NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SILENT WARNING: UNDERSTANDING THE NATIONAL TERRORISM ADVISORY SYSTEM

by

Roy B. Brush

December 2014

Thesis Advisor:	Erik Dahl
Second Reader:	Carolyn Halladay

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

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

4. TITLE AND SUBTITLE
SILENT WARNING: UNDERSTANDING THE NATIONAL TERRORISM ADVISORY SYSTEM

5. FUNDING NUMBERS

6. AUTHOR(S) Roy B. Brush

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)

This research investigated two questions: How effective is the United States Department of Homeland Security (DHS) National Terrorism Advisory System (NTAS) when compared to its predecessor, the Homeland Security Advisory System? And, does NTAS provide sufficient decision advantage for the nation it serves? The research methodology/design used a comparative analysis of results observed for each system as it addressed the problem set presented in a case study. The research found that NTAS is effective but continued improvement is needed.

These improvements include: the formal establishment of a DHS Office of Counterterrorism Coordination; the renewal of the DHS Counterterrorism Advisory Board Charter or other appropriate governance documents to ensure sustainment of necessary decision making and execution authority for NTAS; refine the NTAS Concept of Operations to better demonstrate the system's scalable outcomes other than an NTAS-generated alert, such as Joint Intelligence Bulletins, Joint Threat Assessments, etc.; NTAS-related outreach and education efforts with the homeland security enterprise and the public; and the improvement of communication aspects of NTAS integrating with other warning systems, such as the Integrated Public Alert and Warning System. These improvements are critical in sustaining the current effectiveness of the system and ensuring its future success.

14. SUBJECT TERMS national, terrorism, advisory, system, NTAS and National Terrorism Advisory System, warning, alert, decision, advantage, "decision advantage," HSAS and Homeland Security Advisory System, Boston Marathon bombing, Christmas Day bomber, underwear bomber, hurricane, counterterrorism, CTAB, Counterterrorism Advisory Board, DHS and Department of Homeland Security, dilemma, decision maker, "decision maker's dilemma"

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

SILENT WARNING: UNDERSTANDING THE NATIONAL TERRORISM ADVISORY SYSTEM

Roy B. Brush
National Terrorism Advisory System Coordinator, Department of Homeland Security
B.S., St. Martin's University, 2003
M.A., Troy University, 2004

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: Roy B. Brush

Approved by: Erik Dahl
Thesis Advisor

Carolyn Halladay
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research investigated two questions: How effective is the United States Department of Homeland Security (DHS) National Terrorism Advisory System (NTAS) when compared to its predecessor, the Homeland Security Advisory System? And, does NTAS provide sufficient decision advantage for the nation it serves? The research methodology/design used a comparative analysis of results observed for each system as it addressed the problem set presented in a case study. The research found that NTAS is effective but continued improvement is needed.

These improvements include: the formal establishment of a DHS Office of Counterterrorism Coordination; the renewal of the DHS Counterterrorism Advisory Board Charter or other appropriate governance documents to ensure sustainment of necessary decision making and execution authority for NTAS; refine the NTAS *Concept of Operations* to better demonstrate the system's scalable outcomes other than an NTAS-generated alert, such as Joint Intelligence Bulletins, Joint Threat Assessments, etc.; NTAS-related outreach and education efforts with the homeland security enterprise and the public; and the improvement of communication aspects of NTAS integrating with other warning systems, such as the Integrated Public Alert and Warning System. These improvements are critical in sustaining the current effectiveness of the system and ensuring its future success.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AQAM	al-Qaeda-associated movements
AQAP	al-Qaida in the Arabian Peninsula
CBP	Customs and Border Protection
CONOPS	concept of operations plan
COP	community oriented policing
CT	counterterrorism
CTAB	Counterterrorism Advisory Board
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FPCON	force protection conditions
GAO	Government Accountability Office
HSAC	Homeland Security Advisory Council
HSAS	Homeland Security Advisory System
HSE	homeland security enterprise
HSPD	Homeland Security Presidential Directive
HWS	hurricane warning system
I&A	Office of Intelligence and Analysis
IC	intelligence community
ICAT	Intelligence Crisis Action Team
ICE	Immigration and Customs Enforcement
ICPVTR	International Centre for Political Violence and Terrorism Research
IED	improvised explosive device
IPAWS	Integrated Public Alert and Warning System
JIB	Joint Intelligence Bulletin
NCTC	National Counterterrorism Center
NOC	National Operations Center
NPPD	National Protection and Programs Directorate
NSI	National Suspicious Activity Reporting Initiative

NTAS	National Terrorism Advisory System
NWS	National Weather Service
OPSEC	operations security
OPS	Office of Operations Coordination and Planning
PPD	Presidential Policy Directive
RPV	resources-processes-values framework
SAR	suspicious activity reporting
TIDE	Terrorist Identities Datamart Environment
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USG	United States government
USSS	United States Secret Service

EXECUTIVE SUMMARY

Terrorism warning systems provide warnings for internal (organizational or for official decision makers) and external (other partner organizations or the public) categories of constituents. They must support resolution of the decision maker's dilemma and balance between the need to warn people in danger from terrorism with the need to maintain operational security (OPSEC) for counterterrorism (CT) efforts to mitigate that danger. Therefore, a system is effective if it capably fulfills these two thematic functions related to providing warning and decision advantage.

Determining the effectiveness of a seldom-used warning system, such as the National Terrorism Advisory System (NTAS), is a difficult problem to solve. More difficult is determining the effectiveness of a warning system that seldom provides external warnings because it serves a complex community of both internal and external constituents. Another criterion of the effectiveness of a warning system is its ability to provide sufficient "decision advantage" to the decision makers it serves. The type of threats that terrorism warning systems are used for involves mitigating the additional complexity posed from thinking human adversaries. This additional complexity presents a challenge to homeland security officials in accomplishing the daily mission and also for any effort to evaluate a terrorism warning system with a quantitative approach. These factors mean that any examination of a terrorism warning system must qualitatively accommodate the complex warning community, determine the level of decision advantage it provides, and, in assessing system outcomes, incorporate the mercurial human nature of the threat.

In response to the problem, this research compared the case studies of NTAS and its predecessor, the Homeland Security Advisory System. It included a brief contrast/comparison discussion between the tenets of a terrorism warning system, such as NTAS and the U.S. hurricane warning system (also known as the Tropical Cyclone Forecasting and Warning Program). This discussion of similar systems that address different threats provided important context for the NTAS effectiveness/decision advantage evaluation. A standardized panel of questions, Dr. Erik Dahl's theory of

preventive action, and Clayton Christensen's resources-processes-values framework provided assessment tools to compare the effectiveness of these terrorism warning systems.[1] These tools also were used to assess each system's capability to deliver decision advantage.

The research supported that NTAS is an effective system that provides a sufficient decision advantage capability. However, the system requires further improvements. These improvements involve: formally establishing a DHS Office of Counterterrorism Coordination; renewing the DHS Counterterrorism Advisory Board Charter or other appropriate governance documents to ensure sustainment of necessary decision making and execution authority for NTAS; refine the NTAS *Concept of Operations* to better demonstrate the system's scalable outcomes other than an NTAS-generated alert, such as Joint Intelligence Bulletins, Joint Threat Assessments, etc.; conduct NTAS-related outreach and education efforts with the homeland security enterprise and the public; and improve communication aspects of NTAS integrating with other warning systems, such as the Integrated Public Alert and Warning System. These improvements are critical in sustaining the current effectiveness of the system and in ensuring its future success.

[1] Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 175–184; Clayton M. Christensen, *The Innovator's Dilemma: The Revolutionary Book that Will Change the Way You do Business* (New York: Harper Business, 2011), 185–197.

ACKNOWLEDGMENTS

Completing this Naval Postgraduate School master's program represents the academic capstone of my career. Authoring this thesis underscored for me the importance of those people in my life, without whom, I would not be successful in any of my professional or personal endeavors. Therefore, I extend heartfelt and sincere thanks to my family, professional colleagues, my NPS classmates, as well as the NPS faculty and staff. Your support and assistance throughout the last 18 months of this program was indispensable to me.

Although many people played some part in the finishing of this thesis, my family's unwavering support at every step throughout this journey sustained me and propelled me toward the great achievement I hope this thesis represents. It is not that the pages that follow reflect some great American literary opus. However, these pages do represent many hours spent absent from the loved ones I am acknowledging here. With that in mind, I say thank you to my loving wife and children, because without their willing sacrifice of time with husband and father, none of what follows would have been possible.

To my professional colleagues, classmates, and the NPS faculty and staff, thank you for your sage advice, support, and for toiling beside me in the rigorous challenge this program represents. I particularly want to thank Professors Erik Dahl and Carolyn Halladay for their patient and steadfast guidance throughout this thesis development process. I consider completing this program one of my greatest career achievements, an achievement that would not have been possible without the help of this distinguished group.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Throughout its history the United States devised various warning systems designed to provide people with sufficient warning to mitigate harm from hazards. Warning systems assist in protecting people from the harm posed by many hazards, such as fires, floods, blizzards, hurricanes, or attacks from other people; however, systems do not completely mitigate the dangerous effects from such hazards. For example, they do not artificially shield people from harm. Instead, through their warnings, these systems provide a "decision advantage," allowing appropriate choices in advance of danger.

The term "decision advantage" is commonly utilized within the United States Intelligence Community (IC) to describe the desired outcome of the intelligence process. Intelligence experts Jennifer Sims and Burton Gerber define the concept:

> [Intelligence] officials do not value information according to the difficulty with which it was acquired, but according to its relevance and timeliness to the decision at hand. Their purpose is to gain "decision advantages" for political leaders, diplomats, military commanders, and other U.S. government officials in order to secure the country's interests in both peace and war.[1]

In a broader homeland security context, warning systems provide decision advantages to a large and diverse group of decision makers, from senior public officials to individual citizens.

This thesis explores the usage of a terrorism warning system and the benefits of a system such as the current United States system the National Terrorism Alert System (NTAS). As the current NTAS coordinator, my hope is to provide the homeland security enterprise (HSE) partners and the American public with an opportunity to understand why and how NTAS functions as a key counterterrorism (CT) capability.[2]

---

[1] Jennifer E. Sims and Burton L. Gerber, *Transforming US Intelligence* (Washington, DC: Georgetown University Press, 2005), 16.

[2] The author works in the DHS Office of the Counterterrorism Coordinator, as the National Terrorism Advisory System Coordinator. This office coordinates CT functions for the department and supports the DHS CT Coordinator in advising the DHS Secretary on CT issues and incidents.

The evaluation of the sufficiency of terrorism warning systems in providing effective warning and decision advantage presents a problem for every decision maker. In the HSE, this is the collection of decision makers or groups from the individual citizen up to the most senior policy maker.[3] This problem manifests differently based upon the decision maker's context. For example, a senior policy maker may evaluate a system's effectiveness in order to determine if the system remains viable or needs revision. Alternatively, an individual citizen may evaluate effectiveness from a perspective of trust or confidence; in other words, would the citizen take action based on a warning from that system?

From the popular perspective, the NTAS may suffer from a lack of public confidence like its color-coded predecessor, the Homeland Security Advisory System (HSAS), but for a diametrically different reason.[4] The HSAS suffered overexposure and poor utilization, which diminished its public confidence level and its effectiveness as a decision advantage tool.[5] On the other hand, NTAS has never been publically utilized and no warnings have been disseminated outside government circles. This means it does not have a track record of reliability and broad understanding in the public purview. This situation creates a potential credibility gap—just when the public will most need the decision advantage this type of system purportedly provides. Therefore, a fresh look is warranted to determine the value of NTAS. A conceptual measurement framework assessing the NTAS capability to provide decision advantage and warning provides the basis for making an effective evaluation.

---

[3] According to DHS, "The QHSR identifies the importance of what we refer to as the homeland security enterprise—that is, the Federal, State, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population." Department of Homeland Security, *Quadrennial Homeland Security Review* (Washington, DC: U.S. Department of Homeland Security, 2010), iii.

[4] NTAS is supposed to sustain the public trust and confidence, "A system in which the American public can have confidence…." Executive Office of the President, *Presidential Policy Directive/PPD-7* (Washington, DC: The White House, 2011). 1.

[5] This body was tasked by DHS Secretary Napolitano to evaluate the effectiveness of HSAS and provide recommendations for improving the nation's advisory system capability. Homeland Security Advisory Council, *Homeland Security Advisory System Task Force Report and Recommendations* (Washington, DC: U.S. Department of Homeland Security, 2009).

B. RESEARCH QUESTION

The primary research question for this thesis is: How effective is the NTAS when compared to its predecessor the HSAS? A secondary research question is: Does NTAS provide sufficient decision advantage for the nation it serves?

C. SIGNIFICANCE OF RESEARCH

Since its inception in April 2011, NTAS has not released a public alert or received any substantial public mention for its role in supporting CT efforts. But despite the lack of publicly visible output from NTAS or any publicity for its role in the supporting broader CT efforts, it is a system that has been frequently used within the Department of Homeland Security (DHS) due to its ability to provide effective warning and decision advantage.[6]

This potential public confidence gap generates the need for more research in order to better determine and ensure the effectiveness of NTAS. The diminished public awareness of NTAS usage stems from the fact that NTAS more often supports internal government CT decision making and information sharing. This type of internal NTAS support produces a plethora of other derivate decision support products or warnings, such as Joint Intelligence Bulletins (JIBs), etc. that are not inherently designed for public consumption like an NTAS generated public alert.[7]

Therefore, a different research approach from previous research that assessed NTAS is needed to answer the primary and secondary research questions.[8] This research

---

[6] Press statements from former DHS Secretary Janet Napolitano and congressional testimony from former DHS Counterterrorism Coordinator Rand Beers reflect this level of usage during timeframes of increased vigilance, such as the 2011 Bin Laden Raid timeframe or more recently, during domestic incidents, such as the 2013 Boston Marathon Bombing.

[7] According to Interagency Threat Assessment and Coordination Group, "The JIB provides timely information or analysis on a recent or current event or development of interest to all information and analysis customers and is produced at various classification levels. They deal with counterterrorism, homeland security, and WMD-related information. It focuses on Homeland Security issues, is written on an ad hoc basis, and is generally one to three pages. It is available to members of the HSE depending on the classification of the information." Interagency Threat Assessment and Coordination Group, *Intelligence Guide for First Responders*, 2nd ed. (Washington, DC: Interagency Threat Assessment and Coordination Group, 2011), 29.

[8] Vincent H. Sharp, "Faded Colors: From the Homeland Security Advisory System (HSAS) to the National Terrorism Advisory System (NTAS)" (master's thesis, Naval Postgraduate School), 1.

approach defines the tenets of an effective terrorism warning system and nuances of the terrorism threat such a system addresses. It also discusses the characteristics of two different threat types, deliberate and non-deliberate. This research presents a threat assessment methodology and the role of threat assessment in supporting CT efforts. It discusses the decision maker's dilemma, which arises when considering the use of a terrorism warning system. This discussion provides perspective for why such as system can remain invisible to the nation it serves.

This research serves to examine and present an improved understanding for the mechanics of a terrorism warning system. This is achieved through the validation or invalidation of the hypothesis that the NTAS provides an improved system in support of CT decision making, coordination and communication.[9]

D. METHOD

This body of research provides an operating definition of two different threat types, deliberate and non-deliberate respectively. It discusses the dilemma any decision maker faces in situations prompting the use of a terrorism warning system. It presents the debate about the efficacy of terrorism warning systems in the context of broader U.S. government (USG) CT approaches. It also contextually supplies the tenets of an effective warning system with a comparison between the United States hurricane warning system and the current terrorism warning system NTAS.

The HSAS and NTAS represent the two United States terrorism warning systems. Each of these systems supplies a case study for a structured focused comparison designed to answer the primary and secondary research questions. Each system is assessed through a panel of questions within each system's respective case study chapter. In the analysis chapter, these systems are compared and contrasted with one another using these questions. For additional evaluation, each system is analyzed with at least one other

[9] The NTAS replaced the color-coded Homeland Security Advisory System (HSAS). This new system "effectively communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector." Department of Homeland Security, *NTAS Public Guide*, April 2011, http://www.dhs.gov/ntas-public-guide

theory. Based on the outcomes of this analysis, the conclusion chapter presents findings and recommendations as well as other potential considerations related to NTAS or the broader topic of warnings systems in general.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

There is paucity of literature specifically addressing NTAS or its effectiveness. Although there is not a large amount of NTAS specific research, reviewing the broader body of homeland security literature related to other warning systems supplies a basic understanding for how warning systems fulfill their role in homeland security. What follows is a summary of this review. It includes a discussion of deliberate and non-deliberate threat types, the decision maker's dilemma when considering the use of a terrorism warning system and a presentation of important elements of the warning systems. After discussing these topics, a synopsis of the professional discourse amongst detractors and supporters of terrorism warning systems follows as well as the presentation of a potential alternative approach for the current terrorism warning system, NTAS.

The U.S. hurricane warning system (HWS) is included in this literature review for contrast and comparison with the two terrorism warning systems. This comparison provides important context from the perspective of a more publically well-known and reliable warning system because as Congressman Chris Shays pointed out:

> When a blizzard or hurricane is forecasted, the public is not advised to be brave for America and stay in the eye of the storm, but when the threat of terrorism is elevated, citizens are advised to go about their lives as if no real peril approached. We need to make terrorism alerts at least as targeted and accurate as storm projections.[10]

A. THREAT TYPES—DELIBERATE AND NON-DELIBERATE

Presenting these two threat types, non-deliberate and deliberate, supports of the discussion of terrorism warnings more thoroughly later in this literature review. According to Dr. David Alderson, "non-deliberate risk is akin to 'mother-nature' or a random occurrence of threat, such as hurricanes, earthquakes, floods, etc. Deliberate

[10] *Homeland Security Advisory System: Threat Codes and Public Responses: Before the House of Representatives, Subcommittee on National Security, Emerging Threats and International Relations, Committee on Government Reform*, 108th Cong., 2 (2004) (statement of General Patrick Hughes, Assistant Secretary for Information Analysis).

threats are generated from an 'enemy.'"[11] The important distinction is between naturally occurring (non-deliberate) versus human generated (deliberate) threats. Deliberate human threats are more dynamic due to the human attacker's capability to think and counter move against defensive efforts, such as terrorism warnings. This distinction of threat types is a fundamental frame of reference in properly understanding the consistent reasons for outcomes derived from different types of warning systems. The threat a warning system addresses is directly related to the demonstrated outcomes of that system.

A non-deliberate threat, such as a hurricane, is a more obvious type of danger than that of terrorism. This is due to the reality that a hurricane is a force of nature and is not a thinking enemy. It is not attempting to gain the element of surprise with stealthy tactics. A hurricane does not maintain a sense of purpose in its actions. It does not seek to enact political change through acts of violence. It forms and travels wherever the winds and seas take it. It does not knowingly change its course in purposeful attempt to deceive or sow confusion amongst forecasters and first responders in order to achieve a more horrific impact on the communities it affects.

