NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WHAT ARE WE MISSING? A CALL FOR RED TEAMING WITHIN THE DOMESTIC MARITIME DOMAIN FOR ANTI-TERRORISM PROGRAMS

by

Timothy J. List

December 2015

Thesis Advisor: Rodrigo Nieto-Gomez
Second Reader: Lauren Wollman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE WHAT ARE WE MISSING? A CALL FOR RED TEAMING WITHIN THE DOMESTIC MARITIME DOMAIN FOR ANTI-TERRORISM PROGRAMS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Timothy J. List			
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**

13. ABSTRACT (maximum 200 words)

As a component of the Department of Homeland Security and the department's lead for maritime security, the Coast Guard is charged with executing the United States domestic maritime anti-terrorism program. It is critical that Coast Guard policy, plans, and tactics maintain pace with the ever-changing risks associated with terrorism.

This thesis examines alternative analysis red teaming and its potential value to the Coast Guard. Specifically, it seeks to answer how red teaming can be leveraged to enhance the value of domestic maritime anti-terrorism activities. The research reviews elements of the maritime domain and principles of red teaming, and proposes and provides implementation recommendations for a terrorism red teaming program for the domestic maritime domain.

The study revealed that a red team program would be value added to the Coast Guard for domestic maritime anti-terrorism programs. Leveraging the concept of a minimal viable program, the thesis proposes a red team program and strategy to implement the program within the U.S. Coast Guard. The suggested program would be comprised of three elements: physical red teaming, identification of future attack scenarios, and policy red teaming. The thesis further provides insight into the implementation of these programs and suggests a minimal viable program approach to establishing a terrorism red teaming program for the domestic maritime domain.

14. SUBJECT TERMS alternative analysis, red teaming, homeland security risk, domestic maritime domain, maritime terrorism, minimal viable program, social identity theory, port security, Coast Guard			**15. NUMBER OF PAGES** 83
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

WHAT ARE WE MISSING? A CALL FOR RED TEAMING WITHIN THE DOMESTIC MARITIME DOMAIN FOR ANTI-TERRORISM PROGRAMS

Timothy J. List
Commander, U.S. Coast Guard, Washington, DC
B.A., San Diego State University 1999
M.S., National Graduate School, 2005

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 2015**

Approved by: Rodrigo Nieto-Gomez
Thesis Advisor

Lauren Wollman
Second Reader

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As a component of the Department of Homeland Security and the department's lead for maritime security, the Coast Guard is charged with executing the United States domestic maritime anti-terrorism program. It is critical that Coast Guard policy, plans, and tactics maintain pace with the ever-changing risks associated with terrorism.

This thesis examines alternative analysis red teaming and its potential value to the Coast Guard. Specifically, it seeks to answer how red teaming can be leveraged to enhance the value of domestic maritime anti-terrorism activities. The research reviews elements of the maritime domain and principles of red teaming, and proposes and provides implementation recommendations for a terrorism red teaming program for the domestic maritime domain.

The study revealed that a red team program would be value added to the Coast Guard for domestic maritime anti-terrorism programs. Leveraging the concept of a minimal viable program, the thesis proposes a red team program and strategy to implement the program within the U.S. Coast Guard. The suggested program would be comprised of three elements: physical red teaming, identification of future attack scenarios, and policy red teaming. The thesis further provides insight into the implementation of these programs and suggests a minimal viable program approach to establishing a terrorism red teaming program for the domestic maritime domain.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AMSC	area maritime security committee
CF	Canadian Forces
DHS	Department of Homeland Security
FY	fiscal year
GAO	Government Accountability Office
GPS	Global Positioning System
GRT	Games Red Team
ICC	intelligence coordination center
ISPS	International Ship and Port Facility Security
IT	information technology
MSRAM	Maritime Security Risk Analysis Model
MSRO	Maritime Security Response Operations
MTS	Maritime Transportation System
MTSA	Maritime Transportation Security Act
OCONUS	outside continental United States
PSGP	Port Security Grant Program
PWCS	ports, waterways, and coastal security
RBMSRO	risk based maritime security response operations
SIT	social identify theory
SME	subject matter expert
TTP	training, techniques, and procedures
UAV	unmanned aerial vehicle

THIS PAGE INTENTIONALLY LEFT BLANK

I. AN ARGUMENT FOR RED TEAMING IN THE DOMESTIC MARITIME DOMAIN

A. INTRODUCTION

What if we had a Red Team program for the Domestic Maritime Domain?

At 8:15 AM tomorrow in New York City, a Staten Island ferry with over 4,000 people onboard makes its way across the New York Harbor heading for Manhattan. Two Coast Guard boats are conducting patrols of the harbor and are close by as the ferry goes past the Statue of Liberty. Suddenly, a "swarm" of small drones, well over 1,000, come buzzing down from the sky, hitting passengers on deck and exploding on contact. The Coast Guard boats attempt to shoot down some of the drones but are only successful in bringing down a handful of the small, maneuverable drones. Fifty or so hit a side window of the ferry's main deck, making a 4-foot hole; swarms of drones fly through the hole seeking additional passengers. Simultaneously, the same "swarm" happens to a bridge window, and kills the captain and crew piloting the vessel. The ferry veers off course and plows directly into the dock on Liberty Island, which is crowded with visitors who have just arrived to visit the Statue of Liberty. The entire attack is over in 10 minutes, which leaves 1,800 dead on the ferry, and another 200 people on the dock at Liberty Island.

Flashback to 2010: As part of a senior year capstone course of study, a Coast Guard Academy Cadet Future Scenario Red Team identifies drones/unmanned aerial vehicles (UAVs) as an emergent technology with new attack method applications within the domestic maritime domain. Several Cadets, familiar with model aircrafts and computer technology, propose that terrorists could, at some point, leverage the technical advances in these areas to attack large groups of people, undetected, from several miles away.

