight on basic issues such as collaboration and trust in diverse social networking constructs.[208]

The winning team, comprised of five students from the Massachusetts Institute of Technology (MIT), found all 10 balloons in less than nine hours. Their performance roundly beat the other 4,000 individual participants in the challenge and shocked DARPA, which had scheduled the competition for a full week. Incredibly, the team learned of the contest only four days before it started. In less than two days they had a plan, a website, and more than 5,400 people signed up to help them.[209] In less than one week, five students constructed a productive, precise, layered, networked enterprise involving thousands of citizens.

---

[207] Defense Advanced Research Projects Agency [DARPA], "DARPA Network Challenge," accessed July 13, 2013, http://archive.darpa.mil/networkchallenge/

[208] Ibid.

[209] Lance Whitney, "MIT Floats Ideas in DARPA Balloon Challenge," *CNET News*, December 8, 2009, http://www.cnet.com/news/mit-floats-ideas-in-darpa-balloon-challenge-q-a/

Rather than develop a platform, or use any specific existing platform for networking, the MIT team created a simple website, inviting participants to join, outlining their strategy, and encouraging the use of any and all social networking platforms. In their example illustrating how it might work, they cited possibilities such as email, Facebook, and Twitter. At the core of their strategy was an incentive network model, which was developed to encourage social networking of interested people. DARPA offered a total of $40,000 in prize money, which the MIT team allocated equally among the 10 balloons ($4,000 each).[210] The team incentivized individuals by offering $2,000 to the person who found each balloon. They also allocated $1,000 to the person that referred the balloon finder to their website. Then they gave $500 to the person who referred the referrer, $250 to the person that referred them, and so on. This recursive incentive structure essentially propagated itself over existing social networks (e.g., Twitter) as planned. Rather than seeing others as competitors, people were incentivized to get as many friends working for the MIT team as possible, resulting in 5,000+ "workers" in less than two days.[211]

Although no other competitor found all 10 balloons, there were several contestants who successfully located most of the balloons. The strategies employed by other teams and individuals included creating Facebook groups, directly recruiting from social media website groups, utilizing Twitter feeds, and other crowdsourcing techniques. The winning team's ace was the undiminished incentive within each subsequent layer of network modes, which ensured that the social media interest, activity, and impact was more sustained. However, one participant showed that even a more long-term, sustained interest is not necessary to generate enough activity to get the job done; it may be just as possible with a short-term, more focused burst. George Hotz posted a tweet one hour before the start of the competition, but even with only one hour of preparation, Hotz located eight balloons—four directly from his network of 50,000 Twitter followers.[212]

---

[210] Ibid.

[211] Christopher M. Ford, "Twitter, Facebook and the Ten Red Balloons: Social Network Problem Solving and Homeland Security," *Homeland Security Affairs* 7, (February 2011): 1–8.

[212] DARPA, "Network Challenge Project Report," 10.

Another entry with interesting relevance was the iNeighbors team, which included only members of an existing social media site for neighborhood watch communities; they did not market or recruit new participants for the challenge. The goal of iNeighbors was to see how successful an existing network of local users would be. The team successfully located five of the 10 balloons within the nine-hour timeframe.[213] Each of these examples has a particular relevance, but the larger question is whether the DARPA challenge can correlate into a means of funding homeland security needs and incentivizing people to participate.

What the challenge clearly demonstrates is the efficacy crowdsourcing and the power of social media in distributing information and mobilizing people very quickly, all of which are important to the idea of crowdfunding homeland security needs. In regards to incentivizing participation, it is important to note the MIT team's conjecture that people take an active and willing role only if they feel the goal is something good and moral, and that conversely, people are reluctant to participate or recruit participants if they have doubts or mistrust about the purpose.[214] Alexander Petland, Director of the MIT Human Dynamics Laboratory and the professor who collaborated with the team, takes it a step further by hypothesizing that some efforts would fare better with a completely altruistic end-goal.[215] These ideas will play an important role in the discussions of how and why crowdfunding is a viable solution to homeland security funding.