However, a hurricane is similar to an act of terrorism in two factors: it does instill fear in a community and can devastate that community with its violence. The threat assessment process for a non-deliberate threat type is much more predictable and rote. The severe weather and warning system expert, Mike Smith provides this simple bulleted list regarding hurricane warning and mitigation process phases:

- The forecast,
- Action taken to protect life (evacuation) and property (boarding-up), and
- The post-storm aftermath and recovery.[12]

Smith further details the steps the HWS follows in providing warnings:

> The first step in making a forecast is to locate any hurricanes or tropical storms already in existence. The second step is to forecast their future path. The third is to forecast their changes in intensity. Once the changes

[11] David Alderson, "Risk and Critical Infrastructure Systems: Practice and Pitfalls" (presentation, Naval Postgraduate School, Monterey, CA, October 2013).

[12] Mike Smith, *Warnings: The True Story of how Science Tamed the Weather*, 1st ed. (Austin, TX: Greenleaf Book Group Press, 2010), 205.

> in intensity (which meteorologists define in terms of atmospheric pressure and wind speed) are complete, other vital forecasts such as rainfall amounts and storm surge can be made. Then, the final forecast is communicated to the NWS field offices and local emergency management officials so evacuations and other preparatory actions can begin.[13]

In summary, predictability is the central difference between a non-deliberate threat type, like a hurricane, and a deliberate threat type, such as terrorism. Hurricanes present a more persistently obvious danger to the public and do not create a decision-making dilemma for an official charged with warning anyone about this type of danger. There is no doubt about the need to warn anyone in the path of a hurricane.

This is not necessarily the case with the dangers terrorism presents the decision-making official. The deliberate threat type of terrorism is difficult to discern and predict. Framing the concept of threat and how to assess the threat posed from a deliberate thinking adversary is important context. David Strachan-Morris examines this issue presents a framework for defining and assessing a deliberate type of threat. His efforts draw from amongst the combined military and homeland security doctrine of major Western nations, such as the United Kingdom, the United States, Australia, etc.[14] His analysis assists in defining threat and its subordinate elements in order to frame the discourse of whether the terrorism threat is exaggerated or not.

Strachan-Morris supplies a methodology for evaluating the deliberate threat type. According to Strachan-Morris, "Simply put, threat is a function of capability and intent."[15] If an adversary maintains both the capability and intent to cause harm they are a threat. Depending on the assessment of the adversary's capability and intent we can gauge the level of threat that adversary poses. In addition, Strachan-Morris also points out, "Intent can be broken down into two further components, will and opportunity."[16] Evaluating the adversary's previous attacks and public statements together produces an

---

[13] Ibid.

[14] David Strachan-Morris, "Threat and Risk: What is the Difference and Why does it Matter?" *Intelligence and National Security* 27, no. 2 (2012): 174.

[15] Ibid.

[16] Ibid., 175.

assessment of the adversary's will to attack. Determining the opportunity variable for an adversary represents assessing the "level of opportunity available to an organization" to conduct an attack.[17] For example, "an organization that can attack whenever and wherever it wants has a high level of opportunity."[18] Therefore, threat assessment is a function of an adversary's level of capability and its intent to cause harm. If an adversary maintains sufficient capability and intent (will and opportunity), then that adversary poses a threat. Intelligence and CT professionals utilize threat assessment as the basis and substance for providing warning. If the threat assessment and warning are timely and effective, they provide decision advantage to senior officials or other decision makers. This decision advantage can lead to successful actions mitigating the adversary's threat.

The deliberate threat problem set a terrorism warning system addresses boasts additional complexities that are not existent in other non-deliberate threat problem sets faced by the HWS. The terrorism warning system must carefully balance the need to warn communities to potential danger against the need for operations security (OPSEC) inherent to CT efforts attempting to keep those same communities safe. Balancing the need to warn and the need for OPSEC is the crux of the CT decision maker's dilemma.

B. DECISION MAKER'S DILEMMA

The terrorism warning system decision maker faces a two-fold dilemma. A decision maker must avoid creating undue fear, anxiety, and/or confusion amongst those receiving a terrorism warning. The decision maker must also ensure OPSEC for ongoing CT efforts. In 2007, the United States Army released a new regulation defining OPSEC:

> OPSEC is not traditional security, such as information security like marking, handling and classifying information; it's not the physical security of actually protecting classified information though they're all related and part of OPSEC. OPSEC is different from traditional security in that we want to eliminate, reduce and conceal indicators, unclassified and

[17] Ibid.

[18] Ibid.

> open-source observations of friendly activity that can give away critical information.[19]

This perspective provides the working definition of OPSEC for this research effort.

The complete absence of an OPSEC consideration is one major difference between the HWS and any terrorism warning system. Without this OPSEC consideration, there is no dilemma. The warning deliberation is reduced to a simple discussion of when and how to warn people most effectively. It is not encumbered with a deliberation of "if" a warning is appropriate and whether that warning degrades efforts to stop the threat. Human operations cannot stop the forces a hurricane; however, human operations can stop the human threat of a terrorist attack. Therefore, an OPSEC deliberation is a major differentiation between a non-deliberate threat decision to warn and a deliberate threat decision to warn.

In addition to OPSEC considerations, terrorism warnings should not create undue fear or panic for the public. Psychological fatigue could result from undue fear or panic. This fatigue can degrade the benefits of a terrorism warning about the threat, such as a heightened level of public vigilance. Poorly utilized terrorism warnings can also desensitize the public to the danger posed from the terrorist threat. Rose McDermott and Philip Zimbardo reflect this phenomenon in the story of the boy who cried wolf:

> We all know from the classic story of the boy who cried wolf, after only three false alarms, people cease to take seriously the validity of previously credible messages. Indeed, they come to dismiss such warnings fairly quickly over time because they prove to be inaccurate; when warning comes without anything happening afterward, people lose faith in the alert system itself.[20]

It is important to avoid raising unnecessary public distress, which achieves the same affect the terrorists are striving for: instill fear. This is the additional negative outcome McDermott and Zimbardo note with this comment, "Mismanaged alarm procedures do the terrorists work for them." As McDermott and Zimbardo point out,

---

[19] J. D. Leopold, "Army Releases New OPSEC Regulation," U.S. Army, April 19, 2007, accessed September 4, 2014, http://www.army mil/article/2758/army-releases-new-opsec-regulation/

[20] Bruce Bongar et al., eds, *Psychology of Terrorism* (New York: Oxford University Press, 2007), 360.

avoiding these negative impacts requires an effectively managed decision-making process. Additionally, a designated body or group of decision makers increases the sustainability and consistency in this decision making process.

To address both aspects of this decision-making dilemma, a well-managed and deliberate process is needed. For sustainability and consistency in this decision-making process, a designated body or group of decision-makers is advisable.

C. TENETS OF WARNING SYSTEMS

As noted, warning systems provide an opportunity for people to avoid danger. What follows is a presentation of the important elements each system requires to effectively accomplish its purpose. For contrast and comparison reasons, the HWS is reflected first in this review, with the terrorism warning system following immediately afterward.

1. Tenets of a Hurricane Warning System

The essential tenets of a HWS are very similar to a warning system focused upon terrorism, tenets that are covered later in the Tenets of a Successful Terrorism Warning System section in this literature review. These HWS tenets provide context for comparison with the terrorism warning system. The HWS is "an interdepartmental effort to provide the United States and designated international recipients with forecasts, warnings, and assessments concerning tropical and subtropical weather systems."[21] The purpose of the system is: "Tropical Cyclone Forecast/Advisories [hurricane warning system]…provides critical tropical cyclone watch, warning, and forecast information for the protection of life and property."[22] The HWS tenets are more defined and specific because it is more scientific and established due to the frequency of its use over the course of the last 100 years. Additionally, this system is maturely established amongst the

[21] Participating organizations, such as the National Oceanic and Atmospheric Administration (NOAA) of the Department of Commerce; the United States Navy of the Department of Defense; and the National Aeronautics and Space Administration. Department of Commerce, Office of the Federal Coordinator for Meteorological Services and Supporting Research, *National Hurricane Operations Plan* (FCM-P12-2013) (Washington, DC: U.S. Department of Commerce, 2013), 1-1.

[22] Ibid., 3-2.

interdepartmental partners that operate the HWS. This maturity is reflected in the operations plan governing and synchronizing the partners, "The National Hurricane Operations Plan [that] provides the basis for implementing agreements…defines the roles of individual agencies, participating in the tropical cyclone forecasting and warning program [hurricane warning system]…."[23]

Below are important tenets that the HWS employs to effectively warn and provide decision advantage to those under hurricane threat:

1. The HWS must provide timely weather forecasts through the Tropical Cyclone Discussion product. This product "provides coordinated 12-, 24-, 36-, 48-, 72-, 96-, and 120-hour tropical cyclone forecast positions and maximum sustained wind speed forecasts; other meteorological decisions; and plans for watches and warnings."[24]
2. The system must provide watches and warnings of possible hurricane conditions within 48 hours and expected hurricane conditions within 36 hours.
3. The system must provide updates of any significant changes to the conditions of the situation in between regularly scheduled public advisories, such as "…the time and location of [hurricane] landfall, or to announce an expected change in [hurricane] intensity that results in an upgrade or downgrade of status, [etc.]."[25]

These HWS tenets are similar to the tenets of the terrorism warning system. In contrast, the HWS is very defined and predictable because it addresses a defined and predictable non-deliberate or non-thinking threat. In other words, a hurricane does not deliberately change its course or its make-up (wind speed, size, etc.) in order to counter the hurricane forecaster's storm predictions or the first responder's preparations for storm impacts.

2. Tenets of a Successful Terrorism Warning System

Establishing the essential tenets of a terrorism warning system is important in order to assess the efficiency or effectiveness of NTAS. These tenets are more an art form than a well-practiced science represented in the HWS tenets. This generates the need for a composite sketch of terrorism warning system tenets drawn from terrorism experts,

[23] Ibid., 1-1.

[24] Ibid., 3-2.

[25] Ibid., 3-2.

government officials and other respected sources from among the relevant discourse community. This composite sketch includes a central task in addition to the tenets of a terrorism warning system.

a. The Central Task

Beginning the discussion of the terrorism warning system's purpose or central task, Jacob Shapiro and Dara Kay Cohen state, "An effective terrorism alert system has one central task: to motivate actors to take costly protective measures."[26] Shapiro and Cohen further offer how such a system accomplishes this central task, "the government can share specific information to motivate protective action, or it can generate enough confidence in the alert system that its word alone sufficiently increases actors' beliefs about the probability of an attack that they willingly take the desired actions."[27] Moreover, Dr. James Breckenridge underpins the importance of confidence as a matter of trust: "Trust is the essential component to the success of any…system. Perfect messaging, color codes, or adjective threat advisories will not be effective without the public's confidence in the system and those delivering the message."[28] Furthermore, in congressional testimony, DHS Principal Deputy Assistant Secretary for Public Affairs, Robert Jensen articulated confidence and trust as a DHS priority, "During an incident… [one of] our communications priorities [is]…. Employment of risk communications and transparency to gain and maintain public confidence and trust…."[29] Based upon this, it is apparent that confidence in the warning system is a key feature in accomplishing the system's central task of motivating individuals to take action in safeguarding themselves.

---

[26] Jacob N. Shapiro and Dara Kay Cohen, "Color Bind: Lessons from the Failed Homeland Security Advisory System," *International Security* 32, no. 2 (2007): 121.

[27] Ibid.

[28] Homeland Security Advisory Council, *Stakeholder Feedback Report* (Washington, DC: U.S. Department of Homeland Security, 2009).

[29] *Why Can't DHS (Homeland Security Department) Better Communicate with the American People?: Before the U.S. House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency*, 113th Cong., 6 (2013) (statement of Mr. Robert Jensen, Principal Deputy Assistant Secretary, Office of Public Affairs, U.S. Department of Homeland Security).

b. Important Tenets of a Terrorism Warning System

What follows is a list of the important tenets of a terrorism warning system. These tenets are distilled from the myriad of views within the discourse community regarding terrorism warning systems. They generally describe the critical elements of a warning system in accomplishing its central task and importantly, in engendering or maintaining confidence and trust in the system.[30]

1. A terrorism warning system should provide timely detailed information regarding the threat.
2. A terrorism warning system should provide clear and understandable protective actions or other mitigation measures.
3. A terrorism warning system should provide a clear duration for the period of threat.
4. A terrorism warning system should be agile in its ability to raise or lower the threat level in keeping with the conditions of the threat situation.
5. A terrorism warning system should provide effective decision advantage to the people receiving the information.

These terrorism warning system tenets are similar to the tenets of the HWS. The contrast from the HWS resides in applying these terrorism warning system tenets to the thinking human threat. Therefore, a terrorism warning system is more of an art than a science, because a terrorist does deliberately change attack plans, such as tactics, techniques and procedures in order to counter the intelligence analyst's threat warnings or the CT professional's preparations to prevent the attack or mitigate its impacts. The terrorism warning system is defined and predictable to a degree; however, it must remain flexible in addressing a more vague and deliberate or thinking threat.

---

[30] Ibid; James J. Carafano and Jessica Zuckerman, "The Current Threat Level: Ending Color-Coded Terror Alerts," Memo #3068, November 30, 2010, The Heritage Foundation, accessed March 15, 2014, http://www.heritage.org/research/reports/2010/11/the-current-threat-level-ending-color-coded-terror-alerts?ac=1; William O. Jenkins, *Homeland Security Advisory System: Preliminary Observations Regarding Threat Level Increases from Yellow to Orange* (Washington, DC: General Accounting Office, 2004); Sharp, "Faded Colors;" Homeland Security Advisory Council, *Homeland Security Advisory System*; Homeland Security Advisory Council, *HSAS Survey Report* (Washington, DC: U.S. Department of Homeland Security, 2009); Executive Office of the President, *Presidential Policy Directive/PPD-7*; *House of Representatives. Committee on Government Reform. Subcommittee on National Security, Emerging Threats, and International Relations, Homeland Security Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System*, 108th Cong. (2004) (testimony Randall Yim), http://www.gao.gov/assets/120/110679 html

3. Terrorism Warning System Detractors

Three general elements comprise the detractors' argument against the need for a terrorism warning system. The first element is that the terrorism threat is exaggerated or poorly represented to the average citizen. This frequency related argument represents the central building block of the detractors' case. The second element is that heightened vigilance from terrorism warnings is overrated. The third element of the argument deems terrorism warnings as a driver of unnecessary economic burden.

a. The Exaggerated Terrorism Threat—The Main Opposing Argument

The exaggerated terrorism threat is the detractors' main argument. Varied opinions exist concerning the value of terrorism warnings and the need for the USG level of effort put in to countering terrorism in general. Many government officials and terrorism experts argue that the terrorist threat to American citizens remains significant. But some experts, such as John Mueller and Mark Stewart, argue the threat is exaggerated and not as dire as some expert opinions assert: "the exaggerations of the threat presented by terrorism [result in] the distortions of perspective these exaggerations have inspired."[31]

Using 9/11 as a common frame of reference, most detractors focus on the radicalized Islamist variety of terrorist. The detractors' main argument rests on the low occurrence of successful terrorist attacks in the United States since September 11, 2001. This is also the strongest and most easily understood argument detractors employ. For example, Shikha Dalmia provides a profile of a successful would-be terrorist operating in the United States:

> [R]adicalized enough to die for their cause; Westernized enough to move around without raising red flags; ingenious enough to exploit loopholes in

[31] Mueller and Stewart represent the halyards of dissenting opinion regarding the real level of terrorism threat and in proposing alternatively appropriate levels of effort for homeland security efforts in general. They are cited often in this thesis, because they have conducted exhaustive analysis toward determining the real level of threat from terrorism. Subsequently, their articles and books present a comprehensive compendium of evidence collected from the discourse community of dissenting opinions about the level of threat the United States faces from terrorism. John Mueller and Mark G. Stewart, "The Terrorism Delusion: America's Overwrought Response to September 11," *International Security* 37, no. 1 (2012): 83.

> the security apparatus; meticulous enough to attend to the myriad logistical details that could torpedo the operation; self-sufficient enough to make all the preparations without enlisting outsiders who might give them away; disciplined enough to maintain complete secrecy; and—above all—psychologically tough enough to keep functioning at a high level without cracking in the face of their own impending death.[32]

Based on this daunting profile of a terrorist recruit Dalmia presents, it is not surprising that detractors believe the terrorist threat overblown. Finding a recruit meeting these requirements would be very difficult, which makes the argument seem reasonable.

Reinforcing this frequency argument, Mueller and Stewart point out, "In all, extremist Islamist terrorism—whether associated with al-Qaida or not—has claimed 200 to 400 lives yearly worldwide outside of war zones. That is 200 to 400 too many, of course, but it is about the same number as bathtub drowning every year in the United States."[33]

Testing the detractors' frequency-based argument with Strachan-Morris's threat methodology, Islamist terrorist adversaries rate very high in the will aspect of intent. This is due to their rhetoric and track record of attacks or attempted attacks. Although high in the will component, these terrorists seem low in the opportunity component. They appear at least moderately capable. However, they are restricted in opportunity due to their arsenal of conventional weapons, such as mortars, small arms, etc. as well as in their tactics, such as complex small arms attacks and suicide vest equipped bombers. Additionally, these terrorists are not located in close geographic proximity to the United States and do not appear to possess the capability to overcome this challenge of distance. This cursory threat assessment is supported by Mueller and Stewart, "…Islamist militants…are operationally unsophisticated, short on know-how, prone to making mistakes, poor at planning, and limited in their capacity to learn."[34] This assessment

---

[32] Shikha Dalmia, "What Islamist Terrorist Threat? Al Qaeda Doesn't Have What it Takes to Hurt America," February 15, 2011, accessed July 4, 2014, http://reason.com/archives/2011/02/15/what-islamist-terrorist-threat

[33] Mueller and Stewart, "The Terrorism Delusion."

[34] Ibid., 89.

seems to support the detractors' argument for an acknowledgement that the terrorism threat is lower than many would accept as true.

The detractors' frequency argument also cites the lack of positively identified terrorists or terrorist plots discovered from CT efforts as proof the terrorism threat is overstated. Mueller and Stewart submit, "Although the thousands of al-Qaida operatives once thought to be flourishing in the United States were never found, there have been efforts to make that delusion more fully fit reality."[35] The detractors' posit this continued overstatement of the terrorism threat then perpetuates a widespread delusion similar to the "Red Scare" phenomenon and the infamous McCarthy Trials of the 1950s.[36] In this sense, detractors are questioning the motives of government officials and other supporters who present the terrorism threat as an imminent danger to the public. Therefore, detractors portend that supporters are utilizing a false argument about the dire threat from terrorism in order to justify their continued efforts and expenditures of resources.

b. Overrated Benefit of Heightened Public Vigilance—A Supporting Argument

Detractors present that there is little real benefit from raising threat awareness amongst the public. Benjamin Friedman asks and answers, "Does exhorting the public to be vigilant add a layer of defense against terrorism that justifies the anxiety and false leads it causes? I…argue that the answer to all these questions is no…vigilance is overrated."[37] In a sense, Paul Pillar concurs with Friedman and bemoans, "The

---

[35] Ibid.