The team identifies potential terrorist uses for drones, and then develops potential attack scenarios based upon several terrorist organizations' narratives. The team realizes that terrorists could leverage drones to conduct surveillance prior to and during an attack, to deliver small payloads including explosive charges, and to transport equipment and weapons past security screening areas. A similar Coast Guard Academy Cadet Attributes Red Team taking that information identifies some basic characteristics that drones could have in the immediate future: control systems, distances, and payload abilities, all linked back to the identified terrorist intents. The team conducts physical testing and gathers expert solicitation quantifying the potential abilities of terrorist leveraging drone technologies.

Based on the information collected by the Coast Guard Academy teams, a Coast Guard Headquarters Policy Red Team conducts a review of Coast Guard policy guidance, operational plans, and tactics on hand to address such attack methods. The team identifies significant gaps in regulations, policy, operational plans, and tactics to counter drone use by terrorists. Based on these findings, a coordinated effort between the Coast Guard and the Federal Aviation Administration is launched resulting in laws and regulations that limit drone use in and around commercial seaports and near public beaches and other maritime recreational areas. The Coast Guard introduces laws empowering law enforcement to take action when identifying drone use in these restricted areas.

Meanwhile, the Coast Guard research and development center and Department of Homeland Security (DHS) Science and Technology Directorate launch a 3-year project to develop technologies to counter drone use by terrorist actors. By 2014, systems are deployed that allow law enforcement to take control of drones within a 2,000-yard radius of a protected target. The Coast Guard develops tactics for the use of these new technologies and establishes a standard training program for them. By early 2015, these laws, policies, plans, and tactics are in place across the United States (U.S.) domestic maritime domain.

Tomorrow: A drone swarm attack takes place in New York Harbor against a Staten Island Ferry. Coast Guard officers on the ferry and on Coast Guard boats around

the harbor activate counter drone equipment, and 5,000 small drones fall into the water 2,000 yards away from the ferry. At the same time, the New York Police Department automatically receives a Global Positioning System (GPS) location of the operator, some 15 miles away in Brooklyn. One hour later, four subjects are arrested and taken into custody. Video and GPS data from the attackers' equipment are seized and evaluated for further leads. No civilian casualties.

Is this a far-fetched science fiction story or something closer to reality?

Reports of UAV sightings and incidents are increasing within the domestic maritime domain. Cruise ships, U.S. Navy submarines, and facility owners have all reported drones overhead with no clear idea of intent or knowledge of what to do about them. A recent U.S. Army War College publication speaks directly to the potential threats UAVs present for homeland security. "The impact of even singular terrorist UAV use at this level is viewed as an immediate- and near-term problem. It may represent more of a domestic security issue than an overseas basing or deployment threat—although such weaponized devices could just as easily be utilized for terrorist purposes overseas against service personnel and their families as they could be used against civilians in the United States."[1]

In August 2015, the Federal Aviation Administration announced that it had hired "two high-level officials to help lead the agency's regulation of drone flight in the United States."[2] The positions are "designed to focus on outreach to other areas of the government and airspace stakeholders, and help create regulations to safely integrate drones into the nation's airspace."[3]

While these efforts are a step in the right direction, the timing suggests that the federal government did not identify the risks associated with drones in time to develop measures prior to the risks becoming a reality. Regulations are not in place as of this writing. Law enforcement officials currently do not have clear guidance or laws to

[1] Robert Bunker, *Terrorists and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications* (Carlisle, PA: The United States Army War College Strategic Studies Institute, 2015).

[2] Mario Trujilo, "FAA Bolsters Drone Outreach with New Hires," *The Hill*, September 2015.

[3] Ibid.

enforce regarding the use of drones in areas of security concerns. Price points and availability of drones are making this technology a reality for the general public. Payload abilities are increasing and "swarm" drone technology is quickly coming to fruition. Government efforts to establish policies, laws, and countermeasures are lagging. This thesis proposes an alternative analysis red teaming program, whose components if in place, could have identified this emergent technology and the potential impacts it might have on domestic maritime security efforts.

B. PROBLEM SPACE

The importance of DHS anti-terrorism programs cannot be overstated. Protecting U.S. citizens from the threat of terrorism is the cornerstone upon which the DHS is based. As a component of the DHS and the department's lead for maritime security,[4] the Coast Guard is charged with executing the U.S. domestic maritime anti-terrorism program via the ports, waterways, and coastal security (PWCS) mission.[5] The Maritime Security Response Operations (MSRO) Manual establishes the Coast Guard and its other agency partners' operational activity standards, such as maritime critical infrastructure and key resources visits, patrol frequencies, security zone enforcement, and vessel escort requirements.[6] This set of anti-terrorism activities, defined by policy and tactical guidance, is the U.S. government's domestic maritime anti-terrorism program.

Threats from terrorism persist and continue to evolve; attack methods are harder to predict and do not come from any one individual or group.[7] It is critical that Coast Guard policy, plans, and tactics maintain pace with the ever-changing risks associated with terrorism. As both a military and federal law enforcement organization, the Coast Guard faces the broad challenges each of these organizational structures are afflicted

---

[4] U.S. Government Accountability Office, *COAST GUARD Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations* (GAO-12-14) (Washington, DC: U.S. Government Accountability Office, 2011).

[5] "U.S. Coast Guard Port Waterways, and Coast Security," last modified October 31, 2014, http://www.uscg.mil/hq/cg5/cg532/pwcs.asp.

[6] U.S. Government Accountability Office, *COAST GUARD Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*.

[7] "Preventing Terrorism and Enhancing Security," last published August 26, 2015, http://www.dhs.gov/preventing-terrorism-and-enhancing-security.

with, including a lack of creativity for the sake of efficient execution.[8] As with any human system, the organization is fallible, susceptible to beliefs, biases, and constraints that may skew American decision making and analysis.[9] The domestic maritime security enterprise must account for this fluid environment and "address the uncertainty that frames anti-terrorism pragmatic decisions."[10]

The Coast Guard terrorism risk assessment program is one of the most highly regarded risk assessment programs in the federal government.[11] However, the elements involved have limitations, specifically in terms of the ability to conduct alternative analysis and the assessment of risk from the terrorist's point of view. These limitations result in a lack of quantifiable and qualitative data concerning terrorist attack methods within the domestic maritime domain.