B. BONDS

In addition to crowdfunding, bonding can be successfully employed to fund homeland security. Municipal bonds are issued by state and local governments, also called municipalities, to raise money for public works projects like the construction and maintenance of bridges, hospitals, schools, and water treatment facilities, or maintaining and enhancing the current level of security. A **bond issuer** (the municipality) sells the bond

[213] Ibid., 11.

[214] Ibid., 14.

[215] Charles Choi, "How MIT Won Balloon Search-and-Rescue Challenge," *NBC News*, October 27, 2011, http://www.nbcnews.com/id/45078320/ns/technology_and_science-science/t/how-mit-team-won-balloon-search-and-rescue-challenge/#.VI4YeHs2Uic

to the **bond holder** (the investor). The bond holder lends the issuer a fixed amount of money for a certain amount of time in exchange for regularly scheduled interest payments. Municipal bonds are one of the safest long-term investments. Because they are so secure, they usually carry interest rates that average a percentage point or two below the going rate for Treasury bills. But in early 2008, the interest rate for municipal bonds crept higher than that of Treasury bills and remains higher today. This makes municipal bonds attractive investments because they are exempt from federal, state, and local income taxes, if one lives in the issuing municipality. Since 1913, the Internal Revenue Service (IRS) has allowed investors to withhold paying income tax on any earnings from municipal bonds. So when interest rates for municipal bonds are higher than those for Treasury bills, the local citizen earns significantly more, especially since he or she will not pay taxes on those earnings, and the purchase of the bonds allows him or her to feel a direct relationship with building and securing the community.

Similarly to crowdsourcing, where participants have a need to perceive a good and moral end-goal for a bonding alternative to be successful, citizens must perceive the strategy as fair and equitable. The central assumptions around equity theory (Adams, 1963; Homans, 1961; Walster, Walster and Bercheid, 1978) are that people strive for justice in their social relations, and they experience anxiety when they see themselves in unjust relationships.

C. WHY CROWDFUNDING/BONDING WILL WORK

At the core of crowdfunding and/or bonding is the concept of effective change in both the perceptions and the actions of the general public. However, attempting to change perceptions and actions is not always easy, and there are multiple pitfalls that are often anti-intuitive. Social scientists point to three common myths associated with making effective change. This section of the thesis discusses these myths and why crowdfunding and bonding avoid these mistakes and instead can be effective strategies for facilitating change.

1. Myth1: Education Changes Behavior

The first myth of effective change is that education will change behavior. It has been proven time and again that information is not enough to make effective change occur. Rather, information needs to be tangible, personalized, and accompanied by interaction. In 2008, almost seven years after 9/11, survey data utilizing a nationally representative probability sample of several thousand American adults suggests that nearly two thirds felt the government had failed to provide, or clearly explain, ways for average citizens to play a role or participate in their country's defense against terrorism.[216] Most respondents (66 percent) said that government had failed to clearly explain citizens' roles in the country's fight against terrorism and even more (74 percent) that government had failed to adequately explain how to prepare for acts of terrorism.[217] In the years following 9/11, aside from military enlistment, opportunities for civic engagement associated directly with the threat of terror seemed largely confined to citizen vigilance, such as the nationwide "If You See Something, Say Something" public awareness campaign.

Interviewed on the eve of the Iraq War troop surge, President Bush was asked why he had not "asked more Americans and more American interests to sacrifice something," in particular, sacrifices that would "muster support" and would involve Americans "in the struggle."[218] In response, President Bush referred to his earlier call for volunteerism with USA Freedom Corps and asserted that he strongly opposed what were apparently the primary potential forms of sacrifice considered after 9/11: compulsory military service and tax increases.[219]

Crowdfunding and/or bonding homeland security long-term investments will mandate that homeland security proposals are tangible, personalized, and interactive through the use of MBRA. As shown earlier, MBRA provides a scientific answer to the

---

[216] Moghaddam, and Breckenridge, "The Post-Tragedy."