[36] According to History.com, "As the Cold War between the Soviet Union and the United States intensified in the late 1940s and early 1950s, hysteria over the perceived threat posed by Communists in the U.S. became known as the Red Scare. (Communists were often referred to as 'Reds' for their allegiance to the red Soviet flag.) The Red Scare led to a range of actions that had a profound and enduring effect on U.S. government and society. Federal employees were analyzed to determine whether they were sufficiently loyal to the government, and the House Un-American Activities Committee, as well as U.S. Senator Joseph R. McCarthy, investigated allegations of subversive elements in the government and the Hollywood film industry." "Red Scare," accessed July 7, 2014, http://www history.com/topics/cold-war/red-scare

[37] Benjamin H. Friedman, "Do Terrorism Warnings Work?" *The National Interest* [blog], October 13, 2010, accessed April 5, 2014, http://nationalinterest.org/blog/the-skeptics/do-terrorism-warnings-work-4214

uselessness to the public of…vague official alerts about possible terrorist attacks in Europe…."[38] Pillar further states:

> Our government [United States] told us not that we should revise our travel plans but that we should take sensible precautions such as being aware of our surroundings. Sounds like standard advice for any foreign traveler, terrorist threat or no terrorist threat. The public consequently is as bemused as it was by those stoplight charts about levels of terrorist threat for which the former homeland security czar Tom Ridge was criticized when he introduced them.[39]

There are some grounds for belief that the public is conditioned to ignore terrorism warnings as the HSAC Task Force concluded, "The Task Force members agreed that, at its best, there is currently indifference to the Homeland Security Advisory System and, at worst, there is a disturbing lack of public confidence in the system."[40] These points encapsulate this aspect of the detractor argument that the purported value of increase public vigilance is overrated in countering acts of terrorism.

c. Unspecific Warnings Drive Unneeded Costs—Another Supporting Argument

Another aspect of the detractor argument emphasizes the unnecessary costs from terrorism warnings as a reason for doing away with terrorism warnings. At a minimum, detractors desire to improve terrorism warnings in order to improve the effectiveness and efficiencies of actions taken by those responding to them. The detractors point out that a terrorism warning system suffers this foible: unspecific terrorism warnings drive unneeded costs. In making this supporting argument, detractors hope to diminish warning related costs that do not productively assist warning recipients in their response efforts to any threat.

---

[38] Paul R. Pillar, "What Terrorism Alerts Say about Ourselves," *The National Interest* [blog], October 7, 2010, http://nationalinterest.org/node/4193

[39] These comments are in response to the September 2010 Department of State travel alert regarding a threat from terrorism for citizens travelling to or within Europe. Paul R. Pillar, "What Terrorism Alerts Say about Ourselves."

[40] Homeland Security Advisory Council, *Homeland Security Advisory System*, 1.

If the frequency argument is accepted as valid in determining the risk posed from terrorism, Howard Kunreuther is correct in asking, "How much should we be willing to pay for a small reduction in probabilities that are already extremely low?"[41] According to Mueller and Stewart, "Since September 11, expenditures in the United States on domestic homeland security alone…have expanded by more than $1 trillion."[42] Under the old HSAS, Dana Priest and William Arkin note, Americans received "a steady diet of vague and terrifying information from national security officials" and have "shelled out hundreds of billions of dollars to turn the machine of government over to defeating terrorism without ever really questioning what they are getting for their money."[43]

Detractors point out that costs related to terrorism warnings are expensive. One estimate placed the cost of alerting the public under the HSAS at approximately $1 billion per week each time the alert level was raised to orange.[44] According to DHS, this type of alert level change occurred eight times, lasting approximately 31 total weeks, between 2002 and 2011.[45] If the $1 billion per week cost is valid, this totals a cost of $31 billion due to alerting alone. According to Priest and Arkin, "Factoring in the additional costs incurred by state and local governments—and the potential economic losses from reductions in consumer confidence, travel, and tourism—only makes the cost of this imperfect system [HSAS] more exorbitant."[46] In the following statement from Carafano and Zuckerman effectively concludes this aspect of the detractor argument, "Without specific information as to the nature of the threat, states and localities are forced to decide between piling on expensive (and potentially unnecessary) layers of security and doing nothing at all."[47]

---

[41] Howard C. Kunreuther, "Risk Analysis and Risk Management in an Uncertain World," *Risk Analysis* 22, no. 4 (2002): 662–663.

[42] John E. Mueller and Mark G. Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (New York: Oxford University Press, Inc., 2011), 1–3.

[43] Dana Priest and William M. Arkin, *Top Secret America: The Rise of the New American Security State* (New York: Little, Brown and Co., 2011), xviii–xix, 103.

[44] Carafano and Zuckerman, "The Current Threat Level: Ending Color-Coded Terror Alerts."

[45] Department of Homeland Security, "Chronology of Changes to the Homeland Security Advisory System," accessed July 29, 2014, http://www.dhs.gov/homeland-security-advisory-system

[46] Carafano and Zuckerman, "The Current Threat Level: Ending Color-Coded Terror Alerts."

[47] Ibid.

4. Terrorism Warning System Supporters

Conversely, supporters of robust CT efforts, such as terrorism warning systems, posit three general arguments that correspond or counter the arguments of the detractor community. The thrust of these arguments is that the United States should maintain a prudent acknowledgement of the terrorism threat, heightened vigilance is beneficial, and increased security outweighs the increased security costs.

a. Prudent Acknowledgement of Terrorism Threat

Acknowledgement of the threat of terrorism to the United States and its citizens is prudent. As counterinsurgency/counterterrorism expert James D. Kiras suggests, "The most important phase of any counterinsurgency or counterterrorism campaign is recognizing that the threat exists."[48] Terrorism expert Seth Jones of the RAND Corporation presents stark findings concerning the sustained and potentially growing threat of terrorism to the United States. In a 2014 report, Jones' research denotes a 58 percent increase in the number of Salafi-Jihadist terrorist groups since 2010, which comprises a combined force numbering between 40,000 to upwards of 100,000.[49] Although these groups are geographically distant to the United States, located in the Middle East and North Africa, they desire to attack Western nations in Europe as well as in North America. Using David Strachan-Morris's threat assessment method, these groups demonstrate significant intent and capability. Among these Salafi-Jihadi groups Jones cites is the Islamic State of Iraq and Syria (ISIS).[50] ISIS demonstrates a resolute will toward violence and a capability to create attack opportunities, which makes ISIS and groups like them, acutely more deadly. Therefore, ISIS and other kindred groups, represent a real threat for conducting terrorist attacks against their enemies, such as the United States, the United Kingdom, etc.

---

[48] John Baylis, James J. Wirtz, and Colin S. Gray, *Strategy in the Contemporary World: An Introduction to Strategic Studies*, 4th ed. (Oxford, United Kingdom: Oxford University Press, 2013), 184.

[49] Seth G. Jones, *A Persistent Threat: The Evolution of Al Qaida and Other Salafi-Jihadists* (Santa Monica, CA: RAND Corporation, 2014), 26–28.

[50] Ibid., 3.

Clearly detractors such as Mueller and Stewart, make their case essentially utilizing the low frequency of terrorism as a bulwark for their argument. It seems reasonable to consider if something should be treated as a great threat, if it does not occur very often. Mueller and Stewart cite David Banks to assist people in prudently drawing "the distinction between realistic reactions to plausible threats and hyperbolic overreaction to improbable contingencies."[51] Yet, this frequency argument advances a tenuous premise: people should be willing to adjust their security prioritization levels based upon mere chance that a terrorist attack will not happen to them or at least, affect them in some manner. In 2013 congressional testimony, noted terrorism expert Bruce Hoffman articulates the hazard of this tenuous premise,

> Finally, the continued absence of a successful, major al Qaeda attack in North America since 2001 may induce a period of quiet and calm that lulls us into a state of false complacency, lowering our guard and, in turn, provoking al Qaeda or one of its allies to chance a dramatically spectacular attack in the U.S.[52]

In keeping with the lull Professor Hoffman identifies, the 2013 Boston Marathon bombing directly contradicts the detractors' frequency argument because "…the Boston Marathon bombings serve as a reminder that threats from terrorism persist and continue to evolve."[53] Furthermore, a 2013 Pew Research Poll reflected that since the attacks of 9/11, the public has consistently remained at least somewhat concerned about terrorism.[54] This level of concern never dipped below 58 percent of the population over the 12 year period between 2001 and 2013.[55] David Lauter expressed the American citizen's support

---

[51] Mueller and Stewart, *Terror, Security, and Money*, 28.

[52] *Testimony Presented before U.S. House of Representatives, Committee on Homeland Security, Assessing Attacks on the Homeland: From Fort Hood to Boston*, 113th Cong., 2013, 7 (testimony of Bruce Hoffman), http://docs house.gov/meetings/HM/HM00/20130710/101108/HHRG-113-HM00-Wstate-HoffmanB-20130710.pdf

[53] Mike Levine and Lee Ferran, "Boston One Year Later: DHS's Lessons Learned," *ABC News* [blog], April 10, 2014, accessed May 2, 2014, http://abcnews.go.com/blogs/headlines/2014/04/boston-marathon-bombing-homeland-securitys-lessons-learned/

[54] Michael Dimock, Carroll Doherty, and Alec Tyson, *Most Expect 'Occasional Acts of Terrorism' in the Future: Six-in-Ten Say Post-9/11 Steps have made Country Safer* (Washington, DC: Pew Research Center for the People & the Press, 2013), http://www.people-press.org/2013/04/23/most-expect-occasional-acts-of-terrorism-in-the-future/

[55] Ibid.

for CT efforts, "The survey…showed that 60 percent of Americans say they think the government actions taken since Sept. 11, 2001, have made the country safer; 35 percent disagreed."[56] Since CT efforts attempt to provide a safer community from the impacts of terrorism, this poll effectively strengthens the argument for CT efforts like a terrorism warning system. It also counters and diminishes the detractors' arguments that terrorism is an exaggerated concern out of step with America's more pressing concerns, such as the United States economy or domestic public policy issues.

b. Heightened Vigilance Beneficial

Supporters of increasing vigilance believe in the inherent deterrent benefit of an alert HSE actively participating in security. Therefore, heightened vigilance is beneficial. The power of teamwork in defeating terrorism is central to the supporters' argument regarding vigilance. The importance of vigilance is reflected in this comment from the

> [Former British] MI5 chief Jonathan Evans signaled that the service wants to raise public vigilance to the terrorist threat, and to stress that intelligence agents alone cannot solve the Islamist extremist problem…[because] this is not a job only for the intelligence agencies and police.[57]

Former DHS Secretary Napolitano echoed this position, "As I said, this new National Terrorism Advisory System is built on the common-sense belief that we are all in this together, and that we all have a role to play."[58]

There are community based programs that provide programmatic evidence supporting the heightened vigilance argument. In keeping with the emphasis on a team approach toward homeland security efforts, engendering assistance from the community or other non-traditional partners for providing effective public safety is not a new

---

[56] David Lauter, "Poll: Terror Acts 'Part of Life' in America," *Spokesman Review* (Spokane, WA), April 24, 2013, sec. A.

[57] Mark Rice-Oxley, "Home-Grown Terrorist Recruitment Rising, Says British Spy Chief," *The Christian Science Monitor*, November 8, 2007.

[58] "Written Testimony of Department of Homeland Security Janet Napolitano for a Senate Committee on the Judiciary Hearing Titled 'The Oversight of the Department of Homeland Security,"' April 25, 2012, Department of Homeland Security, http://www.dhs.gov/news/2012/04/25/written-testimony-department-homeland-security-secretary-janet-napolitano-senate

approach. For decades the community-oriented policing (COP) model has performed a very similar function. The United States Department of Justice (DOJ) defines the COP model,

> Community policing is a philosophy that promotes organizational strategies, which support the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime.[59]

The DOJ also notes that this model promotes teamwork, "Community policing, recognizing that police rarely can solve public safety problems alone."[60]

Suspicious activity reporting (SAR) programs also present evidence that heightened vigilance helps counter terrorism. Programs such as, the DHS "If You See Something; Say Something" campaign and the National Suspicious Activity Reporting Initiative (NSI) are examples that diminish the effectiveness of the detractors' argument about vigilance. These programs are nationwide and provide a pathway for information about suspicious activity to officials. It is sometimes difficult to quantify how programs such as this directly mitigate or counter acts of terrorism.

However, a 2010 Institute for Homeland Security Solutions report provides some sense as to the SAR impact. This report, "examines open-source material on 86 foiled and executed terrorist plots against U.S. targets from 1999 to 2009 to determine the types of information and activities that led to (or could have led to) their discovery."[61] Scott Erickson and Matt Mayer of the Heritage Institute examined the report and drew the following conclusion, "A well-informed and capable infrastructure of law enforcement personnel, coupled with a vigilant citizenry, has proven to be an important shield against the machinations of diverse and disparate groups of organizations and individuals with

---

[59] Department of Justice, Office of Community Oriented Policing Services, *Community Oriented Policing Defined* (Washington, DC: Department of Justice, 2009), 1.

[60] Ibid., 5.

[61] Kevin Strom, *Building on Clues Successes and Failures in Detecting U.S. Terrorist Plots, 1999–2009* (Research Triangle Park, NC: Institute for Homeland Security Solutions, 2010), 25.

terrorist inclinations."[62] This was based upon their analysis of the following report findings:

> The report collated and analyzed 86 terror plots through the 10-year period of January 1, 1999, to December 31, 2009, 18 of which were executed. Each of the 68 failed plots analyzed had a nexus to terrorism, the majority of which were related to al-Qaeda or al-Qaeda-associated movements (AQAM), or al-Qaeda–inspired incidents (often committed by the proverbial "lone wolf" terrorist). Revealingly, over 80 percent of the 68 thwarted cases were the subject of full criminal investigations that resulted from the initial observations of federal, state, and local law enforcement officers conducting routine police work, and through the vigilant observations of the public. Reports of suspicious activity, tips from the public, and the investigation of seemingly unrelated "ordinary" criminal activity accounted for a substantial number of lead-ins to full investigations that would ultimately frustrate the terrorist intentions of those apprehended.[63]

This analysis provides strong evidence of the deterrent effect of heightened vigilance and it is clearly beneficial in support of CT efforts.

c. Increased Security Outweighs the Increased Mitigation Costs

Supporters present evidence that increased security outweighs the increased mitigation costs. The detractors presented a figure of $1 trillion as the cumulative security cost over the period of the past decade since the 9/11 attacks. However, this figure is counterbalanced with staggering short and long-term costs incurred by the attacks on that single day. A 2009 report compiled by three Federal Reserve Bank researchers finds that the 9/11 attack on the World Trade Center in New York City resulted in the following:

> The total physical capital loss was estimated to be $21.6 billion and the lifetime earnings loss was estimated to be $7.8 billion, yielding a total estimated loss of $29.4 billion ($2001)…. Over this period [2001-2006] it

[62] Jason Bram, Andrew Haughwout, and James Orr, "Further Observations on the Economic Effects on New York City of the Attack on the World Trade Center," *Peace Economics, Peace Science and Public Policy* 15, no. 2 (2009):1 1–22, http://www.heritage.org/research/reports/2012/01/a-comprehensive-suspicious-activity-reporting-sar-system-requires-action

[63] Scott Erickson and Matt Mayer, *A Comprehensive Suspicious Activity Reporting (SAR) System Requires Action* (Washington, DC: The Heritage Foundation, 2012).

> is estimated that [lost] wage and salary income was roughly $6 billion ($2006).[64]

The staggering magnitude of these costs, incurred from one coordinated terrorist attack, comprises a strong argument in the supporters' calls for security spending sufficient to prevent another occurrence.

Furthermore, an assessment conducted of homeland security spending for the period of 2001–2005 concluded, "Given the modest increase—as well as the robust economic performance of the U.S. economy since 2001—we conclude that the broader economic impact of higher security spending has been very limited."[65] Moreover, this sum could be considered a security-related maintenance cost in order to avoid another successful terrorist attack or attacks accumulating the costs of United States blood and treasure on the scale of 9/11. The cost consequences of the 9/11 terrorist attacks, combined with the limited impact of security related spending, present the fundamental core of the supporters' counterargument for the detractors' claims of overspending.

If a straightforward cost-based counterargument is insufficient, supporters present the chilling facts of the 9/11 attacks expressed in more kinetic terms.

> Between the jets, the fuel, and the kinetic force of the collapsing World Trade Center buildings, the southwestern tip of Manhattan had been struck with a force estimated at twice the size of the smallest U.S. tactical nuclear weapon.[66]

Supporters also remind us of other horrific acts of terrorism, such as the July 7, 2005 London bombings, or the March 11, 2004, Madrid Train bombing. Sometimes the terrorists themselves weigh in to this cost argument with a cold reminder in the form of a successful attack, such as the 2013 Boston Marathon bombing. This aspect of the supporters' argument is not expressed with financial or economic terms. This aspect of the supporters' argument is a sobering reminder of the very real catastrophic impacts

---

[64] Bram, Haughwout, and Orr, "Further Observations on the Economic Effects."

[65] Bart Hobijn and Erick Sager, "What Has Homeland Security Cost? An Assessment: 2001–2005," *Current Issues in Economics and Finance* 13, no. 2 (2007): 2.

[66] Linda Rothstein, "After September 11," *Bulletin of the Atomic Scientists* 57, no. 6 (2001), 44.

from just one successful terrorist attack. This type of reminder makes the more theoretical and statistical frequency argument of the detractors diminished in effectiveness.

5. Terrorism Warning System Alternative

Other current terrorism warning system research presents at least one alternative to NTAS, "[A] merger of HSAS with [the Department of Defense Force Protection Conditions (FPCON)] would provide one credible and recognizable viable system."[67] This alternative concept advanced the argument that the well-recognized system of HSAS alert levels combined with a more prudent use and communication of those levels through the FPCON methodology supplies a more effective national system. According to Sharp,

> The easy color-coding recognition of HSAS combined with the threat levels and established measures in the FPCON system are a match that should be implemented to provide federal agencies, the industrial sector, and the general public with the best threat advisory system.[68]

This alternative integrates the color codes with military terminology. This does not sufficiently address the issues of providing specific detailed warning and in improving the diminished level public confidence and trust. These are significant issues noted in the *Homeland Security Advisory Council (HSAC) Task Force Report* as well as in other numerous expert criticisms of what the United States terrorism warning system should address. This alternative approach does not effectively address the central task and supporting aspects of an effective terrorism warning system presented earlier in this chapter. Subsequently, this alternative does not answer the need for an improved terrorism warning system.

6. Theories Supporting Warning System Evaluation

The literature review also revealed theories directly related to evaluating decision making regarding both deliberate, such as terrorism. The "preventive action theory"

---

[67] Information in brackets provides clarification for the author's use of FPCON acronym in the original text. Sharp, "Faded Colors," 5–6.

[68] Ibid., 66.

directly applies to assessing decision making efforts in preventing terrorism. Dr. Erik Dahl's preventative action theory supplies an important framework in understanding the interaction between the decision-makers and those charged with supplying them with the decision support materials.[69] It is essential in understanding the decision advantage value between the two terrorism warning systems. This is a great approach for capturing the difficulties inherent with a decision regarding a deliberate threat type such as terrorism.

Complementing the preventive action theory, "resources-processes-values" (RPV) framework provides another assessment structure sufficient to address both the similarities between the warning systems as well as their differences. Although Christensen originally applied RPV to the business world, it effectively allows evaluation of the elements of each warning system and then supports comparison of these elements amongst the systems.[70]

[69] Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013).

[70] Clayton M. Christensen, *The Innovator's Dilemma: The Revolutionary Book that Will Change the Way You do Business* (New York: Harper Business, 2011), 185–197.