Quantifiable data is data that can be measured, verified, and are amenable to statistical manipulation. Qualitative data are more varied and include virtually any non-numerical information that can be captured.[12] Current Coast Guard domestic maritime terrorism risk assessment efforts depend heavily on qualitative data from local subject matter expert (SME) judgments.[13] While SME observations are useful in providing context to assessment processes, quantifiable data is a critical element to terrorism risk assessment.[14] To date, the domestic maritime domain has not experienced any attempted terrorist attacks. While a good thing, it makes risk assessment more difficult precisely because of the absence of data or precedent. Without baseline examples of terrorist

---

[8] UK Ministry of Defense, *Red Teaming Guide*, 2nd ed. (London: UK Ministry of Defense, 2013).

[9] UK Ministry of Defense, *Red Teaming Guide*, 1–1.

[10] Mateski, "Why We Red Team: The Tyranny of Uncertainty."

[11] U.S. Government Accountability Office, *COAST GUARD Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*.

[12] "Qualitative Data," last revised October 20, 2006, http://www.socialresearchmethods.net/kb/qualdata.php.

[13] U.S. Government Accountability Office, *COAST GUARD Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*.

[14] Steve Ressler, "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research," *Homeland Security Affairs* 2, art. 8 (July 2006), https://www.hsaj.org/articles/171.

abilities and intent within the domestic maritime domain, maritime homeland security professionals must rely on risk assessment and analysis models.

The Coast Guard conducts terrorism risk assessment and analysis for the maritime transportation sub-sector via its Maritime Security Risk Analysis Model (MSRAM).[15] Within the MSRAM program, experts gather information and make assessments of terrorist abilities and intent against a predetermined set of attack scenarios and targets. These assessments are based on the knowledge of the expert and aided by a core set of tools and standards. While MSRAM is a validated terrorism risk assessment model, its reliance on SME judgments is problematic because "SME judgments provide ambiguous probabilities of a successful attack occurring."[16]

Current Coast Guard terrorism risk analysis defines risk based on a predetermined set of attack scenarios.[17] While it provides stability for the MSRAM assessment program, it does not allow for the evaluation of other potential and emerging attack scenarios. A 2010 GAO report regarding passenger ferry security states that while the Coast Guard assesses terrorism risk in the maritime domain, the organization "may be missing opportunities to enhance ferry security."[18] By not evaluating alternative attack scenarios, the Coast Guard limits the opportunities for successfully reducing the terrorism risk in the domestic maritime domain.

According to Fishbein and Treverton, "alternative analysis seeks to help analysts and policy-makers stretch their thinking through structured techniques that challenge underlying assumptions and broaden the range of possible outcomes considered."[19] Red

---

[15] U.S. Government Accountability Office, *COAST GUARD Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*.

[16] Louis Anthony Cox, "Some Limitations of Risk= Threat x Vulnerability x Consequence for Risk Analysis of Terrorist Attacks," *Risk Analysis International Journal* 28, no. 6 (December 2008): 749–1761.

[17] U.S. Government Accountability Office, *COAST GUARD Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, 3.

[18] U.S. Government Accountability Office, *Ferry Security Measures Have Been Implemented, but Evaluating Existing Studies Could Further Enhance Security* (GAO-11-207) (Washington, DC: U.S. Government Accountability Office, 2010), 29.

[19] Warren Fishbein and Gregory Treverton, "Rethinking "Alternative Analysis" to Address Transnational Threats," Occasional Papers, *Sherman Kent Center, Central Intelligence Agency* 3, no. 2 (October 2004), https://www.cia.gov/library/kent-center-occasional-papers/vol3no2.htm.

teaming is a form of alternative analysis that is well suited to support terrorism risk assessment and analysis. Red teaming is a practice carried out by a group in a cooperative environment to question conventions, procedures, administrations, and competencies from an adversarial perspective.[20] This thesis conducts research into the principles and practises of red teaming, applies them to the Coast Guard anti-terrorism constructs in place, and proposes a model for a domestic maritime anti-terrorism red teaming program.

"Defined loosely, red teaming is the practice of viewing a problem from an adversary or competitor's perspective."[21] The Coast Guard conducts terrorism risk analysis from a defender's point of view.[22] The integration of an adversarial perspective into the existing Coast Guard risk analysis constructs could add valuable insights into current and future terrorist attack methods within the domestic maritime domain.

An additional application for alternative analysis is in support of policy development. "The goal of most red teams is to enhance decision making, either by specifying the adversary's preferences and strategies or by simply acting as a devil's advocate."[23] Red teaming can be used to review current and under development policies from an adversary's point of view. This approach could prove value added within the area of domestic maritime anti-terrorism policy formulation.

This thesis explores an application of alternative analysis red teaming not currently addressed in the literature. A wealth of information is available on red teaming for business and military applications. However, a gap exists regarding red teaming's application in the homeland security terrorism risk management field of practice. This evaluation highlights a potential use of red teaming in support of domestic maritime anti-terrorism programs.

---

[20] Matthew Lauder, "Red Dawn: The Emergence of a Red Teaming Capability in the Canadian Forces," *Canadian Army Journal* 12, no. 2 (2009): 31.

[21] "Red Teaming and Alternative Analysis," accessed January 11, 2015, http://redteamjournal.com/about/red-teaming-and-alternative-analysis/.

[22] U.S. Government Accountability Office, *COAST GUARD Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*.

[23] "Red Teaming and Alternative Analysis."

Conceptually, the program would be comprised of three components:

- Physical red teaming that identifies the capabilities of would-be attackers to conduct elements of a terrorist attack within the maritime domain. The program's outputs would be quantifiable data elements incorporated into the existing MSRAM program.
- Identification of future attack scenarios. A program that conducts assessments of emerging technologies and their potential application for terrorist attacks within the domestic maritime domain. The program's outputs would include descriptions of the technologies, application within the domestic maritime domain, and potential countermeasures.
- Policy red teaming. A program that assesses the level to which policy meets strategic goals. Specifically, how Coast Guard domestic maritime anti-terrorism policies reduce the risk of terrorist attacks.