[217] Ibid.

[218] Ibid.

[219] Jim Lehrer, "President Bush Defends Decision to Send Additional Troops to Iraq," interview by Jim Lehrer, *PBS NewsHour*, January 16, 2007, http://www.pbs.org/newshours/bb/white_house/jan-june07/bush_01-16.html

question "what is worthwhile protecting, and for how much?" MBRA combines asset identification with quantitative analysis to reach a policy decision.[220] It tells the public how much money to spend on protecting the most critical infrastructure components. By securing the most critical components of the infrastructure, communities are assured that they can reduce risk and become more resilient to all hazards. MBRA makes homeland security spending tangible and provides visible ROI.

2. Myth 2: Attitude Changes Behavior

The second myth of effective change is that one needs to change one's attitude to change one's behavior. Instead, if behavior expectations are set, the corresponding attitude will follow. Homeland security strategies presented thus far by DHS have focused on local, state, and or federal government. Even with the PPD-8 "whole community" concept, one has yet to see how the local citizen (the consumer) is involved unless "whole community" refers only to local public safety officials. DHS has never set expectations for individual citizens. In contrast, crowdsourcing, crowdfunding, and bonding set behavior expectations by placing authority over what occurs or does not occur into the hands of the individual citizen. Citizens are expected to express their interest regarding the homeland security concept or strategies being presented, by either contributing or voting "yes" or not contributing and voting "no." The expectation is that the citizen needs to be involved in decision-making, and both crowdfunding and bonding allow for such involvement.

3. Myth 3: People Know What Motivates Them to Take Action

The third and final myth of effective change is that people know what motivates them to take action. However, social scientists believe that people actually do not know what motivates them; people are motivated by other people's actions or by social norms.[221] Crowdfunding and bonding allow people to demonstrate their interest in protecting their community, allow others to witness those demonstrations as they happen, and allow for the

[220] Lewis, *Critical Infrastructure Protection in Homeland Security*, 107.

[221] . Moghaddam, and Breckenridge, "The Post-Tragedy."

maintenance of short- and long-term homeland security strategies as part of the social norm.

4. Historical Perspective on Homeland Security Investments

For capital to be raised, Americans will need to fulfill the calls for public sacrifice, understand the homeland security issues, and vote, if they want their dollars used to support the most vital homeland security needs. History suggests that Americans are willing to make such sacrifices. A World War II campaign called upon American citizens in all income categories to make voluntary contributions through war bonds. The War Bond campaign was carefully crafted to create an emotionally compelling sense of civic duty and public partnership in the war effort. During an all-day fundraising radio broadcast in 1943, the popular singer and celebrity, Kate Smith, explained to her fellow citizens: "When we buy War Bonds, we're not buying tanks and guns and shells and planes. What we're doing is buying our boys back…bringing them home to us, safe and sound once again."[222] The call for voluntary contributions through war bond commitments generated approximately $98.3 billion by 1945, representing almost half the then gross national product.[223]

Another example of American self-sacrifice was the victory garden. Victory gardens, also called war gardens or food gardens for defense, were vegetable, fruit, and or herb gardens planted at private residences and public parks in the U.S. during World War I and World War II to reduce the pressure on the public food supply brought on by the war effort. Basic information about gardening appeared in public services booklets distributed by the Department of Agriculture, as well as by agribusiness corporations such as International Harvester and Beech-Nut. The U.S. Department of Agriculture estimates that more than 20 million victory gardens were planted.[224] The amount of fruits and vegetables harvested from these home and community plots was estimated at 9–10 million tons—an amount equal to all commercial production of fresh vegetables at the time. In addition to

[222] James T. Sparrow, "Buying our Boys Back: The Mass Foundations of Fiscal Citizenship in World War II," *Journal of Policy History* 20, no. 2 (2008): 263.

[223] Ibid.