III. HOMELAND SECURITY ADVISORY SYSTEM

This chapter provides the background of HSAS. The process portion of this chapter discusses how HSAS was utilized. HSAS is then presented through a case study. An assessment of the system follows the case study, which utilizes a standardized panel of questions as well as the preventive action theory and the RPV framework. Finally, a conclusion is drawn about HSAS before transitioning to case study discussion of NTAS.

A. BACKGROUND

Understanding HSAS, even its problems, provides solid context for assessing whether NTAS is the solution to the failures of this original advisory system. On March 11, 2002, President George W. Bush signed *Homeland Security Presidential Directive/HSPD-3*, creating a graduated threat advisory system to alert government authorities at all levels, as well as the American people, concerning the risk of terrorist attacks. HSAS was the "system of record" outlined in HSPD-3, with aspects amended by subsequent policy and statute.[71] The HSAS consisted of five levels, ranging from the lowest threat level, "green," to the most severe, "red." The movement from one threat level to another resulted in the modification of activated protective measures and security posture. The HSPD-3 identified the Attorney General as having primary responsibility for the HSAS; however, this was altered by later policy and statute.

Both HSPD-5 as well as the Homeland Security Act of 2002 (HSA 2002), section 203, (as amended by the 9/11 Act) named the Secretary of DHS as having primary responsibility to administer the HSAS. Section 203 directed the Secretary to develop a HSAS that was more comprehensive than that of HSPD-3, in that DHS was directed to establish criteria and methodology for the issuance and revocation of advisories; develop the content of these advisories; develop targeted advisories for specific regions, localities or economic sectors; and go beyond a simple color-coded system to advise of threats.

[71] Executive Office of the President, *Homeland Security Presidential Directive/HSPD-3* (Washington, DC: The White House, 2002).

B. HSAS PROCESS

Pursuant to HSPD-3 and as clarified later in HSPD-5, HSAS level changes were decided through a less defined and rather inconsistent decision-making process,

> Except in exigent circumstances, the Secretary of Homeland Security shall seek the views of the Attorney General, and any other federal agency heads the Secretary deems appropriate, including other members of the Homeland Security Council, on the Threat Condition to be assigned.[72]

The distribution of alert/warning information was also less defined:

> The Secretary shall ensure that, as appropriate, information related to domestic incidents is gathered and provided to the public, the private sector, State and local authorities, Federal departments and agencies, and, generally through the Assistant to the President for Homeland Security, to the President.[73]

Even with HSPD-3 and the clarification provided in HSPD-5, making HSAS changes and communicating them was not a science but more of an art form. This created great difficulty in consistently conducting HSAS decisions and notifications. In 2004, the Government Accountability Office (GAO) conducted an investigation into HSAS in an effort to understand the process and present potential recommendations for improvement. As lead for one of these investigations, Randall Yim stated in testimony to the United States Congress, "They [DHS officials] said no explicit criteria or other quantifiable factors are used to decide whether to raise or lower the national threat level."[74] In a related GAO report, "DHS officials told us that they have not yet formally documented protocols for notifying federal, state, and local government agencies of national threat level changes."[75] This lack of consistent process violated GAO guidance regarding

---

[72] White House, *Homeland Security Presidential Directive/HSPD-5: Management of Domestic Incidents* (Washington, DC: U.S. Government Printing Office, 2003), in Public Papers of the Presidents of the United States: George W. Bush, 229–234, http://www.gpo.gov/fdsys/pkg/PPP-2003-book1/html/PPP-2003-book1-doc-pg229.htm

[73] Ibid.

[74] *House of Representatives. Committee on Government Reform. Subcommittee on National Security, Emerging Threats, and International Relations, Homeland Security Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System*, 108th Cong. (2004) (testimony Randall Yim), http://www.gao.gov/assets/120/110679 html

[75] Jenkins, *Homeland Security Advisory System*, 8–9.

internal controls for government agency operations, "For an entity to control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events."[76]

A cumulative conclusion drawn from the multiple studies of HSAS is that the decision-making process for HSAS was convoluted, lacked transparency, and engendered little public trust.[77] The convoluted nature of HSAS and its lack of public trust are exemplified in a comment from an HSAS risk communications respondent to DHS in August 2009:

> Consistently, citizens from my community will ask me what are the trigger points, or bench marks to change the color, but more importantly, what actions should they be taking in their personal lives should that threat level change? Unfortunately, I can't give them any real clear guidance.[78]

The *HSAC Task Force Report* further highlighted the need for improved transparency with the Task Force receiving input such as:

> We also noted that 41% of citizen respondents to the DHS HSAS website cited the lack of specificity in the current HSAS process as a major concern. This reinforces the need for communicators to be advocates of transparency, as threats and as any new threat advisory system is developed and presented to our citizens.[79]

As reflected in the numerous reports and studies cited thus far, HSAS did not maintain any tenet of an effective terrorism warning system. It did not provide timely detailed threat information, nor did it provide clear and understandable protective actions. In addition, it did not provide a clear duration of a period of threat. Finally, it was not consistent in changing the color-code levels. It did not provide decision advantage.

---

[76] General Accounting Office, *Internal Control Standards for Internal Control in the Federal Government* (Washington, DC, General Accounting Office, 1999).

[77] Homeland Security Advisory Council, *Stakeholder Feedback Report*, 15; Homeland Security Advisory Council, *HSAS Survey Report*; Homeland Security Advisory Council, *Homeland Security Advisory System*.

[78] Homeland Security Advisory Council, *Stakeholder Feedback Report*.

[79] Homeland Security Advisory Council, *Homeland Security Advisory System*, 23.

C. CASE STUDY: 2009 "CHRISTMAS DAY BOMBING"

After more than six years of HSAS, these combined factors of systemic ineffectiveness resulted in a widespread loss of confidence in the system. HSAS was so ineffective that it was not central in addressing a clear incident of terrorism in December 2009.[80] The 2009 Christmas Day bombing case study illustrates this assessment.

The 2009 Christmas Day bombing case is also known as the "Underwear Bomber" case thanks to the incorporation of an improvised explosive device (IED) into a pair of underwear worn by the convicted terrorist Umar Farouk Abdulmutallab in his attempt to blow up Northwest Flight 253 over Detroit. According to the report from the International Centre for Political Violence and Terrorism Research (ICPVTR) Northwest Flight 253 carried 290 passengers and crew.[81] If his attack had succeeded, it could have resulted in the death of the 290 people onboard and in an untold number of others—depending on the location over which this attack occurred. This case study reflects the HSAS role in dealing with a terrorist attack. As previously discussed, HSAS suffered from a lack of confidence and ineffectiveness from the lack of a defined or focused process. The results of this are readily apparent in how the USG did not utilize HSAS in addressing the Christmas Day bombing incident in 2009.

As noted, the ICPVTR conducted an analysis and compiled a report of the events leading up to the incident as well as the attack itself. According to this report,

> In August 2009, Abdulmutallab visited his hometown in Abuja, Nigeria and is said to have spent two weeks there before going to Yemen…it was during this time there [Yemen] that he became a full-fledged radicalized extremist."[82] There, known terrorist Anwar al-Awlaki, completed

[80] Ineffectiveness due to HSAS failure to accomplish the mandated requirements noted earlier in this chapter: HSA 2002, Section 203 required the secretary to develop a HSAS that was more comprehensive than that of HSPD-3, in that DHS was directed to establish criteria and methodology for the issuance and revocation of advisories; develop the content of these advisories; develop targeted advisories for specific regions, localities or economic sectors; and go beyond a simple color-coded system to advise of threats.

[81] Diane Russel and Ong Junio, *Report on the Attempted Bombing of Northwest Airlines Flight 253 'Christmas Bombing Plot'* (Singapore: Nanyang Technological University, S. Rajaratnam School of International Studies, 2010).

[82] Russel and Junio, *Report on the Attempted Bombing of Northwest Airlines Flight 253*,' 5.

> Abdulmutallab's recruitment, selection and preparations for a "martyrdom mission.[83]

On December 7, 2009, after completing necessary preparations in Yemen, Abdulmutallab transited through Ethiopia to Ghana. On December 16, he purchased, with cash, a round-trip plane ticket to Detroit, Michigan that included a connection through Amsterdam. He flew to Nigeria on December 24 and began his flight to Detroit, which ultimately culminated in his failed bombing attempt.

During the period when Abdulmutallab was in Yemen,

> The suspect's own family had some concerns with his behavior. Sometime in November 2009 (approximately four weeks before the attempted bombing), Dr. Mutallab [Abdulmutallab's father] told the United States Embassy in Abuja, Nigeria, about his concerns for his son's religious beliefs.[84]

The White House review report of this incident confirmed this communication with the embassy occurred on November 18.[85] The ICPVTR report noted, "The information was passed on to U.S. intelligence agencies, which placed Abdulmutallab's information in…, the Terrorist Identities Datamart Environment (TIDE) database, which is managed by the U.S. National Counterterrorism Center."[86] According to NCTC.gov:

> TIDE is the U.S. Government's (USG) central repository of information on international terrorist identities. The TIDE supports the USG's various terrorist screening systems or 'watchlists' and the U.S. Intelligence Community's overall counterterrorism mission. This information is available to counterterrorism professionals throughout the Intelligence Community, including the Department of Defense, via the web-based, read-only 'TIDE Online.'[87]

---

[83] Ed White, "Feds Release New Details about Underwear Bomber," *The Washington Times*, February 10, 2012.

[84] Russel and Junio, *Report on the Attempted Bombing of Northwest Airlines Flight 253*, 6.

[85] "Summary of the White House Review of the Details of the December 25, 2009 Attempted Terrorist Attack," 2009, Federal Depository Library Program, http://purl.access.gpo.gov/GPO/LPS118485

[86] Russel and Junio, *Report on the Attempted Bombing of Northwest Airlines Flight 253*, 6.

[87] National Counterterrorism Center, "Terrorist Identities Datamart Environment Fact Sheet," National Counterterrorism Center, August 1, 2014, http://www nctc.gov/docs/tidefactsheet_aug12014.pdf

This fact is key because it represented a missed opportunity for intelligence and CT professionals to possibly prevent the attack. The availability of this information, combined the lack of analysis to understand what it meant, provided one of the most vexing points of frustration.

This failure to secure the American people created great frustration in every part of the HSE and American public. Senator Joseph Lieberman gave voice to the broad level of frustration this case generated regarding the systemic failures in homeland security:

> In the Christmas Day bombing case, there was so much intelligence and information available to our government that pointed to Abdulmutallab's violent intentions that it is beyond frustrating—it is infuriating—that this terrorist was able to get on that plane to Detroit with explosives on his body. He was able to do so, in sum, as President Obama has correctly said, because of systemic failures and human errors.[88]

The White House review of the incident stated, "Unfortunately, despite several opportunities that might have allowed the CT community to put these pieces together in this case…that was not done."[89]

The White House review revealed,

> The most significant failures and shortcomings that led to the attempted terror attack fall into three categories:
>
> - A failure of intelligence analysis, whereby the CT community failed before December 25 to identify, correlate, and fuse into a coherent story all of the discrete pieces of intelligence held by the U.S. Government related to an emerging terrorist plot against the U.S. Homeland organized by al-Qa'ida in the Arabian Peninsula (AQAP) and to Mr. Abdulmutallab, the individual terrorist.
> - A failure within the CT community, starting with established rules and protocols, to assign responsibility and accountability for follow up of high priority threat streams, run down all leads, and track them through to completion; and

[88] *Hearing before the Committee on Homeland Security and Governmental Affairs, Intelligence Reform, 2010 Hearings before the Committee on Homeland Security and Governmental Affairs, United States Senate*, 111th Cong. (2010), http://www.gpo.gov/fdsys/pkg/CHRG-111shrg56838/pdf/CHRG-111shrg56838.pdf

[89] "Summary of the White House Review of the Details of the December 25, 2009," 1.

- Shortcomings of the watchlisting system, whereby the CT community failed to identify intelligence within U.S. government holdings that would have allowed Mr. Abdulmutallab to be watchlisted, and potentially prevented from boarding an aircraft bound for the United States.[90]

The report also points out that the difficulties and failures of the "Christmas Day bombing" differ from those of the attacks on 9/11. According to the "Summary of the White House Review," "Previously [during 9/11] there were formidable barriers to information sharing among departments and agencies…. [The Christmas Day bombing] problem appears to be more about a component failure to 'connect the dots,' rather than a lack of information sharing."[91] This conclusion indicates a lack of coordination of efforts and not only a lack of information sharing amongst intelligence and CT officials.

The congressional testimony from the first DHS CT Coordinator, Rand Beers, highlights the absence of an HSAS capability to provide a methodology supporting CT coordination and decision making:

> Following the attempted attack on December 25, 2009, Secretary Napolitano assigned me [DHS CT Coordinator, Rand Beers] an additional duty within the Department to improve coordination among the operational components and to bring together the policy and intelligence components to support this effort. As the Department's Coordinator for Counterterrorism, I am responsible for coordinating all counterterrorism activities for the Department and across its directorates, components, and offices related to detection, prevention, response to, and recovery from acts of terrorism.[92]

The creation of the CT Coordinator role reflects the management/coordination gap HSAS represented among decision makers in DHS. This appointment of a CT Coordinator demonstrated DHS Secretary Napolitano's solution to the need for a senior decision maker/manager was needed. This appointment and the chartering of the DHS Counterterrorism Advisory Board (CTAB) in November 2010 addressed the management

---

[90] Ibid., 2.

[91] Ibid., 2–3.

[92] *Senate Committee on Homeland Security and Government Affairs, Ten Years After 9/11: Preventing Terrorist Travel: Before the U.S. Senate Committee on Homeland Security and Government Affairs Committee*, 112th Cong. (2011) (statement of Mr. Rand Beers, Under Secretary for the National Protection and Programs Directorate, U.S. Department of Homeland Security), 122–150, 449, 593.

gap and lack of a designated decision making body for HSAS. These were gaps that existed in HSAS since its establishment. However, the Christmas Day bombing presented a more glaring indictment of HSAS. Since August 2006, the HSAS threat level was "high" or orange specifically for the aviation sector. Despite this fact, Abdulmutallab successfully boarded a plane and came very close to successfully conducting a terrorist attack.

The HSAS did not play a central role in dealing with this situation, as evidenced in the fact that there was no warning provided through a color code change for aviation. According to the historic DHS timeline of HSAS level changes, there was not even an announcement reiterating the importance of security measures consistent with the existing threat level. The fact that even at the point of a terrorist attack, HSAS remained an inert system speaks volumes in regards to its effectiveness and the level of confidence it enjoyed. HSAS was not used to communicate any information regarding this terrorist attack. It remained static at level orange for aviation, even after the attack. In fact, HSAS had not changed at all for three years. Although the color code was at orange at the time for the aviation sector, this was due to a thwarted threat to aviation in 2006 and had nothing to do with the 2009 Christmas Day bombing threat.[93]

D. CASE STUDY ASSESSMENT

Table 1 reflects the outcome of examining HSAS with the standard panel of questions. The problems are apparent. HSAS did not provide a consistent methodology for terrorism warnings nor did it provide a system HSE decision makers at every level could have confidence in. However, over its lifetime, HSAS did maintain a certain level of heightened vigilance/visibility to the threat of terrorism. Even if, toward the end of that lifetime, this vigilance and visibility was more often in the form of jibes on late night talk shows.

[93] Department of Homeland Security, "Chronology of Changes."

Table 1. HSAS Assessment Panel Responses

HSAS Assessment Panel	Answer	Explanation
Management of system established?	No	No formal management system was ever established.
Was management of system sustained, durable, and effective?	No	
Was there a defined decision making process utilized to reach a decision?	No	No defined decision making process was utilized.
Was the decision-making process sufficiently effective?	No	Several cited reports, testimony and assessments provide evidence that HSAS supported decision making was ineffective.
Was the decision making process sustainable in providing a repeatable and consistent method of reaching a decision?	No	
Was the decision making process timely in supporting the situation?	No	
Was the decision making process sufficiently adaptable to provide effective decision support for situations anticipated and unanticipated and/or deliberate/non-deliberate?	No	
Was there a decision making body designated to make this decision?	No	Presidential Directives named cabinet level officials responsible for collaborating on these decisions. However, no formal decision making body was chartered.
Was it necessary for a designated decision making body to exist?	Yes	This presented a major gap in HSAS. The successful application of a designated body in support of NTAS provides evidence of how detrimental this gap was for HSAS.
Was there a defined convening process for gathering the decision makers together?	No	Several cited reports and assessments note the lack of defined process for HSAS.
Was this convening process timely and sustainable when the situation required multiple decisions over the course of extended periods?	No	Several cited reports, testimony and assessments provide a cumulative picture of the lack of sustainability and timeliness in HSAS supported decision making.
Based upon the outcome of the original decision, was the decision making process sufficient in supplying decision advantage to subsequent decision makers dealing with the situation?	No	Cited reports, testimony and assessments note that the HSE at large was often confused by HSAS decisions. This created cascading failures in decision making at every level of the HSE.
Was this system the only or principal decision support pathway through which the decision reached decision makers?	No	This system was not the only or even principal system toward the end of its service life.
Did the system support original and secondary decision makers?	No	Note the previously mentioned cascading failures in decision making throughout the HSE.
Did the system support coordination of efforts dealing with the situation?	No	According to cited reports, testimony and assessments support for coordination was inconsistent at best.

HSAS Assessment Panel	Answer	Explanation
If supporting coordination of efforts, how did the system work effectively?	No	
Was there a designated communication method for the dissemination of the decision?	Yes	Color coded alert levels represented the principle communication method.
Was the decision communicated effectively?	Yes	Color coded alerts minimally communicated threat level changes. However, as noted in reports and testimony, these color code changes were neither well detailed nor contained enough specificity for decision makers to effectively utilize.

1. Standard Panel of Questions Examination

There was a failure to build a repeatable and durable warning and decision support methodology in HSAS. This is represented in the failure to accomplish the mandated requirements noted earlier in this chapter: HSA 2002, Section 203 required the secretary to develop a HSAS that was more comprehensive than that of HSPD-3. Specifically, DHS was directed to establish criteria and methodology for the issuance and revocation of advisories; develop the content of these advisories; develop targeted advisories for specific regions, localities, or economic sectors; and go beyond a simple color-coded system to advise of threats.

The complete absence of HSAS in the management of the Christmas Day bombing incident is telling. At the time of this failed attack in 2009, HSAS was peripheral and of marginal value. The color codes did not change even though this was a clear terrorist incident, which is a clear indication of its ineffectiveness. Even the official White House summary report for the incident did not mention HSAS, instead focusing upon other aspects of the IC and the CT communities of the United States.[94] It had truly become an inert system in need of change. As Shapiro and Cohen concluded, "Given the failure of the HSAS, the time has come to take on the challenge of creating a better system."[95]

[94] "Summary of the White House Review of the Details of the December 25, 2009."

[95] Shapiro and Cohen, *Color Bind: Lessons from the Failed Homeland Security Advisory System*, 154.