To develop the program and capture intermediate results, in this thesis, the author proposes a minimum viable program approach for domestic maritime red teaming. This minimum viable program would provide value to Coast Guard risk management practices and allow the organization to learn more about and developed an integrated red teaming program in real time.

To describe the concept of minimum viable program, it is helpful to understand the more common term of minimum viable product. "A minimum viable product is that version of a new product that allows a team to collect the maximum amount of validated learning about customers with the least effort."[24] In other terms, "a minimum viable product is the smallest thing you can build that delivers customer value (and as a bonus captures some of that value back)."[25]

Within this thesis, the author utilizes the definitions and concepts of minimum viable product to propose a minimum viable program within the Coast Guard. He defines a minimum viable program as the collection of initial policy, training, techniques, and procedures (TTP), and tools, which are entered into a learning loop to establish a

[24] Eric Ries, *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses* (New York: Random House LLC, 2011), 70.

[25] Ash Maurya, "Minimum Viable Product," LeanStack, accessed July 21, 2015, http://practice trumpstheory.com/minimum-viable-product.

program, while improving and developing its elements to meet strategic objective(s) of an agency.

C. RESEARCH QUESTION

This thesis answers the question of "How can the alternative analysis concepts of red teaming be leveraged to enhance the value of domestic maritime anti-terrorism activities?"

D. LITERATURE REVIEW

1. Introduction

The literature review focuses on the schools of thought regarding the types of red teaming, and implementation of red teaming programs. The literature can be divided into three subcategories. The first is the definition of red teaming, and related lexicon. The second category relates to the development of red teaming through history. The third category is literature that focuses on the elements of and execution of red teaming programs.

In the academic homeland security field, little research is currently associated with the subject of red teaming. One of the most significant references to red teaming within homeland security can be found in the 9–11 Commission Report, which states that red teaming programs are "notably lacking within the homeland security and intelligence elements of the Federal government."[26]

2. Red Teaming Literature Approaches/Methods/Techniques

This subcategory of red teaming literature is generally comprised of journal articles and postings that focus on the execution of red teaming programs. For the most part, this area of red teaming sub-literature is recent, and most content can be accessed via online society journal websites, such as *The Red Teaming Journal*.[27] The majority of

[26] National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission on Terrorist Attack upon the United States* (Washington, DC: National Commission on Terrorist Attacks Upon the United States), 352.

[27] "Home," accessed January 11, 2015, http://redteamjournal.com/.

the literature in this category focuses on military applications of red teaming, the starting points of which are captured in a Department of Defense report entitled *Defense Science Board Task Force on The Role and Status of DOD Red Teaming Activities.*[28] The same can be said internationally. In 2013, the United Kingdom (UK) Ministry of Defence produced a report within which the authors argue that "Red Teaming activities range from scrutinizing and challenging emerging thoughts, ideas, and underpinning assumptions, to considering the perspectives of adversaries, competitors or outsiders."[29] Both these documents provide clear arguments for the role of red teaming, and red cell activities in support of defense department mission planning and management elements.

Red teaming homeland security concepts are of limited focus, most of which are focused upon counter-terrorism aspects. The Government Accountability Office (GAO) has produced several reports involving red teaming for homeland security items including a 2007 testimony report regarding GAO's red teaming activities with Transportation Security Administration passenger screeners.[30] Of note is a current focus within many journals on red teaming within the cyber domain, for example.

3. Value of Red Teaming

This subcategory of red teaming literature is generally comprised of congressional reports and testimony related to the value of red team programs. The majority of this collection focuses on military applications,[31] along with some homeland security applications. For example, a 2004 Sandia National Laboratories report discusses the value of red team and red gaming programs for homeland security applications.[32]

---

[28] Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *The Role and Status of DOD Red Teaming Activities* (Washington, DC: Department of Defense, 2003).

[29] UK Ministry of Defense, *Red Teaming Guide,* 2–1.

[30] Gregory Kutz and John Cooney, *Aviation Security: Vulnerabilities Exposed through Covert Testing of TSA's Passenger Screening Process: Testimony before the Committee on Oversight and Government Reform, House of Representatives* (GAO-08-48T) (Washington, DC: U.S. Government Accountability Office, 2007).

[31] Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *The Role and Status of DOD Red Teaming Activities.*

[32] Judy Moore, John Whitley, and Rick Craft, *Red Gaming in Support of the War on Terrorism: Sandia Red Game Report* (SAND2004-0438) (Albuquerque, NM and Livermore, CA: Sandia National Laboratories, 2004).

4. Red Teaming Structure and Focus

An area of differing opinion with the literature revolves around the structure of red teaming programs. Authors, such as Gregory Fontenot, write from the position that red teaming should be free form in nature, and devoted to planning elements. It needs to be empowered to submit independent opinions and alternative perspectives separated from an organization's functional processes and procedures.[33]

Others, such as Richard Craft, view red teamer's true role as developing the options and responses available to adversaries or competitors.[34] The Department of Army literature generally describes the functional elements of red teaming as "a critical insight process, supporting decision makers via a structured iterative process."[35] Homeland security literature tends to view red teaming from the point of view of SMEs with the skills to understand how to attack systems and specific target types.[36]

From a strategic point of view, red teaming literature focuses upon processes that support senior level decision making. The *Red Team Handbook* states, "The penultimate purpose of red teaming and applying critical thinking techniques is to support the organization in reaching good decisions while avoiding the lure of groupthink"[37]

Generally speaking, a disparity exists regarding the focus of red teaming efforts. In other words, should red teaming concentrate upon assuming the role of adversaries, or place a full emphasis on challenging aspects, plans, and the program's abilities to meet desired results.[38]

---

[33] Moore, Whitley, and Craft, *Red Gaming in Support of the War on Terrorism: Sandia Red Game Report*.

[34] Richard Craft, *A Concept for the Use of Red Teams in Homeland Defense* (Livermore, CA: Sandia National Laboratories, 2002).

[35] Timothy Malone and Reagan Schaupp, "The Red Team, Forging a Well-Conceived Contingency Plan," *Aerospace Power Journal* XVI, no. 2 (Summer 2002).