[224] United States Department of Agriculture, "About Us," March, 28, 2014, http://www.csrees.usda.gov/qlinks/extension.html

indirectly aiding the war effort, these gardens were also considered a civil morale booster, in that gardeners felt empowered by their contributions of labor and rewarded by the produce grown (see Figure 4). All of these benefits made victory gardens a part of daily life on the American home front.

Figure 4. Sow the Seeds of Victory[225]

Many aspects of the public's response to 9/11 followed a similar pattern and revealed an opportunity bubble—a promising, yet fleeting, opportunity to shape the course of subsequent events.[226] In the immediate aftermath, Americans were ready and willing to make personal and collective sacrifices. During the first three weeks following the attacks, the rate of volunteerism increased more than six standard deviations throughout the

[225] "Sow the Seeds of Victory" [image], accessed November 4, 2014, http://upload.wikimedia.org/wikipedia/commons/0/03/Sow_victory_poster_usgovt.gif

[226] Moghaddam, and Breckenridge, "The Post-Tragedy."

nation.[227] Within only three months, charitable donations for 9/11 victims and their families exceeded $1.5 billion.[228] An extraordinary increase in social capital signaled the public's readiness for civic contribution. Public trust and confidence in government reached a 30-year peak in the first few weeks following the attacks[229]; support for leadership was extraordinarily high and widespread. Even prestigious, traditionally skeptical newspapers—for example, *The New York Times* and the *Washington Post*—were uncritically supportive of leadership decisions after 9/11, including the momentous decisions to wage wars in Iraq and Afghanistan, according to retrospective scholarly analysis.[230]

Such self-sacrifice can be explained through pervasive trends in social behavior and the relationship between perceived in-group threat and group cohesion.[231] War bonds and victory gardens during World War II and the increase in volunteerism following 9/11 are examples demonstrating this relationship; when individuals perceive a serious threat to the in-group (such as from an enemy attack or natural disaster), they show greater solidarity with other group members.[232] Showing greater solidarity can mean making enormous sacrifices in order to support the in-group and demonstrating extraordinary resilience in the face of pressures and difficulties.

Judging correctly when and how to make constructive use of the opportunity-bubble after a tragedy is a hallmark of great leadership. Enormous potential for civic generosity and sacrifice is available at the height of an opportunity-bubble, but leaders must choose the types of sacrifices and the timing of calls to action carefully. Timing is of the

---

[227] Penner et al., "Effects on Volunteering of the September 11, 2001 Attacks."

[228] Foundation Center, *Giving in the Aftermath of 9/11: Foundations and Corporations Respond* (New York: Foundation Center, 2002), http://www.fdncenter.org/research/trends_analysis/pdf/sept11.pdf

[229] Pew Research Center, "Trust in Government 1958–2010," in *Distrust, Discontent, Anger and Partisan Rancor: The People and Their Government* (Washington, DC: The Pew Research Center for the People and the Press, 2010), 13–22, http://pewresearch.org/pubs/1569/trust-in-government-distrust-discontent-anger-partisan-rancor

[230] Andrew Rojecki, "Rhetorical Alchemy: American Exceptionalism and the War on Terror," *Political Communication* 25 (2008): 67–88.

[231] Arthur Stein, "Conflict and Cohesion," *Journal of Conflict Resolution* 20 (1976): 143–172.

[232] Fathali M. Moghaddam, *Multiculturalism and Intergroup Relations* (Washington, DC: American Psychological Association Press, 2008).

greatest importance: too early, and people, still reeling from the impact of the tragedy, may be unable to respond. Too late, and people may have grown too detached from the tragedy and accustomed to no commitment. Even later, people (and the media) may focus critically—and perhaps angrily—on leadership's failure to have asked for more, sooner.

D. CONCLUSION

DHS must break through traditional linear methods of relying primarily on formal expertise and replace them with nonlinear, socially constructed processes to engage both experts and stakeholders.[233] Unfortunately, funding decisions have been formulated by locally elected homeland security officials from DHS homeland security strategies and grant guidance. These officials do not operate on the assumption that there is an optimal solution. Instead, they formulate options and consider what the consequences may mean.[234] What has emerged are unofficial experts, inconsistent determinations of risk, and bureaucratic processes at federal, state, and local levels.