2. Theory of Preventive Action

An assessment of HSAS with the preventive action theory reveals critical shortcomings that generated a clear lack of trust in this system. HSAS lacked a defined repeatable decision making process. A consistently receptive decision-making body designed to function strictly in a CT capacity did not exist for HSAS. This lack of a consistent decision-making process and designated CT decision-making body played a role in the mercurial results of the HSAS. Directed in HSPD-3 and HSPD-5, the decision makers consisted of a small group of the most senior policymakers in the USG, the President of the United States, the Attorney General, and the DHS Secretary. The level of HSAS usage over the course of its history from 2002–2011 demonstrates a clear fluctuation in decision-maker receptivity and confidence in HSAS. From its inception in March 2002 until August 2006, 16 changes to the color codes occurred. However, during the last year of the Bush administration no changes occurred. What is particularly telling is that after the presidential administration transition in 2008, HSAS remained inert until its replacement by NTAS in April 2011. This is despite at least two clear terrorist attacks occurring after transition, the 2009 Najibullah Zazi and Christmas Day bomber terrorist incidents. This demonstrates a clear degradation of decision makers' confidence for HSAS.

It also consistently failed to provide a reliable pathway for detailed and timely information in support of senior decision-makers' needs. Consequently, this lack of trust impaired decision making at all levels of the HSE, which in turn, sowed a great deal of confusion amongst the members for the HSE in coordinating, communicating, or executing appropriate countermeasures. This means HSAS never consistently provided strategic warning or successfully addressed the paradox of strategic warning.[96] As a result, HSAS did not consistently provide decision advantage to HSE decision makers.

[96] This paradox contributes to the likelihood terrorist attacks succeed, because decision makers lack the type of detailed timely information necessary to prevent a terrorist attack.

3. RPV Framework

The HSAS did not succeed in its intended mission due to repeated missteps that degraded confidence in the system over time as well as significant organizational design flaws. HSAS suffered from the lack of an effective management system, a haphazard methodology and lack of defined decision making values. This hampered the consistency, sustainability and organizational focus in HSAS performance.

In accordance with the numerous studies of HSAS reflected in this chapter, HSAS did not have a management system or designated body. It did not have organized resources, defined processes, or established decision making values. Unlike its successor NTAS, the DHS CTAB and the CT Coordinator did not manage HSAS until its last months of existence. There was no defined process, such as the NTAS *Concept of Operations* (CONOPS) or other supporting documents, such as the DHS CTAB Charter. This meant there was no defined set of organizational values. This is important as the RPV framework points out, "An organization's values are the standards by which employees make prioritization decisions."[97] The collected organizations attempting to make an HSAS decision or comply with the outcomes of an HSAS decision lacked the ability to anticipate these decisions or interpret how to effectively respond to them. This continually hampered HSAS performance and continued the degradation of confidence members of the HSE maintained in the system.

According to the RPV framework, an organization that relies solely on the competency of the individuals operating a system without the benefit of a defined process is doomed to fail. Christensen explains this maxim of the RPV framework in this way,

> Frequently, they [the organization] assume that if the people working on a project individually have the requisite capabilities to get the job done well, then the organization in which they work will also have the same capability to succeed. This often is not the case.[98]

Due to a lack of management, defined process and organizational values, the HSAS relied too heavily on individual performances in order to accomplish the collective

[97] Christensen, *The Innovator's Dilemma*, 188.

[98] Ibid., 185.

organizational mission of HSAS. This resulted in the outcome Christensen forecasts for any organization or system overly reliant on individual performance, repeated failure.

E. CHAPTER CONCLUSION

As reflected in the case study and the numerous reports and studies cited thus far, HSAS did not maintain any tenet of an effective terrorism warning system. Unfortunately, it did not provide timely detailed threat information, nor did it provide clear and understandable protective actions. It did not provide a clear duration of a period of threat. Furthermore, it was not consistent in changing the color-code levels. Additionally, it did not provide decision advantage. After over six years of using HSAS, these combined factors of systemic ineffectiveness resulted in a widespread loss of confidence in the system. This ineffectiveness resulted in the continued marginalization of HSAS as a terrorism warning system. HSAS was so ineffective that it was not central in addressing a clear incident of terrorism in December 2009.

Subsequently, DHS Secretary Janet Napolitano was already considering major changes in the advisory system as well as the decision-making process it supported. The ineffectiveness of HSAS during the 2009 Christmas Day bombing incident galvanized the DHS Secretary's considerations for changing the system. What resulted was a sea change for how DHS conducted CT decision making, coordination, and communication as well as how it led and supported this process at every level of the HSE.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NATIONAL TERRORISM ADVISORY SYSTEM

The NTAS is the current United States terrorism warning system. The United States DHS maintains responsibility for NTAS. This chapter provides background sketching out the path of how the United States adopted NTAS. The process portion of this chapter discusses how NTAS is utilized. NTAS is then presented through a case study of the 2013 Boston Marathon bombing. An assessment of the system follows the case study, which utilizes a standardized panel of questions as well as the preventive action theory and the RPV framework. Finally, a conclusion is drawn about NTAS before transitioning to a case study discussion of the HWS.

A. BACKGROUND

On July 14, 2009, DHS Secretary Napolitano announced the formation of a HSAC Task Force to conduct a 60-day review of the HSAS. This task force, co-chaired by Fran Townsend and William Webster, consisted of a group of highly respected experts in the field. On September 15, 2009, this task force submitted its report through the HSAC.[99] This report included the following bulleted list of observations/recommendations:

- Enduring Merit of a Dedicated Terrorism Advisory System: In the view of the Task Force, a national threat warning system for terrorist attacks is as central now as it was when today's system [HSAS] was established in 2002.
- Two Audiences—The Public and "Institutions": The Task Force members agreed that there are two primary audiences for the Homeland Security Advisory System.
- The Current Advisory System—Commanding Insufficient Public Confidence: The Task Force members agreed that, at its best, there is currently indifference to the [HSAS] and, at worst; there is a disturbing lack of public confidence in the system.
- Changing the Alert Level Baseline to Guarded Status: In the judgment of the Task Force, a central undermining feature of the current alert system is that the threat level more easily moves up than comes down.

[99] Homeland Security Advisory Council, *Homeland Security Advisory System*.

- Greater Precision is Required in Identifying the Specific Local Governments, First Responders and Private-Sector Companies Threatened and the Protective Measures that Necessitate a Response: The Task Force believes the cost in dollars—and skepticism—of overly broad alerts is a substantial problem requiring remedy.
- The [HSAS] Will Require Dedicated Infrastructure, Staff, Established Protocols and Procedures: The Task Force believes the Secretary should establish the protocols, procedures, and the staff capable of supporting the Secretary.[100]

Based upon the recommendations of the HSAC Task Force, DHS worked toward developing the next variation of a national advisory system throughout 2010. In January of 2011, the president signed *Presidential Policy Directive-7 (PPD-7)*, which superseded HSPD-3, established NTAS and replaced HSAS. The president directed the Secretary of DHS to implement NTAS within 90 days from the signing of PPD-7; this was successfully accomplished on April 26, 2011.

In addition to establishing a new terrorism advisory system, former DHS Secretary Napolitano concurrently chartered the DHS CTAB and the position of the DHS CT Coordinator. The DHS CTAB fulfills the 9/11 Commission recommendation for DHS to

> regularly assess the types of threats the country faces to determine (a) adequacy of the government's plans to protect America's critical infrastructure; and (b) the readiness of the government to respond to threats that the United States might face.[101]

It does both by providing DHS a senior decision-making body, which reviews terrorism threat information and strategically coordinates the department's CT efforts in response to those threats. In doing so, the DHS CTAB lives up to another 9/11 Commission concept of "joint action" within government.[102]

---

[100] Ibid., 1–4.

[101] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W.W. Norton & Company, 2004), 428.

[102] Ibid., 400.

B. NTAS PROCESS AND THE ROLE OF THE DHS CTAB

As discussed earlier, NTAS is designed to provide a decision advantage to a large and diverse group of decision makers, from senior public officials to the individual citizen. The NTAS process is a repeatable deliberate methodology that functions with sufficient agility to address routine CT issues as well as the emergent high tempo of surprise terrorist attacks. This agility is demonstrated in its support for the DHS CT Coordinator and DHS CTAB. The NTAS process guides the timing and sequencing of DHS CT Coordinator and DHS CTAB strategic decision making and coordination activities enabling tactical level success during periods of routine activity and incidents.

As Chapter III notes, the DHS CT Coordinator and the DHS CTAB represent a dramatic improvement in timely and deliberate decision making at the strategic level. Mr. Rand Beers testified to the full breadth of this CT participation/coordination:

> In November 2010, DHS stood up the Counterterrorism Advisory Board (CTAB) to further improve coordination on counterterrorism among DHS components. As the Coordinator for Counterterrorism, I serve as the chair of the CTAB with the Under Secretary of Intelligence and Analysis and the Assistant Secretary for Policy supporting the Board as Vice Chairs. Members include the leadership of TSA, CBP, ICE, the Federal Emergency Management Agency, the U.S. Coast Guard, USCIS, the United States Secret Service, NPPD, and OPS. The DHS General Counsel serves as legal advisor to the CTAB and is present at all meetings.[103]

Each member of the DHS CTAB pools its pertinent information and intelligence about a CT issue in order to develop a focused cogent common knowledge base of the issue. This shared situational awareness supplies decision advantage in affording these leaders a tactically informed capability for strategic decision making, coordination, and communication.

This CT coordination approach addresses a paradox revealed in Dr. Erik Dahl's preventative action theory, which is a major contributing factor in failures to prevent acts

[103] *Senate Committee on Homeland Security and Government Affairs, Ten Years after 9/11*.

of terrorism.[104] Dr. Dahl refers to this major contributing factor as the paradox of strategic warning.[105] This paradox contributes to the likelihood terrorist attacks succeed because decision makers lack the type of detailed timely information necessary to prevent a terrorist attack. Through the NTAS process, the DHS CTAB provides a forum for decision makers to receive sufficient details in order to plan, coordinate and execute timely CT countermeasures.

In congressional testimony, Beers laid out how the NTAS process and DHS CTAB supported addressing the heightened terrorism threat during the time period immediately following the 2011 Osama bin Laden raid:

> While DHS did not issue an NTAS alert based on the threat of reprisal attacks or information obtained at Bin Laden's hideout, the CTAB met daily for the first week, sometimes multiple times per day. In each meeting, the CTAB considered whether any of the new threat information, when weighed against current preventative measures, met the threshold of being "imminent and actionable" to warrant the issuance of an NTAS alert. While none did, I&A worked closely with the FBI and our partners throughout the intelligence community to disseminate information as appropriate to the local law enforcement community and the private sector. Additionally, TSA engaged in extensive outreach efforts with airports, airlines, and freight carriers, and implemented a series of new security measures in the weeks following while CBP identified additional targeting measures to disrupt potential retaliatory attacks.[106]

This testimony represents the current strategic CT decision-making process, now known as the NTAS process. The NTAS process facilitates the timing and sequencing of DHS CT Coordinator and DHS CTAB strategic decision making and coordination activities, which enable tactical level success during periods heightened threat. The NTAS process outlined in this testimony remains the common practice in addressing terrorism threats and incidents since April 2011.

---

[104] "If intelligence is to be successful in preventing major surprise attacks, it must provide specific, tactical-level warning, and policymakers must be receptive to that warning." Dahl, *Intelligence and Surprise Attack*, 176.

[105] According to Dahl, "Policymakers…typically say they want strategic intelligence; but…they are actually less likely to respond to long-range, broad assessments than to specific tactical-level warnings." Ibid.

[106] *Senate Committee on Homeland Security and Government Affairs, Ten Years after 9/11*.

What is also important to note is Mr. Beers' comment concerning how NTAS assisted in navigating the decision maker's dilemma when considering the issuance of a terrorism warning. The CTAB considered its options and opted to utilize other methods. This option effectively facilitated CT efforts, while adequately balancing the need for OPSEC and in avoiding unnecessarily raising the public level of concern from a non-specific terrorism threat. The CT Coordinator/CTAB provided strategic management of the NTAS process throughout this threat period. This clearly avoided "doing the terrorist's job for them," as McDermott and Zimbardo warned was a consequence of a mismanaged terrorism warning system.[107]

In supporting the DHS CT Coordinator and the DHS CTAB, the NTAS process provides improvement in coordinating CT efforts. In communicating information with HSE partners regarding terrorism incidents and corresponding CT activities through JIBs, etc., the NTAS process also addresses the need for any alert or other warning it generates to provide timely detailed information. The NTAS positions DHS for continued improvement in the areas former DHS Secretary Napolitano declared:

> We also continue to expand our risk-based, intelligence-driven security efforts. By sharing and leveraging information, we can make informed decisions about how to best mitigate risk, and the more we know, the better we become at providing security that is seamless and efficient.[108]

This statement represents the vision of former DHS Secretary Napolitano regarding how the NTAS and its process fulfills its mandate: "As I said, this new National Terrorism Advisory System is built on the common-sense belief that we are all in this together, and that we all have a role to play."[109]

---

[107] Bongar et al., eds, *Psychology of Terrorism*, 358.

[108] "Written Testimony of Department of Homeland Security Janet Napolitano for a Senate Committee on the Judiciary Hearing Titled 'The Oversight of the Department of Homeland Security,"' April 25, 2012, Department of Homeland Security, http://www.dhs.gov/news/2012/04/25/written-testimony-department-homeland-security-secretary-janet-napolitano-senate

[109] Janet Napolitano, "State of America's Homeland Security Address," January 27, 2011, http://www.dhs.gov/news/2011/01/27/state-americas-homeland-security-address

C. CASE STUDY: 2013 BOSTON MARATHON BOMBING

The Boston Marathon bombing occurred on April 15, 2013. The attack included two IEDs devised from common household pressure cookers. Two suspects carried out these attacks, brothers Tamerlan and Dzhokhar Tsarnaev. The two IEDs successfully detonated, killing three and wounding over 260 marathon attendees. After these attacks, the FBI led a multi-agency investigation, which identified the two suspects and culminated in the death of Tamerlan Tsarnaev and in the capture of Dzhokhar Tsarnaev on April 19.

The Tsarnaev family history in the United States spans approximately 11 years. Over the course of 2002 and 2003, the Tsarnaev family moved from Dagestan to the United States after their father, Anzor Tsarnaev, applied for asylum. In 2006, Tamerlan was granted lawful permanent resident status. On September 11, 2012, Dzhokhar Tsarnaev became a naturalized U.S. citizen. According to a *Wall Street Journal* article, "The Tsarnaev family struggled with money during their time in the United States. [The Tsarnaevs] reportedly separated, though both returned to Russia before the Boston Marathon bombing."[110]

Despite the family financial struggles, the Tsarnaev brothers completed high school in the United States, Tamerlan in 2006 and Dzhokhar in 2011. Both pursued college educations with mixed results. According to a 2014 U.S. House of Representatives Committee on Homeland Security report, "[I]n the fall of 2006 [Tamerlan] attended Bunker Hill Community College part-time. He left the school in 2008."[111] Dzhokhar attended the University of Massachusetts at Dartmouth; however, "His grades were poor, but by nearly all public accounts he was well-liked and social."[112] At the time of the bombing Dzhokhar remained enrolled at this university.

---

[110] Alan Cullison, Paul Sonne and Jennifer Levitz, "Life in America Unraveled for Brothers," *Wall Street Journal (Online)* April 20, 2013, http://online.wsj.com/news/articles/SB10001424127887323809304578432501435232278

[111] Committee on Homeland Security, *The Road to Boston: Counterterrorism Challenges and Lessons from the Marathon Bombings* (Washington, DC: Government Printing Office, 2014), 10. http://homeland.house.gov/sites/homeland.house.gov/files/documents/Boston-Bombings-Report-Findings.pdf

[112] Ibid., 10.

Although the Tsarnaev brothers' individual paths to radicalization appear different, the length of time for their radicalization is similar to the "Christmas Day bomber," Abdulmutallab's radicalization experience. The Tsarnaevs' radicalization potentially occurred over the course of prior years, with their preparation timeline for the attack beginning a few months before April 15, 2013. According to the 2014 congressional report, "The Tsarnaev family is ethnic Chechen."[113] This fact suggests a clear source of empathy for the brothers regarding the Chechen separatist movements against Russia raging in the North Caucasus region over the past two decades:

> It has not been determined whether the Boston Marathon bombing…is tied directly to the…ongoing terrorist activity in Dagestan, Chechnya, and across the North Caucasus. However, it is reasonable to assume that Tamerlan Tsarnaev was at least inspired by their activity and ideology, and driven to take part in the vision of global jihad which they share with al Qaeda.[114]

Tamerlan's radicalization experience appears to have started during his time in the United States, but it accelerated and calcified during a trip to the North Caucasus region in 2012. Upon returning to the United States, Tamerlan viewed and posted radical jihadi YouTube videos, "indicating some degree of radicalization had taken place while he was in Russia."[115] Additionally, Russian media reports a relationship with a radicalized Canadian citizen William Plotnikov: "Russian authorities were alerted to Tamerlan Tsarnaev after finding evidence of 'frequent contacts' between the two on William Plotnikov's computer."[116] Plotnikov "converted to Islam 2009 and left Canada to join rebels in Dagestan."[117] However, "Plotnikov died during a shootout with Russian security services on July 14, 2012," which is roughly when Tamerlan was in the

---

[113] Ibid., 9.

[114] Ibid.

[115] Ibid., 15.

[116] Fatima Tlisova, "Russians Closely Monitored Boston Bombing Suspect," *Voice of America*, May 7, 2013, accessed July 14, 2014, http://www.voanews.com/content/tsarnaev-dagestan-bombing/1656176.html

[117] Stewart Bell, "The Canadian Who Converted to Jihad: Boxer Turned Militant Killed in Dagestan," *National Post*, August 20, 2012, accessed July 14, 2014, http://news.nationalpost.com/2012/08/20/dagestan/

Caucasus.[118] The implications of this relationship are that Tamerlan was seeking or potentially had a relationship with radicalized groups in the North Caucasus. Regardless the nature of the direct relationship with Islamist radicals in the North Caucasus, Tamerlan's behavior clearly demonstrates a consistent identification with the radical Islamist perspective and a disturbing evolution into a radical Islamist.

Dzhokhar's radicalization appears more vicarious, occurring through his "close relationship with his older brother" Tamerlan.[119] This timing allowed Tamerlan to act as a mentor for Dzhokhar's transformation. Psychologist Clark McCauley described the relationship: "His brother [Dzhokhar] admired him [Tamerlan], following him around the gym like a puppy."[120] When the Tsarnaev parents left the United States, leaving Dzhokhar alone and without a support network, "[i]t was Jahar's [Dzhokhar's] love and respect for his radicalized brother that gave him new direction after he lost everyday connections with high school friends and most of his family."[121] Dzhokhar grew more isolated as his broader social network degraded, and he drew closer to his brother. According to McCauley, "Jahar had lost connection with all of his family except Tamerlan."[122] In addition, McCauley expresses Dzhokhar's radicalization in this way, "mechanisms of radicalization [were] at work…escalating [Dzhokhar's] commitment to his brother's bombing project."[123]

McCauley's theory on Dzhokhar's radicalization is further supported with accounts during the period of time when the two brothers were isolated building the bombs "in the third-floor Cambridge apartment that authorities say served as the unlikely epicenter of the Boston Marathon bombing plot."[124] Their downstairs Cambridge

---

[118] Ibid.

[119] Committee on Homeland Security, *The Road to Boston*, 10.

[120] Clark McCauley, "Radicalization of Tamerlan and Dzhokhar Tsarnaev," *Psychology Today* [blog], April 19, 2013, http://www.psychologytoday.com/blog/friction/201304/radicalization-tamerlan-and-dzhokhar-tsarnaev

[121] Ibid.