[36] Barbara Tuchman, *The Guns of August* (New York: Macmillan Publishing Co., Inc., 1962), 73.

[37] University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook (formerly the Red Team Handbook* (Ft. Leavenworth, KS: University of Foreign Military and Cultural Studies, 2015), 57, http://usacac.army.mil/sites/default/files/documents/ufmcs/The_Applied_Critical_Thinking_Handbook_v7.0.pdf.

[38] Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *The Role and Status of DOD Red Teaming Activities*, 2.

5. Red Teaming Definition

A source of divergence within red teaming literature is the definition of the actual term red teaming. Red teaming is not easily defined, as it is applied to different forms and various types of problems.[39] The widespread range of activities includes red teaming for business decisions, federal government policy, war fighting plan development, and insurance industry standards to name a few. Literature focused on homeland security tends to focus on terrorist actions, and "attacker and defender" type of scenarios. One area of agreement within the literature is included within the goal or stated objective of red teaming. Red teaming should contest organizational assumptions from the adversarial perspective to gain a greater understanding of vulnerabilities and risks.[40] Otherwise, stated, red teaming is "a peer review process of a concept or proposed course of action."[41]

6. Red Cell Definition

Red teaming literature points out the specific differences between the terms red teaming and red cell. The UK Ministry of Defense *Red Teaming Guide* provides the most relevant definitions.

> The role of the red team is to challenge the perceived norms and assumptions of the commander and his staff in order to improve the validity and quality of the final plan. Red Cell is a J2 (intelligence) entity which focuses on the activities of potential adversaries and threats. A red cell may also play the adversarial role(s) in any wargaming or debate undertaken to assist decision making during the planning process. The red cell uses established red teaming techniques to achieve their role, but their terms of reference are much more specific than those of the red team.[42]

---

[39] Mike McGannon, "Developing Red Team Tactics, Techniques and Procedures," *Red Team Journal*, April 2004.

[40] Anna Culpepper, "Effectiveness of Using Red Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack" (master's thesis, Naval Postgraduate School, 2004), 9.

[41] Malone and Schaupp, "The Red Team: Forging a Well-Conceived Contingency Plan," 23.

[42] UK Ministry of Defense, *Red Teaming Guide*, 4–2.

7. Red Teaming Development Across History

A subcategory of the literature speaks to the use of and development of red teaming through the course of time. In their paper on military problem solving, Brewer, Shubik, and Martin state that the origins of red teaming can be traced to 19th century Germany and the development of Kliegspiele or war game.[43] According to that group, Kliespiele is "a rules-based map simulation war game, allowed for the opportunity to train and test concepts and plans while evaluating leadership."[44]

This concept of wargaming evolved over the years, and expanded out to other countries and branches of government. During the Cuban Missile Crisis of 1962, the Executive Committee of the National Security Council was established to inform the Kennedy White House on the situation and to develop a suite of potential courses of action.[45] The committee was charged, among other things, to seek alternative courses of action to the strong military response proposals being presented.

8. Red Teaming Programs

An additional subcategory of literature addresses how red teaming programs are executed. As many methods of execution exist as do red teaming programs, which contributes to the lack of a clear, concise red teaming definition.[46] However, most red teaming approaches can be described as falling into two broad groups, either passive or active.[47]

Kirpatrick states that passive red teaming is used to "define alternatives and challenge existing assumptions."[48] It may also help define how an adversary might adapt.

---

[43] Gary Brewer and Martin Shubik, *The War Game: A Critique of Military Problem Solving* (Cambridge MA, Harvard University Press, 1979), 23.

[44] Ibid.

[45] Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *The Role and Status of DOD Red Teaming Activities*, 3.

[46] Ibid., 4.

[47] Malone and Schaupp, "The Red Team: Forging a Well-Conceived Contingency Plan."

[48] Shelley Kirkpatrick, Shelly Asher, and Catherine Bott, *Staying One Step Ahead: Advancing Red Teaming Methodologies through Innovation* (Arlington, VA: Homeland Security Institute, 2005), 4.

The U.S. Department of Defense states the purpose of passive red teaming "is to aid and organization by providing critical analysis to anticipate problems and avoid surprise."[49]

Active red teaming is generally used to test tactics before use. Referencing Kirpatrick, graduate research student A. Bentley Nettles, explains that by acting as a competitor, red teaming "is used to train staffs to respond to adversarial actions."[50] In the perspective of military planning the U.S. Department of Defense identifies the purpose of active red teaming "is to sharpen skills, expose vulnerabilities that adversaries might exploit and, in general, increase understanding of potential actions and counter-actions of potential adversaries."[51]

9. Areas for Further Research

Areas of red teaming that further research would be value added include the use of gaming, or virtual red teaming tools, and how social media "tools" factor into red teaming. In both cases, identifying how emerging technologies fit into the programs and procedures for red teaming would enhance the understanding of red teaming concepts.

10. Conclusions

The literature related to red teaming provides a wide spectrum and disparate views regarding the definition of red teaming, its development and use throughout history, and elements of red teaming programs. While the volume of information is of value, the variation in views results in difficulties in defining subcategories of literature and capturing a consensus of views on red teaming. One conclusion seems to be appropriate, if you have seen one red teaming program, you have seen one red teaming program. As a result, the author would argue that further research into elements of red teaming, and its value at the strategic, operational, and tactical levels, is appropriate. Further, the author would say that additional research in the red teaming applications for

---

[49] Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *The Role and Status of DOD Red Teaming Activities*, 4.

[50] A. Bentley Nettles, "The President Has No Clothes: The Case for Broader Application of Red Teaming within Homeland Security" (master's thesis, Naval Postgraduate School, 2010).

[51] Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *The Role and Status of DOD Red Teaming Activities*, 4.

non-military applications, such as homeland security and business applications, is warranted.

E. RESEARCH DESIGN

The following sections take the reader through the research design used in this thesis and describe the design in terms of object/sample, selection, limits, data sources, type of analysis, and output of this project.