What needs to emerge is a new process of collaborative rationality, exemplified in crowdfunding and bonding of homeland security needs. This is an alternative to the traditional linear model with its emphasis on expert knowledge and reasoning based upon argumentation;[235] instead, the affected interested parties jointly engage in face-to-face dialogue, bringing their various perspectives to the table to deliberate on the problems they face together. All interested parties must also be fully informed and able to express their views, and be listened to, whether they are powerful or not. Techniques must be used to mutually assure the legitimacy, comprehensibility, sincerity, and accuracy of what is stated in order for substantial agreement to be reached among a majority.[236]

A social constructionist view, in the form of crowdfunding and bonding homeland security needs, has to begin to take hold, along with a critical/communicative approach to

---

[233] Innes, and Booher, *Planning with Complexity*, 5.

[234] Ibid.

[235] Ibid.

[236] Ibid.

why and how homeland security dollars are spent. This author believes that such an approach begins with the development of an informed, reporting, and just culture.

The nation must begin to rely on the ability of local residents to be effective public citizens. To engage and empower citizens successfully, a homeland security culture must develop that is (1) an *informed culture* in which the individual citizen has an understanding of what constitutes homeland security and the knowledge of the risks and costs associated with existing programs and efforts, (2) a *reporting culture* in which the local government is reporting on the progress of homeland security initiatives, and (3) a *just culture* in which citizens believe they are receiving an adequate ROI. Such a culture is necessary to prepare citizens for their involvement in crowdfunding and bonding efforts.

1. Informed Culture

To develop an informed culture and ensure citizens understand the factors that affect homeland security, communication, and meaningful engagement need to occur between the individual citizens and public safety officials. By sharing information on homeland security programs, policies, costs, and initiatives, public safety officials provide a platform to educate individuals. This may be done in a variety of ways such as convening forums, developing brochures, responding to correspondence, and posting information on websites.[237]

Public safety officials need to get out from behind their desks and engage the community in homeland security discussions at all types of public forums.[238] It would be an interesting scenario if every little league baseball game were to start with a reminder of the phone number to call about suspicious activity within the neighborhood or what to prepare in case of a power outage. The beginning of every school year could start with a security briefing to parents on what happens when a school goes into lockdown. When a resident purchases a new home, a local public safety official might call with a

[237] White House, *Empowering Local Partners to Prevent Violent Extremism in the United States* (Washington, DC: White House, 2011), 5.

[238] Robert Bach, and Kaufman, David, "A Social Infrastructure for Homeland Security: Advancing the Homeland Security Paradigm," *Homeland Security Affairs* 5, no. 2 (May 2009).

neighborhood welcome, a review of key critical infrastructure within the community, and a reminder to report any suspicious activities around the key infrastructure. With measures like these, over time, the individual citizen would become more informed, and an informed culture would be developed within the community.

Such a strategy was utilized by Washington Metropolitan Area Transit Authority (WMATA) in the development of its new safety culture after a train crashed killing nine people in June 2009. This accident revealed numerous safety concerns throughout WMATA. Employees were ill-informed regarding basic safety measures.[239] To begin to develop an informed culture within WMATA, the general manager mandated that all meetings, no matter what the topic, begin with a safety tip. The general manager also began producing a weekly newsletter that included safety lessons. By incorporating this strategy for over three years, employees became more informed of safety issues, and the number of employee accidents dramatically declined.[240]

2. Reporting Culture

Reporting the success or failure of homeland security initiatives could be accomplished by having states and local governments utilize MBRA to develop a long-term homeland security strategy and continue to report the reduction in risk and/or vulnerabilities for a vast network of assets in a community.[241] Every community in the nation must report its annual budget to residents so they understand how their tax dollars enhance the community; this type of reporting needs to exist for homeland security expenditures as well.