[122] Ibid.

[123] Ibid.

[124] Mark Morales, "Inside Devils' Den Half-Eaten Meal on Table Sibs Lived Amid Squalor in Ramshackle Apt," *New York Daily News,* April 21, 2013, sec. News.

apartment neighbor stated, "I lived right underneath them, and they were making bombs. It's scary."[125] This period of time also reflects the level of commitment the two brothers demonstrated in conducting these attacks. They traveled to attain materials: "At Seabrook, NH… [Tamerlan] Tsarnaev paid $199.99 in cash for each of two…mortar kits that come with a tube and 24 shells."[126] The brothers painstakingly accumulated the materials and fabricated the bombs; they "emptied hundreds of packages of fireworks to create fuel for the bombs…. [T]he fuses were fashioned from Christmas lights and the improvised remote-control detonators were built from model car parts."[127]

It appears that whereas Tamerlan actively pursued radicalization, Dzhokhar radicalized more passively through the conditioning effects of his exclusive attachment to Tamerlan. Although the individual pathways varied, Fathali M. Moghaddam explains the Tsarnaev brothers' shared radicalization: "[T]errorism is explained by perceptions of deprivations, by feelings of being treated unfairly, by a subjective sense of injustice, rather than by objective conditions, including poverty and low education."[128] This explanation is consistent with the paradoxical circumstances of the Tsarnaev radicalizations. Despite the fact that both enjoyed the opportunities afforded them from their living in the United States, through their radicalization they came to identify more with their Chechen roots. This radicalization resulted in their pursuit of terrorism in support of the Chechen societal frustration against their perceived enemy embodied in the adopted society they grew up in. As the brothers reached the conclusion of their journey to radicalization, they arrived as fully functioning terrorists. It is certainly demonstrated in Dzhokhar's scrawled message on the inside of the boat in which he was captured:

---

[125] Ibid.

[126] Phil Mattingly, Roxana Tiron, and Margaret Talev, "Officials Study Brothers' Islam Ties; Pair Allegedly behind Boston Marathon Attack were Said to be Drawn to Radical Islam on Internet," *Charleston Daily Mail* (West Virginia), April 25, 2013, sec. News.

[127] Richard A. Serrano, "Boston Attackers May Have Had Help, U.S. Says," *Los Angeles Times*, May 22, 2014, sec. LATextra, Part AA, http://www.latimes.com/nation/la-na-boston-bombing-20140522-story html

[128] Fathali M. Moghaddam, *From the Terrorists' Point of View What They Experience and Why They Come to Destroy* (Westport, CT: Praeger Security International, 2006), 46.

"[T]he U.S. government is killing our innocent civilians…. I can't stand to see such evil go unpunished…. We Muslims are one body, you hurt one, you hurt us all."[129]

In late April 2013, the United States IC Inspectors' General Forum directed an assessment related to the Boston Marathon bombing. This assessment evaluated three aspects of USG actions:

- The extent of the information available to the U.S. government concerning the relevant individuals and events preceding the Boston Marathon bombings.
- Whether the sharing of this information was complete, accurate, and in compliance with U.S. counterterrorism and information sharing, policies, regulations, and U.S. laws.
- Whether there are weaknesses in protocols and procedures that impact the ability to detect potential threats to national security.[130]

The Inspectors General (OIGs) for the Intelligence Community, the DOJ, the Central Intelligence Agency (CIA) and the DHS conducted this assessment and published it in April 2014 titled *Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombings*.[131] This report targets tactical level actions taken by individuals in an effort to understand gaps in procedures, which may have led to the bombing on April 15, 2013. By identifying these gaps and recommending solutions, this assessment will assist in preventing future attacks.

Firstly, the Inspectors General (IGs) assessment concludes that in the broader efforts of the USG, which may have been able to mitigate the Boston Marathon bombing occurred appropriately, "In light of our findings and conclusions…the participating OIGs found no basis to make broad recommendations for changes in information handling or sharing."[132] Secondarily, the assessment concludes that gaps in tactical level procedures and policies created an environment in which individual USG personnel decisions and

---

[129] McCauley, "'Friction' Mechanisms at Work: More about Dzhokhar Tsarnaev."

[130] Inspectors General for the Intelligence Community, the Department of Justice, the Central Intelligence Agency, the Department of Homeland Security, *Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombings* (Washington, DC: Inspectors General of the Intelligence Community, 2014), 3.

[131] Ibid.

[132] Ibid., 25.

actions did not adequately prevent or otherwise mitigate this travel opportunity, "We nonetheless identified some areas in which existing policies or practices could be clarified or improved."[133] It is hard to quantify the degree to which Tamerlan Tsarnaev's travel to the North Caucasus contributed to the radicalization of Tamerlan and Dzhokhar and led to their attack upon the Boston Marathon. However, the missed opportunities to identify this travel and understand what the pattern of behavior may have indicated created a lost opportunity to potentially prevent this attack.

A 2014 DHS lessons learned report, *Boston One Year Later: DHS's Lessons Learned*, regarding the Boston Marathon bombing notes the CTAB as point of coordination and synchronization as the department supported the incident. DHS notes the CTAB role in strategically integrating communications into the overall DHS and USG efforts, as it provided a senior decision making forum.[134] Citing this 2014 report, Mike Levine of *ABC News* highlights many of the coordinated DHS actions for Boston:

> The DHS established 'an extended perimeter to intercept potential suspects and interview witnesses,' CBP helped deploy air assets and other forms of transportation support over the area, DHS provided briefings to State and local law enforcement and homeland security officials, critical infrastructure owners and operators, and faith-based organizations, 'TSA heightened security throughout the Northeast region airports with increased explosive trace detection, canine deployment, gate checks and behavior detection activities,' the Coast Guard 'immediately raised and coordinated its on-water security presence with increased patrols 24/7 in the inner harbor and along ferry routes,' and the Secret Service 'utilized its New England Electronic Crimes Task Force to collect and review business surveillance videos in proximity to the bombing site for evidence related to investigation.'[135]

During this incident the NTAS and its process was supported CT decision making, coordination, and communication through the DHS CT Coordinator and the CTAB. This NTAS support is demonstrated in the activities above specific to the Boston incident. It is also evidenced in the previously cited congressional testimony from the

---

[133] Ibid.

[134] Department of Homeland Security, *Boston One Year Later: DHS's Lessons Learned* (Washington, DC: Department of Homeland Security, 2014), 9.

[135] Levine and Ferran, "Boston One Year Later: DHS's Lessons Learned."

former DHS CT Coordinator regarding the common practice the NTAS process provides during incidents.

The actions of state and local officials in the Boston Metro area present solid evidence regarding how targeted communications, similar to that embodied in NTAS, are effective. State and local officials used the same approach as NTAS, which is to provide detailed and timely information to the citizenry in order to elicit their assistance in the situation through press conferences and other public statements. An example of how the NTAS process supported the incident is the use of other methods of communication, such as a JIB as well as various press statements and press conferences from various officials involved in handling the incident. The following prepared statement describes this support:

> NTAS was designed to provide information to the public and stakeholders in a timely manner when there is a specific and credible terrorist threat. A public alert is only one part of that system, which also includes the distribution of information to state, local and federal officials, as well as pertinent stakeholders. Following the Boston Bombing, out of an abundance of caution, DHS remained at a heightened state of vigilance, but the specific facts did not warrant the issuance of a public NTAS alert. Still, significant outreach occurred including several intelligence bulletins, multiple briefings not only with state, local and federal officials but also with private sector stakeholders and faith-based groups, and with the public through a variety of public statements. In this instance, state and local entities in the affected area had already issued public alerts and there was widespread coverage of this FBI led investigation.[136]

The Tsarnaevs' successfully conducted an act of terrorism; their murderous act left three people dead and 260 injured. Mistakes were made within the HSE that potentially enhanced the likelihood of success for this attack. However, despite the initial success the Tsarnaevs' enjoyed, they were neutralized in relatively quick order, within the span of four days. This is in no small part a result of a well-coordinated investigation and the activities of the HSE partners supporting that investigation, such as the NTAS process and the CTAB.

---

[136] Department of Homeland Security, *Prepared Statement Regarding NTAS during Boston Marathon Bombing* (Washington, DC: Office of Public Affairs, 2013).

D. CASE STUDY ASSESSMENT

1. Standard Panel of Questions Examination

Table 2 reflects the outcome of examining NTAS with the standard panel of questions. The NTAS successes are apparent and scored well in response to the questions. What follows is a summary supporting the answers reflected in the panel of questions.

Table 2. NTAS Assessment Panel Responses

NTAS Assessment Panel	Answer	Explanation
Management of system established?	Yes	DHS established management through designating the CT Coordinator and chartering the CTAB.
Was management of system sustained, durable, and effective?	Yes	Noted in testimony and lessons learned reporting, the CTAB functioned well.
Was there a defined decision making process utilized to reach a decision?	Yes	As directed in PPD-7, the NTAS provided this process.
Was the decision making process sufficiently effective?	Yes	NTAS proved effective decision advantage, supporting strategic CT coordination, communication and decision making.
Was the decision making process sustainable in providing a repeatable and consistent method of reaching a decision?	Yes	In two noted terrorism situations, NTAS provided repeatable and consistent decision support.
Was the decision making process timely in supporting the situation?	Yes	NTAS met its 24 hour a day and seven day a week mission support requirement. Noted in the Boston incident, NTAS was immediately executed within minutes of the explosions.
Was the decision making process sufficiently adaptable to provide effective decision support for situations anticipated and unanticipated and/or deliberate/non-deliberate?	Yes	NTAS adapted to the fluid Boston Marathon bombing tempo.
Was there a decision making body designated to make this decision?	Yes	The CTAB is the chartered decision making body.
Was it necessary for a designated decision making body to exist?	Yes	As proved in the failures of HSAS, a designated decision making body is needed.

NTAS Assessment Panel	Answer	Explanation
Was there a defined convening process for gathering the decision makers together?	Yes	The NTAS process provides this convening process.
Was this convening process timely and sustainable when the situation required multiple decisions over the course of extended periods?	Yes	The NTAS process supported multiple CTAB meetings and other operation tempo requirements throughout the four day period.
Based upon the outcome of the original decision, was the decision making process sufficient in supplying decision advantage to subsequent decision makers dealing with the situation?	Yes	As noted in testimony and lesson learned reports, the strategic coordination and decisions positively supported downstream decisions and actions dealing with the situation.
Was this system the only or principal decision support pathway through which the decision reached decision makers?	Yes	The NTAS process provided the principal pathway.
Did the system support original and secondary decision makers?	Yes	As noted in testimony and lessons learned reports, information and guidance derived from the NTAS process supported both groups of decision makers.
Did the system support coordination of efforts dealing with the situation?	Yes	As noted in testimony and lessons learned reports, NTAS provide support to strategic CT coordination throughout the incident.
If supporting coordination of efforts, did the system work effectively?	Yes	NTAS effectively supported the successful neutralization of the terrorist threat presented from the Tsarnaev brothers.
Was there a designated communication method for the dissemination of the decision?	Yes	Although an alert was not generated from the NTAS Process, JIBs, press statements and other direct forms of communication were utilized as part of the flexible NTAS process.
Was the decision communicated effectively?	Yes	NTAS facilitated effective communication from the first few minutes until the concluding moments of the incident.

NTAS enjoyed the advantage of a dedicated CT decision-making body in the DHS CTAB. Just as it did during the time following the Osama Bin Laden raid, the NTAS process provided decision advantage to DHS and other members of the HSE. During that four-day period in April 2013, officials followed the same NTAS process in support of the same tempo the former DHS CT Coordinator Rand Beers articulated in

congressional testimony regarding the threat period after the Osama Bin Laden raid.[137] In fulfillment of its chartered CT coordination mission, the DHS CTAB convened repeatedly and strategically guided the overall effort for the department. The DHS CTAB, supported through the NTAS process, ensured decision makers at every level of the HSE received the information needed to make decisions and take appropriate actions. Through ensuring information and intelligence was shared appropriately, as pointed out in the OIG report and in Principal Deputy Assistant Secretary Jensen congressional testimony:

> The attack in Boston on April 15, 2013 fully engaged the communications processes and capabilities DHS has put in place over the past ten years. Within minutes of notification of the attack the [DHS] Office of Public Affairs began mobilizing its resources and our Federal incident communications process. The U.S. Attorney's Office in Boston, FBI Boston Field Office, Massachusetts State Police, Boston Police Department, and the Suffolk County Sherriff's Office served as the lead on-scene communicators and participated in NICCL calls [National Incident Communications Coordination Line]. These calls, which included the Federal interagency, provided participants with a coordinated communications path in the immediate aftermath of the attack.[138]

The Office of Public Affairs (OPA) activities Mr. Jensen mentions provides one example of the strategically coordinated activities. This example is part of the numerous CT activities the NTAS process leverages in support of the DHS CTAB and other members of the HSE.

In addition to the previously cited DHS actions for the bombing, the DHS report, *Boston One Year Later*, further reflects other DHS CTAB coordinated and NTAS process supported activities:

> [DHS] OPS [Office of Operations Coordination and Planning] and I&A [Intelligence and Analysis], together with other DHS components, immediately began working on what was known in order to keep DHS officials, stakeholders, law enforcement, and the wider public informed.

---

[137] *Senate Committee on Homeland Security and Government Affairs, Ten Years after 9/11*.

[138] *Why Can't DHS (Homeland Security Department) Better Communicate with the American People?: Before the U.S. House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency*, 113th Cong., 8 (2013) (statement of Mr. Robert Jensen, Principal Deputy Assistant Secretary, Office of Public Affairs, U.S. Department of Homeland Security).

> The DHS National Operations Center (NOC) began immediate notification and communications support…the DHS Crisis Action Team initiated National Level Reporting…displayed and shared on the DHS Common Operating Picture. The NOC facilitated communication requests between the Boston Mayor's Office and several DHS components…and leveraged its close working relationship with the Boston Police Department. I&A activated the Intelligence Crisis Action Team (ICAT) to analyze and confirm information regarding the incident. Later, the ICAT expanded to a DHS Threat Task Force to include representatives from CBP, FEMA, ICE, NPPD, OPS, TSA, USCG, USCIS and USSS…assuming other law enforcement and Intelligence Community support responsibilities. The Task Force published a twice-daily common intelligence picture of vetted all-source reporting and actions for internal dissemination within DHS and to inform external engagements. I&A and FBI published three unclassified Joint Intelligence Bulletins for use by law enforcement, covering confirmed aspects of the investigation, including details about the explosive devices and protective measures for use by law enforcement.[139]

An NTAS generated alert was not issued. However, it is clear that information and intelligence was effectively shared in other methods or pathways. Therefore, effective warning and decision advantage was facilitated through the NTAS process and the DHS CTAB.

2. Theory of Preventive Action

In the case of the Boston Marathon bombing, the Tsarnaev brothers were able to achieve surprise and successfully conduct their attack. As noted earlier, the paradox of strategic warning proves instructive to understanding what enhanced the likelihood of the Tsarnaevs' enjoying the element of surprise for their attack. This case study noted there was sufficient information available to potentially identify a developing threat and provide specific warning to receptive decision-makers; thereby, potentially mitigating this attack. According to the theory of preventive action, this equates to a failure of effective warning for officials in order to take necessary measures to prevent the attack.

As the OIG report and congressional lessons learned report for this incident reflect, the Tsarnaevs' radicalization combined with Tamerlan's travel and the two

[139] Department of Homeland Security, *Boston One Year Later: DHS's Lessons Learned*, 8.

brothers' other activities, presented an opportunity for warning and potentially for receptive decision makers to take steps in mitigating this threat. Unfortunately, this did not happen, and the Tsarnaevs' were able to successfully conduct a surprise attack on the marathon. However, after the initial attack, the case study demonstrates that officials were able to successfully capture or kill the Tsarnaev brothers. The preventive action theory provides a favorable assessment for the level of warning provided to the decision-making officials guiding the handling of the situation as well as their level of receptiveness to act on the warning information provided. This level of warning and decision advantage enabled the successful neutralization of the persistent threat posed from the Tsarnaev brothers.

3. The RPV Framework

The RPV framework states, "Organizations create value as employees transform inputs of resources—people, equipment, technology, product designs, brands, information, energy, and cash—into products and services of greater worth."[140] In keeping with the tenets of the RPV framework, the CTAB and the NTAS process assisted DHS and other HSE members with "The patterns of interaction, coordination, communication, and decision-making" sufficient to address the persistent threat.[141] Therefore, the RPV framework reveals the success of the NTAS process in addressing the continued threat from the Tsarnaev brothers in the aftermath of the initial bombing attack at the Boston Marathon. NTAS succeeded through supporting strategic level coordination of the very diverse independent actions members of the HSE conducted in dealing with the fluid challenges the Boston Marathon bombing situation presented. The NTAS process provided a sustainable and repeatable methodology for CT decision making, coordination, and communication, vis-à-vis improved decision advantage.

[140] Christensen, *The Innovator's Dilemma*, 187.

[141] Ibid.

E. CHAPTER CONCLUSION

In this case study, NTAS demonstrated its agility and its sustainability throughout the four-day situation. The NTAS process supported CT coordination in a sustainable and repeatable manner consistent with the manner in which the former DHS CT Coordinator outlined regarding previous incidents. Although an NTAS generated alert was not issued, other forms of communication, such as JIBs and press statements, were produced and utilized effectively in support of CT efforts. This sustained responsiveness is critically important in light of the consequences avoided through the timely neutralization of the Tsarnaev brothers. Consequences, as Dzhokhar Tsarnaev related "…to investigators during questioning that he and his brother at one point intended to drive to New York City and detonate their explosives in Times Square."[142] If the Tsarnaev brothers managed to change the conditions of the situation, NTAS provided the necessary flexibility to support the broadened scope of CT coordination amongst the members of the HSE. NTAS also was positioned to supply effective warning to a much broader community through an alert generated from NTAS.

Support for the Boston Marathon bombing incident demonstrates NTAS fulfills its PPD-7 mission by providing:

> A system the American public can have confidence in; Advisories that contain clear and concise language, readily understandable by the American public; Advisories that contain as detailed information as possible, without jeopardizing sources, collection methods, or an active disruption effort or investigation; Advisories that identify protective measures, where appropriate, that are tailored to specific sectors across the country, to including components of the Federal Government; State, local, and tribal government entities; critical infrastructure entities; and selected private sector partners; Advisories that have a set duration, where the information is regularly re-evaluated; and A system that is consistent and agile, where the advisories are capable of being raised or lowered quickly and efficiently.[143]

[142] Jerry Markon, Sari Horwitz and Peter Finn, "Authorities: Tsarnaev Brothers Planned Attack on New York's Times Square," *The Washington Post* April 26, 2013.

[143] Executive Office of the President, *Presidential Policy Directive/PPD-7*.

NTAS is a consistent and agile system as it supplies a durable and flexible methodology in accomplishing its mission. For these reasons, NTAS is an effective terrorism warning system capable of providing sufficient warnings. It also provides decision advantage to decision makers at every level of the HSE and the American public.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS

This research topic required a qualitative approach in answering the research questions. Case studies for the two U.S. terrorism warning systems support the standard comparative analysis method. The assessment framework for this method relied upon a standardized panel of questions and two additional theories (RPV framework and theory of preventative action). The RPV framework assessed the process or functional aspects of each warning system. The theory of preventive action supported assessment of the decision advantage provided from the systems.