Object/Sample: The author has studied red team analysis, and its application within the Coast Guard's terrorism risk analysis programs, as well as its use for policy analysis. He have also reviewed federal government reports and publications that highlight the role of red teaming at the tactical, operational, and strategic levels. The concepts of social identity theory and its role in red teaming were additionally analyzed.

In addition, he has reviewed Coast Guard terrorism risk management programs and policy that made it possible to identify areas within the organization that would benefit from red teaming processes. This review led to his exploration of intergrading and leveraging red team functions within the Coast Guard Academy to benefit the organization and enhance educational experience of future Coast Guard officers.

Selection: U.S. Department of Defense publications provide detailed information on red teaming in various levels of the department. A similar UK Ministry of Defense publication provides further details on the benefits of red teaming, and its integration into a planning cycle. A Government of Canada homeland security journal discusses red team applications for national level security events and its application for the 2010 Vancouver Winter Olympics. The author intended to research the various approaches, identify value added red team concepts, and apply them to current domestic maritime anti-terrorism constructs.

Limits: This research does not address red teaming in terms of cyber security; rather, the focus is on red teaming for physical attacks. It also does not discuss red teaming use for exercises, or any training requirements for red teams with the exception of potential integration of red teaming concepts into Coast Guard Academy syllabi.

Additionally, the research does not explore the specific details of the Coast Guard risk assessment and analysis programs, nor specifics on the qualitative and quantitative data contained within.

The scope of this thesis focused on establishing red teaming programs in support of the existing Coast Guard maritime terrorism risk assessment and analysis constructs. The author chose this area of study after identifying a potential opportunity to make improvements to the existing risk assessment programs. His scope did not include the testing of any other tools to address areas of improvement in Coast Guard terrorism risk assessment.

Data Sources: The author leveraged Coast Guard terrorism doctrine and policy, as well as red teaming principles and processes as his primary data sources. GAO reports, Department of Defense and DHS publications, red team society journals, and books discussing red teaming rounded out the rest of his sources.

Type and Mode of Analysis: This thesis includes analysis and an examination of implementing a red team program within the Coast Guard. Analysis begins with a discussion of the domestic maritime domain and the Coast Guard's terrorism risk assessment and analysis programs. There will also be inquiry into why red teaming would be value added functions at the tactical, operational and policy levels within the Coast Guard.

Output: A finished product of the analysis would include specific recommendations about the benefits of incorporating red teaming into the existing maritime terrorism risk management system. It further makes recommendations regarding the potential value of leveraging the Coast Guard Academy within the described red teaming program.

F. UPCOMING CHAPTERS

In the upcoming chapters, the author provides readers insight into the complex operating environment known as the domestic maritime domain. Following this discussion, he explores red teaming, best practices, components, and examples of its use

within both military and homeland security frameworks. He also discusses the concept of social identity theory's role in red teaming. From these foundational principles, he explores a proposal for a domestic maritime domain red team program. This proposal includes specifics on a physical red team program, future attack scenario red team program, and policy red team program. In addition, he provides information on the implementation of the proposed red team programs, which includes the concept of a minimal viable program in the federal government, and considerations for the successful implementation of the proposed programs, as well as an exploration of the use of Coast Guard Academy Cadets within the proposed red team programs.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE DOMESTIC MARITIME DOMAIN

A. INTRODUCTION

This thesis explores the potentials of red teaming for domestic maritime anti-terrorism programs within the Coast Guard. To investigate these concepts, it is first necessary to define the geographic and operational landscape within which the Coast Guard operates. This chapter provides an overview of the diverse elements that make up, and influence, the domestic maritime domain. In addition, this chapter informs the reader on the regulations, operations, and risk management functions the Coast Guard leverages to address terrorism risks. This fundamental information is a base of knowledge that supports an examination of red teaming within the domestic maritime domain.

The maritime domain is defined as "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances."[52] The Maritime Transportation System (MTS) is within the maritime domain. The National Infrastructure Protection Plan defines the MTS as "about 95,000 miles of coastline, 361 ports, over 10,000 miles of navigable waterways, 3.4 million square miles of Exclusive Economic Zone to secure, and intermodal landside connections."[53] This system is a vital link in the U.S. intermodal transportation system. Over 75% of all international goods and the majority of all bulk and containerized cargo enter U.S. maritime ports with follow-on transportation primarily via the rail and trucking modes.[54]

In 2014, an estimated $2.56 trillion of goods were imported into the United States, which constitutes an average overall growth of 5.29% since 2009, with forecasts

---

[52] Department of Defense and Homeland Security, *National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security* (Washington, DC: Department of Defense and Homeland Security, 2005).

[53] "National Infrastructure Protection Plan, Transportation Systems Sector," accessed December 9, 2014, http://www.dhs.gov/xlibrary/assets/nipp_transport.pdf.

[54] *House Committee on Transportation and Infrastructure, Improving the Nation's Freight Transportation System: Findings and Recommendations of the Special Panel on 21st Century Freight Transportation* (2013), 29.

indicating an increase to $3.09 trillion worth of goods being imported by 2019.[55] The World Trade Organization lists the United States as the largest importer of goods in the world, "accounting for 12.6% of the world total."[56] Also, 99.4% of all overseas cargo volume moves through U.S. seaports, roughly totaling $3.8 billion worth of goods each day.[57] Impacts of any disruption of the MTS can "have national ramifications, as the MTS is the critical component of the national supply chain."[58] Understanding the potential and future threats to the system are a key basis in managing the risks of terrorism within the domestic maritime domain.

The MTS is a system of systems, comprised of waterways, seaports, vessels, and facilities. The United States has roughly 360 commercial ports that consist of both public (owned and managed by state, regional, and local port authorities) and privately owned facilities with approximately 150 different seaport agencies, navigation districts, and port authorities making up the industry.[59] The maritime system is comprised of more than 3,700 cargo and passenger terminals and nearly 8,200 commercial cargo-handling docks.[60] The volume of containerized cargo entering the United States has increased by over 170 percent since 1990.[61] Container ship size and capacity is continuing to grow with the most recent production of the "Triple-E" cargo ship capable of carrying 9,000 containers.[62] The MTS is a transportation mode through which goods and people are transported in, out, and across the United States via maritime means. The system is

---

55 "Business Environment Profiles—Total Import," March 2014, http://clients1.ibisworld.com.nduez proxy.idm.oclc.org/reports/us/bed/default.aspx?entid=1533.