---

[239] National Transportation Safety Board, *Collision of Two Washington Metropolitan Area Transit Authority Metrorail Trains near Fort Totten Station* (Washington, DC: National Transportation Safety Board, 2009).

[240] Washington Metropolitan Area Transit Authority Safety and Security Committee, *Safety Report*, (Washington, DC: Washington Metropolitan Area Transit Authority, 2011).

[241] Lewis, *Critical Infrastructure Protection in Homeland Security*, 107.

3. Just Culture

To create a just culture, the public must weigh the reduction in risk against the potential offset of making a small contribution to protect a community's infrastructure. If the public believes that such an ROI is acceptable, then and only then will America truly begin becoming a safer and more secure nation.

The Natural Hazards Center in Boulder, Colorado states:

> Local leaders must define a vision of the future, provide the direction to get there, and establish the priorities to make it happen. They must develop and create a will that is infectious among community politicians and constituents alike. Disaster recovery managers must juxtapose short-term and long-term community needs against the quick-and-easy fix or the perceived rights of select property owners. They must protect the health, safety, and welfare of the community from the desires, power, and influence of those who promote short-sighted solutions. They need to foster personal and community responsibility for recovery decisions that will affect their community for years to come.

The conventional homeland security grant-funding construct (determining associated threats, calculating risks, and understanding public safety needs) must be reconsidered if states and localities are going to maintain their current level of capabilities and continue to build resilient communities. Crafting short- and long-term homeland security budgets, calculating ROIs, and engaging the public allows for a more rigorous evaluation of homeland security needs and delineates where the public is willing to spend time and money. The processes for determining an ROI and mechanisms for engaging the public in funding decisions create the opportunity for citizens—area residents—to determine the levels of need and want for continued security in their own communities. To those ends, this thesis offers a rigorous yet contemporary, multi-approach experiment in legitimizing homeland security spending.

APPENDIX. CRITICAL INFRASTRUCTURE SECTORS AS DEFINED BY DHS

1. Chemical Sector
2. Government Facilities Sector
3. Communications Sector
4. Critical Manufacturing Sector
5. Dams Sector
6. Defense Industrial Base (DIB) Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agricultural Sector
11. Government Facilities Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Transportation Sector
16. Water and Wastewater Systems Sector

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Appelbaum, Binyamin. "As the U.S. Agencies Put More Value on Life, Business Fret." *New York Times*, February 16, 2011. http://www.nytimes.com/2011/02/17/business/economy/17regulation.html

Bach, Robert, and Kaufman, David. "A Social Infrastructure for Homeland Security: Advancing the Homeland Security Paradigm." *Homeland Security Affairs* 5, no. 2 (May 2009).

Barnett, Chance. "Donation-based Crowdfunding Sites: Kickstarter vs. Indiegogo." *Forbes*, September 9, 2013, http://www.forbes.com/sites/chancebarnett/2013/09/09/donation-based-crowdfunding-sites-kickstarter-vs-indiegogo/

Best, Jason, and Sherwood Neiss. "Crowdfund Investing—Trick or Treat? Crowdfund Capital Investors Isn't the Bogeyman Some Would Have to Believe." October 29, 2012. http://www.crowdfundcapitaladvisors.com/blog/crowdfund-investment/108-crowdfund-investing-trick-or-treat-cfi-isn-t-the-bogeyman-some-would-have-you-believe.html

Boyer, Dave, Tom Howell, and Shaun Waterman. "5.8 Magnitude Quake Jolts Eastern US." *Washington Times*, August 23, 2011. http://www.washingtontimes.com/news/2011/aug/23/earthquake-jolts-dc-area/?page=all

Breckenridge, James N. *The American Perceptions Study: Attitudes and Appraisals of Homeland Security*. Monterey, CA: The Center for Homeland Defense and Security, 2009.