Two major themes spring from this body of research in response to the primary and secondary research questions: functional effectiveness and decision advantage. The first theme relates to the functional effectiveness of a terrorism warning system. Terrorism warning systems address a complex problem set due to the adaptability of the deliberate human threat these systems face. These systems provide warnings for internal (organizational or for official decision-makers) and external (other partner organizations or the public) categories of constituents. They must support resolution of the decision maker's dilemma, balancing between the need to warn people in danger from terrorism with the need to maintain OPSEC for CT efforts mitigating that danger. A system is effective if it capably fulfills these two thematic functions related to providing warning and decision advantage.

The functional effectiveness theme directly correlates to the second theme evident in this research. The second theme, decision advantage, embodies the level of trust or confidence the system sustains from the organizations and people it serves. This confidence factor demonstrates the belief level attributed to the system, which translates into the level of responsiveness or willingness to take action the system generates with its warnings or decision advantage efforts.

A. FUNCTIONAL EFFECTIVENESS

Table 3 presents the combined assessment results for both HSAS and NTAS. Reflected in the Christmas Day bombing case study and the numerous reports and studies cited thus far, HSAS did not maintain or function with any tenet of an effective terrorism warning system. It did not provide timely detailed threat information, nor did it provide clear and understandable protective actions. Furthermore, it failed to provide a clear duration of a period of threat. Additionally, it was not consistent in changing the color-code levels. Finally, it also failed to provide decision advantage. The results, reflected in Table 3, further demonstrate the HSAS failures in maintaining a methodology to warn and provide decision advantage. In reports, surveys and testimony concerning HSAS, it is clear that HSAS created more confusion amongst decision makers than it provided decision advantage. After over six years of using HSAS, these combined factors of systemic ineffectiveness resulted in a widespread loss of confidence in the system. This ineffectiveness resulted in the continued marginalization of HSAS as a terrorism warning system. HSAS was so ineffective that it was not central in addressing a clear incident of terrorism in December 2009.

Table 3. NTAS/HSAS Comparison System Characteristics Matrix

System Characteristic	HSAS	NTAS	Comparative Evaluation
Management of system established?	No	Yes	HSAS had no formal management system. NTAS had established management through designating the CT Coordinator and chartering the CTAB.
Was management of system sustained, durable, and effective?	No	Yes	Not applicable for HSAS. Noted in testimony and lessons learned reporting, the CTAB functioned well for NTAS.
Was there a defined decision making process utilized to reach a decision?	No	Yes	HSAS had no defined decision making process was utilized. As directed in PPD-7, the NTAS provided this process.
Was the decision making process sufficiently effective?	No	Yes	Several cited reports, testimony and assessments provide evidence that HSAS supported decision making was ineffective. NTAS proved effective decision advantage, supporting strategic CT coordination, communication and decision making.
Was the decision making process sustainable in	No	Yes	Not applicable for HSAS. In two noted terrorism situations, NTAS provided

System Characteristic	HSAS	NTAS	Comparative Evaluation
providing a repeatable and consistent method of reaching a decision?			repeatable and consistent decision support.
Was the decision making process timely in supporting the situation?	No	Yes	Not applicable for HSAS. NTAS met its 24 hour a day and seven day a week mission support requirement. Noted in the Boston incident, NTAS was immediately executed within minutes of the explosions.
Was the decision making process sufficiently adaptable to provide effective decision support for situations anticipated and unanticipated and/or deliberate/non-deliberate?	No	Yes	Not applicable for HSAS. NTAS adapted to the fluid Boston Marathon bombing tempo.
Was there a decision making body designated to make this decision?	No	Yes	Presidential Directives named cabinet level officials responsible for collaborating on these decisions. However, no formal decision making body was chartered for HSAS. For NTAS the CTAB is the chartered decision making body.
Was it necessary for a designated decision-making body to exist?	Yes	Yes	This presented a major gap in HSAS. As proved in the failures of HSAS, a designated decision making body is needed. The successful application of a designated body in support of NTAS provides evidence of how detrimental this gap was for HSAS.
Was there a defined convening process for gathering the decision makers together?	No	Yes	Several cited reports and assessments note the lack of defined process for HSAS. The NTAS Process provides this convening process, in accordance with written NTAS *Concept of Operations* and standard operating procedures.
Was this convening process timely and sustainable when the situation required multiple decisions over the course of extended periods?	No	Yes	Several cited reports, testimony and assessments provide a cumulative picture of the lack of sustainability and timeliness in HSAS supported decision making. The NTAS Process supported multiple CTAB meetings and other operation tempo requirements throughout the four day Boston Marathon bombing incident.
Based upon the outcome of the original decision, was the decision making process sufficient in supplying decision advantage to subsequent decision makers dealing with the situation?	No	Yes	Cited reports, testimony and assessments note that the HSE at large was often confused by HSAS decisions. This created cascading failures in decision making at every level of the HSE. As noted in testimony and lesson learned reports, the strategic coordination and decisions from

System Characteristic	HSAS	NTAS	Comparative Evaluation
			NTAS positively supported downstream decisions and actions dealing with the situation.
Was this system the only or principal decision support pathway through which the decision reached decision makers?	No	Yes	HSAS was not the only or even principle system toward the end of its service life. The NTAS Process provided the principal pathway.
Did the system support original and secondary decision makers?	No	Yes	As noted in testimony and lessons learned reports, HSAS ineffectively provided decision support. However, information and guidance derived from the NTAS Process supported both groups of decision makers.
Did the system support coordination of efforts dealing with the situation?	No	Yes	As noted in testimony and lessons learned reports, HSAS did not effectively support strategic CT coordination throughout the incident; whereas, NTAS effectively performed this role.
If supporting coordination of efforts, did the system work effectively?	No	Yes	NTAS effectively supported the successful neutralization of the terrorist threat presented from the Tsarnaev brothers.
Was there a designated communication method for the dissemination of the decision?	Yes	Yes	HSAS color coded alert levels represented the principle communication method. Although an alert was not generated from the NTAS process, JIBs, press statements and other direct forms of communication were utilized as part of the flexible NTAS process for the Boston Marathon bombing.
Was the decision communicated effectively?	Yes	Yes	HSAS color coded alerts minimally communicated threat level changes. However, as noted in reports and testimony, these color code changes were neither well detailed nor contained enough specificity for decision makers to effectively utilize. NTAS facilitated effective communication from the first few minutes until the concluding moments of the incident.

On the other hand, NTAS continues to function in keeping with the tenets of an effective terrorism warning system, which are listed above as HSAS points of failure. These tenets are demonstrated in the Boston Marathon bombing case study. The NTAS supported effective warning through the provision of communication tools, such as JIBs, etc. In support of the ongoing investigation, it provided decision advantage to the CTAB and other senior leaders throughout the four day incident. It was also positioned to

provide broader support to the larger HSE community and the public, if the Tsarnaev brothers managed to escape authorities and put other areas under threat.[144] Since its inception in 2011, the system continues to provide a durable and sustainable process critical for success as a terrorism warning system. As shown in Table 3, when assessed with the standard panel of questions the NTAS results reflect this reality. It is also demonstrated in the comments provided from Mr. Beers concerning the 2011 Osama Bin Laden raid.[145]

1. The RPV Framework

Christensen's RPV framework evaluates three factors indicating an organization, system, etc. is capable in accomplishing its goals. These factors are resources, processes and values. Resources "are usually *things*, or *assets*…,"[146] and processes are "[t]he patterns of interaction, coordination, communication, and decision-making…."[147] Additionally, values are, "the criteria by which decisions about priorities are made."[148] The RPV framework assesses the requirements of a job and then matches the job with an individual, process, etc. capable of accomplishing that job successfully.

(1) HSAS

The HSAS suffered from poorly defined process or methodology. The patterns of interaction, coordination, and decision making for HSAS were not repeatable or durable. The RPV framework states: "Organizations create value as employees transform inputs of resources—people, equipment, technology, product designs, brands, information, energy, and cash—into products and services of greater worth."[149] As reported to the U.S. Congress, HSAS did not establish this RPV success requirement. It did not have a defined methodology or even a designated group of decision makers, who were

[144] In the HSE, this is the collection of decision makers or groups from the individual citizen up to the most senior policy maker.

[145] *Senate Committee on Homeland Security and Government Affairs, Ten Years after 9/11*.

[146] Christensen, *The Innovator's Dilemma*, 186.

[147] Ibid., 187.

[148] Ibid., 188.

[149] Ibid., 187.

consistently involved in these decisions. This lack of methodology bespeaks a lack of a management capacity. This lack of a management capacity means that HSAS was dependent upon the individuals, who were coincidentally responsible for operating the system whenever it was needed. This fact is demonstrated throughout its performance history, and it is highlighted in the Christmas Day bombing case study by the fact that it served no central role for any party involved with the incident.

The results of this type of approach are predictable. According to the RPV framework, an organization that relies solely on the competency of the individuals operating a system without the benefit of a defined process is doomed to fail. Christensen explains this maxim of the RPV framework in this way:

> Frequently, they [the organization] assume that if the people working on a project individually have the requisite capabilities to get the job done well, then the organization in which they work will also have the same capability to succeed. This often is not the case.[150]

This lack of consistent process was identified in previous GAO reports as well as in the HSAC Task Force review of the system.

Due to a lack of methodology, such as management, defined process, and organizational values, the HSAS relied too heavily on individual performances in order to accomplish the collective organizational mission of HSAS. The HSAS did not maintain a consistent repeatable methodology for warning (color code change) or in providing decision advantage (no designated decision-making body, etc.). This resulted in the outcome Christensen forecasts[151] for any organization or system overly reliant on individual performance—repeated failure.

However, HSAS did maintain a successful grant funding authorization capability. This capability provided jurisdictions, "funds for necessary operational overtime costs in response to an increase in threat level under the HSAS."[152] These jurisdictions applied

---

[150] Ibid., 185.

[151] Christensen, *The Innovator's Dilemma*, 185–208.

[152] Elizabeth M. Harmon, "Impact of National Terrorism Advisory System on Homeland Security Grant Programs," Grants Program Directorate Information Bulletin no. 367 (Washington, DC: Federal Emergency Management Agency, 2011).

for reimbursement authorization through the DHS FEMA Grants Program Directorate. Once approved, these jurisdictions could utilize currently available grant funds awarded to their State, locality, urban area or tribe in order to reimburse related overtime expenses. This funding authorization capability transitioned to NTAS when it replaced HSAS.

(2) NTAS

The NTAS and the CTAB successfully demonstrate this RPV hallmark of success. The NTAS and CTAB provide sufficient management, defined process and organizational values. Unlike HSAS, it is not overly reliant upon individual performance, because it provided internal controls through a chartered decision-making body as well as concept of operations and standard operating procedures documents. In keeping with the tenets of the RPV framework, the CTAB and the NTAS process empowers DHS and other HSE members with "The patterns of interaction, coordination, communication, and decision-making…" sufficient to address the persistent threat.[153]

The NTAS is positioned for success because it improves the level of CT focus for the organizations and decision makers it serves. This focus derives from a well-defined process and effective management by the DHS CT Coordinator and the CTAB. Christensen articulates this critical success of NTAS where HSAS failed: "This is why focused organizations perform so much better than unfocused ones: their processes and values are match carefully with the set of tasks that need to be done."[154] Therefore, the RPV framework reveals the success of the NTAS process in addressing the continued threat from the Tsarnaev brothers in the aftermath of the initial bombing attack at the Boston Marathon. NTAS succeeded in focusing DHS and its decision makers throughout the incident. It accomplished this through supporting strategic level coordination of the diverse independent actions members of the HSE conducted in dealing with the fluid challenges the Boston Marathon bombing situation. This improved CT focus is a direct result of the NTAS because it provides a sustainable and repeatable methodology for CT

[153] Christensen, *The Innovator's Dilemma*, 187.

[154] Ibid., 197, 286.

decision making, coordination, and communication, vis-à-vis improved decision advantage.

2. Trust and Confidence Level

As experts argue, engendering and sustaining trust and confidence is a terrorism warning system's central task. It is critical that a terrorism warning system enjoy the trust and confidence of the organizations and people it serves. These constituents fit into two categories: internal and external. The internal category consists of the officials and organizations performing CT efforts to counter the threat of terrorism. The external category consists of those who are in danger and benefit from the advisories of the terrorism warning system.

HSAS suffered a downward trajectory of trust and confidence clearly demonstrated in over six years of performance history and numerous reports and congressional testimony. Inconsistent methodology for its usage as a warning system and in how it provided little decision advantage resulted in this low trust and confidence level amongst both constituent categories. The Christmas Day bombing case study presented the low ebb on this downward trajectory for the system. By 2009, it was so marginalized from the decision-making process and in supporting CT efforts the system did not play any role in addressing this situation. Emblematic of this lack of trust and confidence, Secretary Napolitano requested the HSAC Task Force review the system, which ultimately resulted in its decommissioning and complete replacement in 2011.

Despite the failure of HSAS as a terrorism warning system, it provided three useful services. First, it maintained a level of visibility concerning the threat of terrorism. It supplied a funding vehicle through which affected jurisdictions could receive reimbursement for operating costs. Secondly, it served as a source of lessons learned in developing its successor NTAS. HSAS did provide some decision advantage to the HSAC Task Force. As the task force analyzed the system and its performance, it represented the tenets of what a terrorism warning system should be in displaying all that it was not.

Unlike HSAS, the NTAS enjoys sufficient trust and confidence amongst the internal category of constituents. This conclusion is supported from the NTAS performance during the 2013 Boston Marathon bombing case study as well as from the collective weight of public statements and testimony about the system's performance at other times.

The NTAS maintains sufficient trust and confidence amongst the internal category, but it is difficult to assess the level of trust and confidence among the external category. NTAS has never issued a public alert. Subsequently, these external constituents do not have any experience with the system and therefore sufficient familiarity with the system. This lack of experience creates a possible credibility gap due to a lack of understanding amongst members of the external category.

Within this theme, a lack of understanding of the role of NTAS and its functions seems to emerge regarding the external category of constituents. Billy Hallowell's comment reflects this:

> To date, though, no practical information has been disseminated through the NTAS system. If its creation was intended to alert the public about credible and important information regarding threats, then one must assume that there has either been no legitimate information about threats intercepted by the government since its official adoption in April 2011—or that the system is simply not being used.[155]

This lack of understanding potentially creates an undue focus upon the issuance of an alert and not on the real "heart" of the system, which is the coordination process used to make it work. This misplaced focus creates a misperception that the NTAS is not working, when in fact, it is working as intended. This potentially casts doubt about the system within external category of decision-makers. This doubt may cause a lack of sufficient responsiveness to any alert issued from the system to this category, such as a public NTAS alert.

---

[155] Billy Hallowell, "Looking for Gov't-Issued Terror Alert? DHS Has Never Used its 'Terrorism Advisory System' (Here's the Evidence)," *The Blaze*, April 18, 2013, http://www.theblaze.com/stories/2013/04/18/dhs-has-never-sent-an-alert-through-its-terrorism-advisory-system-even-following-the-boston-terror-attack

3. Preventive Action Theory

Dr. Erik Dahl's theory of preventive action seeks to explain how to avoid surprise attacks from occurring. In his explanation of the theory's application, Dr. Dahl states, "If intelligence is to be most useful in preventing major surprise attacks, it must provide specific, tactical-level warning, and policymakers must be receptive to that warning."[156] Although a terrorism warning system is not strictly an intelligence mechanism, it is certainly a pathway through which decision makers receive intelligence and other types of inputs when making a CT decision regarding terrorism.

Decision makers who employ the national terrorism warning systems, such as HSAS or NTAS, reside at the highest strategic level. Subsequently, these national level systems face a difficulty in achieving decision advantage for these decision-makers. Dr. Dahl states, "This is the paradox of strategic warning. Policymakers, especially at senior levels, typically say they want strategic intelligence; but…they are less likely to respond to long-range, broad assessments than they are to specific, tactical-level warnings."[157] The difficulty is in sufficiently providing them the specific, tactical-level warning at this strategic level. Moreover, terrorism warning systems must provide warning in a manner that fosters sufficient decision makers' trust and confidence to effectively employ the warning system. It is this level of decision makers' trust and confidence that Dr. Dahl refers to as "receptivity."[158] Therefore, according to preventive action theory, if the system sufficiently provides warning and it sustains sufficient decision makers' trust and confidence decision advantage is possible. When decision advantage is achieved for "receptive" decision makers, Dr. Dahl's studies conclude this positive outcome, "when warning has been specific, and policymakers have been receptive, attacks have been successfully prevented."[159]

The RPV framework examined the warning aspect or functional effectiveness theme of this research for HSAS and NTAS. The preventive action theory examined the

---

[156] Dahl, *Intelligence and Surprise Attack*, 176.

[157] Ibid., 177.

[158] Ibid., 175–184.

[159] Ibid., 176.

trust and confidence aspect of each system. This is important, because if a system engenders sufficient trust and confidence in decision makers, it is more likely to be successful in accomplishing its role in CT efforts.

(1) HSAS

An assessment of HSAS with the preventive action theory reveals the following critical shortcomings that generated a clear lack of trust and confidence in this system. HSAS lacked a defined and repeatable decision-making process. A consistently receptive decision-making body designed to function strictly in a CT capacity did not exist for HSAS. This combined lack of a consistent decision making process and designated CT decision-making body played a role in the mercurial results of the HSAS.

Directed in HSPD-3 and HSPD-5, the decision makers consisted of a small group of the most senior policymakers in the USG, the President of the United States, the Attorney General, and the DHS Secretary. The level of HSAS usage over the course of its history from 2002–2011 demonstrates a clear fluctuation in decision makers' receptivity and confidence in HSAS. From its inception in March 2002 until August 2006, 16 changes to the color codes occurred. However, during the last year of the Bush administration no changes occurred. What is particularly telling is that after the presidential administration transition in 2008, HSAS remained inert until its replacement by NTAS in April 2011. This is despite at least two clear terrorist attacks occurring after transition, the 2009 Najibullah Zazi and Christmas Day bomber terrorist incidents. This demonstrates a clear degradation of decision makers' confidence for HSAS.

It also consistently failed to provide a reliable pathway for detailed and timely information in support of senior decision makers' needs. Consequently, this lack of trust impaired decision making at all levels of the HSE; which in turn, sowed a great deal of confusion amongst the members for the HSE in coordinating, communicating, or executing appropriate countermeasures. This means HSAS never consistently provided

warning or successfully addressed the paradox of strategic warning.[160] Consequently, HSAS did not consistently provide decision advantage to HSE decision makers.

(2) NTAS

In the case of the Boston Marathon bombing, the Tsarnaev brothers achieved surprise and successfully conducted their attack. Erik Dahl's paradox of strategic warning proves instructive to understanding what enhanced the likelihood of the Tsarnaevs' enjoying the element of surprise for their attack. This case study noted there was sufficient information available to potentially identify a developing threat and provide specific warning to receptive decision makers, thereby, potentially mitigating this attack. According to the theory of preventive action, this equates to a failure of effective warning for officials in order to take necessary measures to prevent the attack. The OIG report and congressional lessons learned report for this incident reflect, the Tsarnaevs' radicalization combined with Tamerlan's travel and the two brothers' other suspicious activities, presented an opportunity for warning and potentially for receptive decision makers to take steps in mitigating this threat. Unfortunately, this did not happen, and the Tsarnaevs' were able to successfully conduct a surprise attack on the marathon.