56 Ibid.

57 "U.S. Port Industry," accessed December 8, 2014, http://www.aapa-ports.org/industry.

58 Committee on the Marine Transportation System, *National Strategy for the Marine Transportation System: A Framework for Action* (Washington, DC: The Secretary of Transportation, 2008).

59 "U.S. Port Industry."

60 *House Committee on Transportation and Infrastructure, Improving the Nation's Freight Transportation System: Findings and Recommendations of the Special Panel on 21st Century Freight Transportation*, 29.

61 Department of Homeland Security, *Safety, Security and Stewardship* (Washington, DC: Director of Strategic Management and Doctrine, U.S. Coast Guard Headquarters, 2011), 4.

62 Marco Werman and Drake Bennet, "Holy Ship! Triple E—The Biggest Container Ship in the World," *PRI The World*, September 9, 2013, http://www.pri.org/stories/2013-09-09/holy-ship-triple-e-biggest-container-ship-world.

critical to the nation's economy and stability and can pose as an attractive target for would-be terrorists.

B. REGULATORY AND GRANT PROGRAMS THAT INFLUENCE MTS SECURITY

In 2002, the DHS was established by combining 22 separate federal agencies under one federal entity responsible for the coordination and unification of homeland security efforts.[63] The Maritime Transportation Security Act (MTSA) was signed into law that same year, primarily to protect the ports and waterways from terrorist attacks. The MTSA established a standard approach to addressing security risk within the ports, waterways, and coastal approaches including constructs for public and private partnerships to address security risks.

The MTSA increased security requirements and put a new lens on how risk is evaluated and assessed within the nation's maritime domain. Specifically, the MTSA set "the requirement for port facilities to conduct vulnerability assessments and develop security plans"[64] and resulted in the establishment of area maritime security committees (AMSCs), led by each Coast Guard Captain of the Port.[65] This construct of assessment, planning, and coordinating bodies set the foundations of maritime risk management systems managed by public, private, and governmental elements. It provides the base of a layered approach to reducing terrorism risk within the MTS. Red teaming can assist in validating or redirecting the efforts of the AMSCs by providing an alternative analysis of plans and threats.

Domestic port security is not solely managed by the federal government. Owners and operators of facilities and vessels play a significant role in reducing terrorism risk. Additionally, local and state law enforcement and emergency responders contribute to the risk reduction efforts. The Port Security Grant Program provides funding to private and public elements within the MTS to reduce vulnerabilities to and consequences of terrorist

63 "Home," accessed December 8, 2014, www.dhs.gov/home.

64 "Maritime Transportation Security Act," accessed December 8, 2014, https://homeport.uscg.mil.

65 Ibid.

attacks within the MTS. Fiscal year (FY) 2014 DHS grant funding across six DHS preparedness grant programs totaled $1.6 billion and was targeted at strengthening the nation's "ability to prevent, protect against, mitigate, respond to, and recover from terrorist attacks, major disasters, and other emergencies in support of the National Preparedness Goal and the National Preparedness System."[66]

For FY 2014, the DHS directed grantees to prioritize grant funds based on the grantees' capability targets and gaps as identified through the *Threat and Hazard Identification and Risk Assessment and annual State Preparedness Report*.[67] Additionally, $1.6 billion was provided across six different grant programs, with $100 million for the Port Security Grant Program (PSGP). The PSGP is designed to "help protect to help protect critical port infrastructure from terrorism, enhance maritime domain awareness, improve port-wide maritime security risk management, and maintain or reestablish maritime security mitigation protocols that support port recovery and resiliency capabilities."[68] Focusing port security grant funding on the greatest risk reduction return of investment is a critical element of the overall domestic maritime anti-terrorism effort. The red teaming program the author proposes would specifically provide assessment and analysis currently not available to the PSGP.

C. COAST GUARD DOMESTIC MARITIME SECURITY OPERATIONS

The PWCS mission is one of the Coast Guard's statutory homeland security missions (Section 888 of the Homeland Security Act of 2002). To fulfill the PWCS mission, the Coast Guard employs a strategy that consists of three key elements executed simultaneously to stem specific threats when known, and to mitigate general terror-related risks in the maritime domain at all times. "The elements are; achieve maritime

---

[66] Department of Homeland Security, *DHS Announces Grant Guidance for Fiscal Year (FY) 2014 Preparedness Grants* (Washington, DC: DHS Press Office, 2014).

[67] U.S. Government Accountability Office, *Testimony Before the Subcommittee on Emergency Management, Intergovernmental Relations, and the District of Columbia, Committee on Homeland Security and Government Affairs, U.S. Senate, National Preparedness—FEMA Has Made Progress, But Additional Steps Are Needed to Improve Grant Management and Assess Capabilities* (Statement of David C. Maurer, Director Homeland Security and Justice) (GAO-13-637T) (Washington, DC: U.S. Government Accountability Office, 2013).

[68] Ibid.

domain awareness, establish and oversee a maritime security regime, and lead and conduct effective maritime security and response operations (MSRO)."[69]

The MSRO element refers to a diverse suite of activities that include but are not limited to the following.

- Security patrols to project credible deterrence near critical infrastructure
- Pre-entry security boardings of high-interest vessels before they transit domestic ports
- Security boardings of small vessels to support DHS' Small Vessel Security Strategy and mitigate risk of a waterborne improvised explosive device attack
- Positive control measures to ensure vessels remain under the control of vetted crews during transits of domestic ports
- Fixed security zone enforcement, primarily to protect key locations or events
- Moving security zone enforcement for point protection of selected shipping

The performance standards for MSRO activities are risk informed. The execution of MSRO activities is measured through a combination of output and outcome measures. To assess the impact of PWCS mission execution, the Coast Guard uses a risk-based performance model to evaluate the percent reduction in maritime security risk that the Coast Guard can influence. Red teaming constructs can be tailored to inform these performance measures.