Choi, Charles. "How MIT Won Balloon Search-and-Rescue Challenge." *NBC News*, October 27, 2011.ws.com/id/45078320/ns/technology_and_science-science/t/how-mit-team-won-balloon-search-and-rescue-challenge/#.VI4YeHs2Uic

Coburn, Tom. *Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities*. 2012. http://www.coburn.senate.gov/public/index.cfm?a=Files.Serve&File_id=b86fdaeb-86ff-4d19-a112-415ec85aa9b6

Dallas Fort Worth International Airport Planning Department. *Security Checkpoints Tiger Team 2005, Improving Throughput*, rev. Dallas Fort Worth, TX: Dallas Fort Worth International Airport Planning Department, 2006.

Dausey, David, Nicole Lurie, and Alex Diamond. "Public Health Response to Urgent Case Reports." Data Watch. August 30, 2005. 10.1377/hlthaff.w5.412

Department of Homeland Security. *Threat and Hazard Identification and Risk Assessment Guide; Comprehensive Preparedness Guide (CPG) 201*, 1st ed. Washington, DC: Department of Homeland Security, 2012.

Federal Emergency Management Agency. *Boston Marathon Bombing, Hospital Readiness and Response, Lessons Learned Information Sharing*. Accessed December 12, 2014. https://www.llis.dhs.gov/sites/default/files/Boston%20Marathon%20Bombings%20Hospital%20Readiness%20and%20Response.pdf

———. *National Preparedness Goal*, 1st ed. Washington, DC: Federal Emergency Management Agency, 2011.

———. *Threat and Hazard Identification and Risk Assessment Information Sheet*. Washington, DC: Federal Emergency Management Agency, 2013.

———. *Use of Threat and Hazard Identification and Risk Assessment for Preparedness Grants: An Addendum to the THIRA*. Washington, DC: Federal Emergency Management Agency, 2012.

Ford, Christopher M. "Twitter, Facebook and the Ten Red Balloons: Social Network Problem Solving and Homeland Security." *Homeland Security Affairs* 7 (February 2011): 1–8.

Foundation Center. *Giving in the Aftermath of 9/11: Foundations and Corporations Respond*. New York: Foundation Center, 2002. http://www.fdncenter.org/research/trends_analysis/pdf/sept11.pdf

Gawande, Atul. "Why Boston's Hospitals Were Ready." *The New Yorker*, April 17, 2013. www.newyorker.com/news/news-desk/why-bostons-hospitals-were-ready

Golan, Ron, Dror Soffer, Adi Givon, and Kobi Peleg. "The Ins and Outs of Terrorist Bus Explosions: Injury Profiles of Onboard Explosions Versus Explosions Occurring Adjacent to a Bus." *Injury* 45, no. (2013): 39–43.

Government of the District of Columbia. *Proposed Budget and Financial Plan, Volume 1, Executive Summary, FY 2010 Meeting the Challenge*. Washington, DC: Government of the District of Columbia, 2008.

Government Accounting Office. *DHS Risk-Based Grant Methodology Is Responsible, But Current Version's Measure of Vulnerability is Limited* (GAO-08-852). Washington, DC: Government Accounting Office, 2008.

———. *Performance Measures and Comprehensive Funding Data Could Enhance Management of the National Capital Region Preparedness Resources* (GAO-13-116R). Washington, DC: Government Accounting Office, 2013.

———. *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened* (GAO-12-47). Washington, DC: Government Accounting Office, 2011.

Homeland Security Studies and Analysis Institute. *FEMA GPD Risk Integration and Cost to Capability Analysis Final Report*. Arlington, VA: Homeland Security Studies and Analysis Institute, 2010.

Innes, Judith E. and David E. Booher. *Planning with Complexity: An Introduction to Collaborative Rationality for Public Policy*. New York: Routledge, 2010.

Jackson, Brian, Kay Sullivan Faith, and Henry Willis. *Are We Prepared? Using Reliability Analysis to Evaluate Emergency Response Systems*. Santa Monica, CA. RAND Corp., 2011. http://www.rand.org/pubs/external_publications/EP201100141.html

Kunreuther, Howard. "Risk Analysis and Risk Management in an Uncertain World." *Risk Analysis*, 2222, no. 4 (2002): 66–63.