There is a theoretical failure presented in the Boston Marathon bombing case study. DHS personnel from at least one component were directly involved in the run-up to the incident. It appears that some of this information did not flow up to decision makers. This indicates a potential NTAS process failure in providing pre-incident information. Moreover, this information could have resulted in sufficient decision advantage to take potentially mitigating actions. Since this conclusion is hypothetical in nature, it is difficult to ascertain with any certainty what this alternative outcome may have looked like. However, after the initial attack, the case study demonstrates that officials were able to successfully capture or kill the Tsarnaev brothers. Subsequently, the preventive action theory provides a favorable assessment for the level of warning NTAS provided to the decision-making officials guiding the handling of the situation as well as

[160] This paradox contributes to the likelihood terrorist attacks succeed, because decision makers lack the type of detailed timely information necessary to prevent a terrorist attack.

their level of receptiveness to act on the warning information provided. This enabled the successful neutralization of the persistent threat posed from the Tsarnaev brothers.

B. CHAPTER CONCLUSION

Thematically, these two systems addressed the same complex terrorism problem set. However, they did so in different manners. From a functional effectiveness perspective, HSAS presented a more inflexible and static system, while NTAS demonstrates a flexible and responsive system. The systems resided on polar ends of the trust and confidence level spectrum. HSAS inspired little trust and confidence; conversely, NTAS enjoys a sufficient level of trust and confidence. As a result of this qualitative analysis, NTAS is an effective warning system and provides sufficient decision advantage. However, NTAS does have detractors in the external constituent group. These detractors do wonder why alerts are not issued readily and conclude that NTAS is not functioning well. This stems more from a lack of understanding on the detractors' part more than from a systemic failure of NTAS.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

This chapter includes the interpretations and conclusions distilled from this research effort. It presents a discussion of the research, its limitations, recommendations for future research and conclusions and/or recommendations for NTAS.

A. DISCUSSION

This research effort sought to answer two questions: How effective is the NTAS, when compared to its predecessor the HSAS. A secondary research question is: Does NTAS provide sufficient decision advantage for the nation it serves? This research examined the mechanics of a terrorism warning system to attain an improved understanding of how such a warning system functions effectively. This was achieved through validating or invalidating the hypothesis that the NTAS provides an improved system in support of CT decision making, coordination, and communication.

B. LIMITATIONS

This research remained limited to examining the United States use of terrorism warning systems over the past 13 years. As the current NTAS Coordinator, a clear limitation is the level of bias my position presents to any reader of this research.[161] Consideration of classification and handling restrictions for some of the research information presented another limitation.

Clearly, my position affords me unparalleled access to the inner workings of NTAS and how it is utilized. It also provides me a unique perspective regarding the topic of decision advantage in using terrorism warning systems. It offers insight into why these decisions were made. However, this level of closeness to NTAS also generated a certain level of bias, which at times, made it difficult to balance with sufficient objectivity. The

[161] As noted on page 1, the author is the current NTAS Coordinator for DHS. In this role he works for the DHS CT Coordinator in the Office of the CT Coordinator. This office coordinates CT functions for the department and supports the DHS CT Coordinator in advising the DHS Secretary on CT issues and incidents.

academic rigor of the Naval Postgraduate School thesis process and the thesis advisory faculty proved to be invaluable in the mitigation of any bias.

Maintaining the broadest extent of availability for this research presented the other challenge. Limiting the research to openly available information proved the biggest obstacle. Attaining official release of more sensitive information for this research was granted; however, utilizing this information incurred the cost of severely restricting access to it. After careful consideration, the benefits of including the sensitive information did not outweigh the costs of restriction. Additionally, the objectives of this research could be achieved without this sensitive information.

C. RECOMMENDATIONS FOR FUTURE RESEARCH

A deeper comparative analysis of terrorism warning system usage in the broader context of how the international community uses these systems would prove insightful. This type of study could serve to advance better understanding of the themes recognized in this research: functional effectiveness and decision advantage. This could validate the tenets of these warning systems derived from the literature review conducted in this research or reveal other principles not accounted for here. This research may also reveal trends in how other governments that face a greater frequency of terrorist attacks approach terrorism warning system usage. This would answer research questions, such as: "Are nations faced with a higher frequency of terrorist attacks more or less likely to issue warnings? If so, how broadly is this warning provided: the general public or only to public officials?"

Conducting a survey of officials responsible for utilizing terrorism warning systems could validate the decision advantage conclusions from this research or advance discovery of other decision-making factors not considered. Since this survey would evaluate national level systems, this prompts the need to interview leaders from the international community who maintain such a system. In addition, a survey of officials who receive and act on warnings could provide an updated analysis regarding the value of these systems. This survey would involve officials from different levels of government, responsibility, or infrastructure sector within the HSE, such as state

homeland security advisors, mayors of major urban areas, county managers, or private sector leaders.

D. CONCLUSIONS

This research confirms that NTAS is a viable system, which effectively employs the terrorism warning system tenets noted in the literature review. NTAS is also a valuable tool in the strategic homeland security inventory for keeping this nation safe. It clearly provides a flexible option for communicating information related to terrorism. Unlike its predecessor HSAS, NTAS is not merely another form of static color-coded alerting. Instead, the system "advises" the public and other members of the HSE in a detailed manner on decisions they need to make and subsequent actions they should consider. Beyond its role as an advisory system, the NTAS process effectively supports strategic CT coordination within DHS and it incorporates every partner from within the HSE as the situation dictates. The combined decision making agility and execution authority, embodied in the DHS CT Coordinator and CTAB, is the fulcrum point for NTAS as well as the system's greatest strength. It also continues to effectively position the federal government's ability to implement the president's guidance in PPD-7, "providing a system in which the American citizen can have confidence."[162]

The NTAS process provides improvement in coordinating CT efforts by supporting the DHS CT Coordinator and the DHS CTAB. The NTAS responsibly communicates information with HSE partners regarding terrorism incidents or other CT issues not inherently designed for public consumption like an NTAS generated public alert. This communication may occur through other products, such as JIB, etc.[163] The NTAS process also maintains the capability to issue its own formal alert in order to provide timely detailed information, which is in keeping with the recommendations of the HSAC Task Force.

---

[162] Executive Office of the President, *Presidential Policy Directive/PPD-7*.

[163] Interagency Threat Assessment and Coordination Group, *Intelligence Guide*, 29.

Although the NTAS remains a key capability for DHS, the members of the HSE, and the American public, improvements remain for this system. The following steps include recommended measures to ensure continued success of this capability:

(1) Renew the DHS CTAB Charter or other appropriate governance documents, which ensure the necessary combined decision making and execution authority for NTAS.

(2) Fulfill HSAC Task Force Recommendation 6 and formally establish an Office of Counterterrorism Coordination, which will provide necessary staffing and budgetary sustainability. This permanent office will ensure effective support for the CTAB as well as coordinate CT counter-measures and other CT related functions of the department, such as NTAS.

(3) Refine the NTAS *Concept of Operations* to better demonstrate the system's scalable outcomes other than a NTAS generated alert, such as Joint Intelligence Bulletins, Joint Threat Assessments, etc.

(4) Continue to improve communication aspects of NTAS and integrate with other warning systems, such as the Integrated Public Alert and Warning System (IPAWS).[164]

(5) Continue to conduct NTAS related outreach and education efforts with the HSE and the public.

In closing, NTAS embodies the necessary teamwork aspect of homeland security also noted in the literature review. The following statement represents the vision of former DHS Secretary Napolitano regarding how NTAS also fosters a broader sense of teamwork, "As I said, this new National Terrorism Advisory System is built on the common-sense belief that we are all in this together, and that we all have a role to play."[165] Therefore, the NTAS and its process, lives up to this vision and effectively fulfills its role as an effective terrorism warning system.

[164] Damon Penn, Antwane Johnson, and Wade Witmer, "Integrated Public Alert & Warning System," Federal Emergency Management Agency, September 20, 2013, https://www.fema.gov/integrated-public-alert-warning-system

[165] Napolitano, "State of America's Homeland Security Address."

LIST OF REFERENCES

Baylis, John, James J. Wirtz, and Colin S. Gray. *Strategy in the Contemporary World: An Introduction to Strategic Studies*. 4th ed. Oxford, United Kingdom: Oxford University Press, 2013.

Bell, Stewart. "The Canadian Who Converted to Jihad: Boxer Turned Militant Killed in Dagestan." *National Post*. August 20, 2012. Accessed July 14, 2014. http://news.nationalpost.com/2012/08/20/dagestan/

Bram, Jason, Andrew Haughwout, and James Orr. "Further Observations on the Economic Effects on New York City of the Attack on the World Trade Center." *Peace Economics, Peace Science and Public Policy* 15, no. 2 (2009): 1–22. http://www.heritage.org/research/reports/2012/01/a-comprehensive-suspicious-activity-reporting-sar-system-requires-action

Bongar, Bruce, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, and Philip G. Zimbardo, eds. *Psychology of Terrorism*. New York: Oxford University Press, 2007.

Carafano, James J., and Jessica Zuckerman. "The Current Threat Level: Ending Color-Coded Terror Alerts." Memo #3068. November 30, 2010. The Heritage Foundation. Accessed March 15, 2014. http://www.heritage.org/research/reports/2010/11/the-current-threat-level-ending-color-coded-terror-alerts?ac=1

Christensen, Clayton M. *The Innovator's Dilemma: The Revolutionary Book that Will Change the Way You do Business*. New York: Harper Business, 2011.

Cullison, Alan, Paul Sonne, and Jennifer Levitz. "Life in America Unraveled for Brothers." *Wall Street Journal (Online)*. April 20, 2013. http://online.wsj.com/news/articles/SB10001424127887323809304578432501435232278

Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond*. Washington, DC: Georgetown University Press, 2013.

Dalmia, Shikha. "What Islamist Terrorist Threat? Al Qaeda Doesn't Have What It Takes to Hurt America." February 15, 2011. Accessed July 4, 2014. http://reason.com/archives/2011/02/15/what-islamist-terrorist-threat

Department of Commerce, Office of the Federal Coordinator for Meteorological Services and Supporting Research. *National Hurricane Operations Plan* (FCM-P12-2013). Washington, DC: U.S. Department of Commerce, 2013.

Department of Homeland Security. *Boston One Year Later: DHS's Lessons Learned*. Washington, DC: Department of Homeland Security, 2014.

———. "Chronology of Changes to the Homeland Security Advisory System." Accessed July 29, 2014. http://www.dhs.gov/homeland-security-advisory-system

———. *NTAS Public Guide*. April 2011. http://www.dhs.gov/ntas-public-guide

———. *Prepared Statement Regarding NTAS During Boston Marathon Bombing*. Washington, DC: Office of Public Affairs, 2013.

———. *Quadrennial Homeland Security Review*. Washington, DC: U.S. Department of Homeland Security, 2010.

Department of Justice, Office of Community Oriented Policing Services. *Community Oriented Policing Defined*. Washington, DC: Department of Justice, 2009.

Dimock, Michael, Carroll Doherty, and Alec Tyson. *Most Expect 'Occasional Acts of Terrorism' in the Future: Six-in-Ten Say Post-9/11 Steps Have Made Country Safer*. Washington, DC: Pew Research Center for the People & the Press, 2013. http://www.people-press.org/2013/04/23/most-expect-occasional-acts-of-terrorism-in-the-future/

Erickson, Scott, and Matt Mayer. *A Comprehensive Suspicious Activity Reporting (SAR) System Requires Action*. Washington, DC: The Heritage Foundation, 2012.

Executive Office of the President. *Homeland Security Presidential Directive/HSPD-3*. Washington, DC: The White House, 2002.

———. *Presidential Policy Directive/PPD-7*. Washington, DC: The White House, 2011.

Friedman, Benjamin H. "Do Terrorism Warnings Work?" *The National Interest* [blog]. October 13, 2010. Accessed April 5, 2014. http://nationalinterest.org/blog/the-skeptics/do-terrorism-warnings-work-4214

General Accounting Office. *Internal Control Standards for Internal Control in the Federal Government*. Washington, DC, General Accounting Office, 1999.

Hallowell, Billy. "Looking for Gov't-Issued Terror Alert? DHS Has Never Used Its 'Terrorism Advisory System' (Here's the Evidence)." *The Blaze*. April 18, 2013. http://www.theblaze.com/stories/2013/04/18/dhs-has-never-sent-an-alert-through-its-terrorism-advisory-system-even-following-the-boston-terror-attack

Hobijn, Bart, and Erick Sager. "What Has Homeland Security Cost? An Assessment: 2001–2005." *Current Issues in Economics and Finance* 13, no. 2 (2007): 1–7.

Homeland Security Advisory Council. *Homeland Security Advisory System Task Force Report and Recommendations*. Washington, DC: U.S. Department of Homeland Security, 2009.

———. *HSAS Survey Report*. Washington, DC: U.S. Department of Homeland Security, 2009.

———. *Stakeholder Feedback Report*. Washington, DC: U.S. Department of Homeland Security, 2009.

Interagency Threat Assessment and Coordination Group. *Intelligence Guide for First Responders*. 2nd ed. Washington, DC: Interagency Threat Assessment and Coordination Group, 2011.

Jenkins, William O. *Homeland Security Advisory System: Preliminary Observations Regarding Threat Level Increases from Yellow to Orange*. Washington, DC: General Accounting Office, 2004.

Jones, Seth G. *A Persistent Threat: The Evolution of Al Qaida and Other Salafi-Jihadists*. Santa Monica, CA: RAND Corporation, 2014.

Kunreuther, Howard C. "Risk Analysis and Risk Management in an Uncertain World." *Risk Analysis* 22, no. 4 (2002): 655–664.

Lauter, David. "Poll: Terror Acts 'Part of Life' in America." *Spokesman Review* (Spokane, WA). April 24, 2013. Sec. A.

Leopold, J. D. "Army Releases New OPSEC Regulation." U.S. Army, April 19, 2007. Accessed September 4, 2014. http://www.army.mil/article/2758/army-releases-new-opsec-regulation/

Levine, Mike, and Lee Ferran. "Boston One Year Later: DHS's Lessons Learned." *ABC News* [blog]. April 10, 2014. Accessed May 2, 2014. http://abcnews.go.com/blogs/headlines/2014/04/boston-marathon-bombing-homeland-securitys-lessons-learned/

Markon, Jerry, Sari Horwitz, and Peter Finn. "Authorities: Tsarnaev Brothers Planned Attack on New York's Times Square." *The Washington Post*. April 26, 2013.

Mattingly, Phil, Roxana Tiron, and Margaret Talev. "Officials Study Brothers' Islam Ties; Pair Allegedly behind Boston Marathon Attack were Said to be Drawn to Radical Islam on Internet." *Charleston Daily Mail* (West Virginia). April 25, 2013. Sec. News.

McCauley, Clark. “Radicalization of Tamerlan and Dzhokhar Tsarnaev.” *Psychology Today* [blog]. April 19, 2013. http://www.psychologytoday.com/blog/friction/201304/radicalization-tamerlan-and-dzhokhar-tsarnaev

Moghaddam, Fathali M. *From the Terrorists’ Point of View What They Experience and Why They Come to Destroy*. Westport, CT: Praeger Security International, 2006.

Morales, Mark. “Inside Devils’ Den Half-Eaten Meal on Table Sibs Lived Amid Squalor in Ramshackle Apt.” *New York Daily News*. April 21, 2013. Sec. News.

Mueller, John, and Mark G. Stewart. *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*. New York: Oxford University Press, Inc., 2011.

———. “The Terrorism Delusion: America’s Overwrought Response to September 11.” *International Security* 37, no. 1 (2012): 81–110.

National Counterterrorism Center. “Terrorist Identities Datamart Environment Fact Sheet.” National Counterterrorism Center. August 1, 2014. Accessed August, 10, 2014. http://www.nctc.gov/docs/tidefactsheet_aug12014.pdf

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton & Company, 2004.

Penn, Damon, Antwane Johnson, and Wade Witmer. “Integrated Public Alert & Warning System.” Federal Emergency Management Agency. September 20, 2013. https://www.fema.gov/integrated-public-alert-warning-system

Pillar, Paul R. “What Terrorism Alerts Say about Ourselves.” *The National Interest* [blog]. October 7, 2010. http://nationalinterest.org/node/4193

Priest, Dana, and William M. Arkin. *Top Secret America: The Rise of the New American Security State*. New York: Little, Brown and Co., 2011.

Rice-Oxley, Mark. “Home-Grown Terrorist Recruitment Rising, Says British Spy Chief.” *The Christian Science Monitor*. November 8, 2007.

Rothstein, Linda. “After September 11.” *Bulletin of the Atomic Scientists* 57, no. 6 (2001): 44–49.

Russel, Diane, and Ong Junio. *Report on the Attempted Bombing of Northwest Airlines Flight 253 ‘Christmas Bombing Plot.’* Singapore: Nanyang Technological University, S. Rajaratnam School of International Studies, 2010.

Serrano, Richard A. “Boston Attackers May Have Had Help, U.S. Says.” *Los Angeles Times*. May 22, 2014. http://www.latimes.com/nation/la-na-boston-bombing-20140522-story.html

Sharp, Vincent H. “Faded Colors: From the Homeland Security Advisory System (HSAS) to the National Terrorism Advisory System (NTAS).” Master’s thesis, Naval Postgraduate School.

Shapiro, Jacob N., and Dara Kay Cohen. “Color Bind: Lessons from the Failed Homeland Security Advisory System.” *International Security* 32, no. 2 (2007): 121–154.

Sims, Jennifer E., and Burton L. Gerber. *Transforming US Intelligence*. Washington, DC: Georgetown University Press, 2005.

Smith, Mike. *Warnings: The True Story of how Science Tamed the Weather*, 1st ed. Austin, TX: Greenleaf Book Group Press, 2010.

Strachan-Morris, David. “Threat and Risk: What is the Difference and Why Does it Matter?” *Intelligence and National Security* 27, no. 2 (2012): 172–186.

Strom, Kevin. *Building on Clues Successes and Failures in Detecting U.S. Terrorist Plots, 1999–2009*. Research Triangle Park, NC: Institute for Homeland Security Solutions, 2010.

“Summary of the White House Review of the Details of the December 25, 2009 Attempted Terrorist Attack.” 2009. Federal Depository Library Program. http://purl.access.gpo.gov/GPO/LPS118485

Tlisova, Fatima. “Russians Closely Monitored Boston Bombing Suspect.” *Voice of America*. May 7, 2013. Accessed July 14, 2014. http://www.voanews.com/content/tsarnaev-dagestan-bombing/1656176.html

White House. *Homeland Security Presidential Directive/HSPD-5: Management of Domestic Incidents*. Washington, DC: U.S. Government Printing Office, 2003. In Public Papers of the Presidents of the United States: George W. Bush. http://www.gpo.gov/fdsys/pkg/PPP-2003-book1/html/PPP-2003-book1-doc-pg229.htm

“Written Testimony of Department of Homeland Security Janet Napolitano for a Senate Committee on the Judiciary Hearing Titled ‘The Oversight of the Department of Homeland Security.”’ April 25, 2012. Department of Homeland Security. http://www.dhs.gov/news/2012/04/25/written-testimony-department-homeland-security-secretary-janet-napolitano-senate

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