Lehrer, Jim. "President Bush Defends Decision to Send Additional Troops to Iraq." Interview by Jim Lehrer. *PBS NewsHour*, January 16, 2007. http://www.pbs.org/newshours/bb/white_house/jan-june07/bush_01-16.html

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security, Defending a Networked Nation*. Hoboken, NJ: John Wiley & Sons, Inc., 2006.

Masses, Ted. *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*. Washington, DC: Congressional Research Service, 2007.

Metropolitan Washington Council of Governments. *Report of the Steering Committee on Incident Management and Response: A Proposal for a Regional Incident Coordination Program and over a Dozen Other Improvements to Enhance Incident Management and Response in the National Capital Region*. Washington, DC: Metropolitan Washington Council of Governments, 2011.

Moghaddam, Fathali M. *Multiculturalism and Intergroup Relations*. Washington, DC: American Psychological Association Press, 2008.

Moghaddam, Fathali M., and James M. Breckenridge. "The Post-Tragedy "Opportunity-Bubble" and the Prospect of Citizen Engagement." *Homeland Security Affairs* 7, The 9/11 Essays (September 2011): 1–4.

Mueller, John, and Mark G. Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*. Ohio State University, Columbus OH, 2011.

Murphy, Elizabeth M. “Petition for Rulemaking, Exempt Security Offerings up to $100,000 with $100 Maximum per Investor from Registration.” Sustainable Economics Law Center. July 1, 2011. http://www.crowdsourcing.org/document/sustainable-economies-law-centers-selc-petition-for-rulemaking-exempt-securities-offerings-up-to-100000-with-100-maximum-per-investor-from-registration/3618

National Research Council. *Review of the Department of Homeland Security's Approach to Risk Analysis*. Washington, DC: National Research Council, 2010.

National Transportation Safety Board. *Collision of Two Washington Metropolitan Area Transit Authority Metrorail Trains near Fort Totten Station*. Washington, DC: National Transportation Safety Board, 2009.

Office of Management and Budget. *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2011*. Washington, DC: Office of Management and Budget, 2011.

Penner, Louis, Michael T. Brannick, Shannon Webb, and Patrick Connell. “Effects on Volunteering of the September 11, 2001 Attacks: An Archival Analysis.” *Journal of Applied Social Psychology* 35, no. 7 (2005): 1333–1360.

Pew Research Center. “Trust in Government 1958–2010.” In *Distrust, Discontent, Anger and Partisan Rancor: The People and Their Government*. Washington, DC: The Pew Research Center for the People and the Press, 2010.

Rojecki, Andrew. “Rhetorical Alchemy: American Exceptionalism and the War on Terror.” *Political Communication* 25 (2008): 67–88.

Sparrow, James T. “Buying our Boys Back: The Mass Foundations of Fiscal Citizenship in World War II.” *Journal of Policy History* 20, no. 2 (2008): 263–286.

Stein, Arthur. “Conflict and Cohesion.” *Journal of Conflict Resolution* 20 (1976): 143–172.

Sunstein, Cass R. *Worst-Case Scenarios*. Harvard University Press, Cambridge, MA, 2007.

Treverton, Gregory. *Intelligence for an Age of Terror*. Santa Monica, CA: Rand Corporation, 2009.

Washington Metropolitan Area Transit Authority Safety and Security Committee. *Safety Report*. Washington, DC: Washington Metropolitan Area Transit Authority, 2011.

White House. *Empowering Local Partners to Prevent Violent Extremism in the United States*. Washington, DC: White House, 2011.

Whitney, Lance. “MIT Floats Ideas in DARPA Balloon Challenge.” *CNET News*, December 8, 2009. http://www.cnet.com/news/mit-floats-ideas-in-darpa-balloon-challenge-q-a/

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California