The layered maritime security construct is not limited to domestic operations. Coast Guard personnel visit foreign ports and "assess the effectiveness of anti-terrorism measures that the ports have implemented to comply with the International Ship and Port Facility Security (ISPS) Code."[70] Boarding teams deployed from Coast Guard cutters conduct suspect vessel security boardings as far offshore the U.S. coasts as practicable. Large Coast Guard cutters maintain a persistent offshore presence. MDA tools, such as

[69] Derived from internal Coast Guard documents drafted by the author.

[70] Ibid.

long-range identification and tracking, and the National Automated Identification System, are used in offshore tracking, surveillance, and interdiction. As U.S. and foreign vessels approach the coast and their ports of call, they give the required advance notice of arrival and provide key vessel, cargo, and crew information. The identification of potential threat streams plays a critical role in these operations. Red teaming protocols can directly support those efforts.

In U.S. waters and ports, vessels perform the security measures required of them by their approved MTSA or ISPS vessel security plans. At all times, MTSA-regulated facilities in U.S. ports perform the security measures required of them by their approved facility security plans. Vessels and facilities control access to their restricted areas to the holders of transportation worker identification credentials. U.S. ports enhance their preparedness and resiliency by periodically exercising their area maritime security plans.[71] This layered approach of security operations combining federal, state, local, and industry efforts seeks to address the risks of terrorism within the domestic maritime domain.

D. RISK MANAGEMENT APPROACH TO DOMESTIC MARITIME TERRORISM

The Oxford dictionary definition of risk management is…"(In business) the forecasting and evaluation of financial risks together with the identification of procedures to avoid or minimize their impact."[72] A recent GAO report defines risk management as... "a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty."[73] To put the definition in the context of homeland security, the 2010 DHS risk lexicon, states that risk management is "the process for identifying, analyzing, and communicating risk and accepting, avoiding,

[71] Derived from internal Coast Guard documents drafted by the author.

[72] "Risk Management," accessed January 14, 2015, http://www.oxforddictionaries.com/us/definition/american_english/risk-management.

[73] U.S. Government Accountability Office, *Testimony Before the Subcommittee on Transportation Security and Infrastructure Protection, Homeland Security Committee, House of Representatives, Risk Management, Strengthening the Use of Risk Management Principles in Homeland Security* (Statement of Norman J. Rabkin, Managing Director, Homeland Security and Justice) (GAO-08-904T) (Washington, DC: U.S. Government Accountability Office, 2008).

transferring, or controlling it to an acceptable level considering the associated costs and benefits of any actions taken."[74] It further defines risk as "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood as well as the associated consequences."[75]

In simple terms, risk management is the "likelihood that a threat will harm an asset with some severity of consequences, and deciding on and implementing actions to reduce it" known as risk reduction measures.[76] For terrorism risk, it can be translated as the likelihood that a terrorist attack would harm a target with some level of consequence. Risk management is the act of determining the level of that risk; then deciding on, planning, and taking actions to reduce that risk. Red teaming alternative analysis is a value added function available to assist in terrorism risk management.

U.S. domestic maritime terrorism risk assessment and analysis is primarily conducted by the U.S. Coast Guard. The MSRAM is the primary tool and program executed by the Coast Guard to define the threats, vulnerabilities, and consequences of potential terrorist actions within the domestic maritime domain.[77] This program relies heavily on SME judgments as the primary method to define attackers' abilities and potential attack methods.

The Coast Guard leverages its role within the intelligence community in its efforts to define maritme terrorism risk. The MSRAM uses threat information from the Coast Guard intelligence coordination center (ICC), which "provides strategic intelligence support [and] serves as the Coast Guard's primary interface with the collection, production, and dissemination elements of the national intelligence and law enforcement

---

[74] Risk Steering Committee, *DHS Risk Lexicon 2010 Edition* (Washington, DC: U.S. Department of Homeland Security, 2010).

[75] Ibid.

[76] "Building Design for Homeland Security," accessed December 8, 2014, http://www.fema.gov/pdf/plan/prevent/rms/155/e155_unit_v.pdf.

[77] "Maritime Security, Risk Analysis Model," accessed January 14, 2015, http://aapa.files.cms-plus.com/PDFs/MSRAMBrochureTrifold.pdf.

communities."[78] In terms of maritime terrorism risk assessment, threat is composed of two distinct elements, intent, and capability.[79]

The Coast Guard conducts strategic assessments and analysis of maritime terrorism under those two categories. MSRAM utilizes threat data provided by the Coast Guard ICC. While this data is regionally specific, it is strategic in nature and not necessarily relevant to local maritime terrorism risk assessment and analysis. "It is not revolutionary to view terrorist through the lens of either intentions or capabilities. Yet terrorism analysis rarely combines the two across the range of potential threats in an area."[80] Red teaming operates in a similar manner; forms of physical red teaming seek to define attack scenarios from the adversary's perspective. To do so, an analyst must approach the problem set with the intents and capabilities of the adversary in mind.

In conclusion, the domestic maritime domain is a complex system of waterways, vessels, and facilities spread across the United States. The risks of terrorist attacks within this domain are substantial and complex. A combined approach by federal, state, local, and private entities seeks to address terrorism risk across the domain through operations, regulations, and grant funding. This risk management approach relies heavily on the Coast Guards' terrorism risk assessment and analysis programs to guide efforts in achieving the greatest return on investment for anti-terrorism efforts. Red teaming functions, applied appropriately, can provide value to this effort.

---

[78] Department of the Navy, *Naval Doctrine Publication 2: Naval Intelligence* (Norfolk, VA: Naval Warfare Development Command, 2008), http://www.nwdc.navy.mil/content/Library/Documents/NDPs/ndp2/ndp20007.htm.

[79] Michael D. Greenberg et al., *Maritime Terrorism, Risk and Liability* (Santa Monica, CA: RAND, 2006).

[80] Shawn Cupp and Michael G. Spight, *A Homeland Security Model for Assessing U.S. Domestic Threats* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2007).

III. RED TEAMING

A. INTRODUCTION TO RED TEAMING

Over the last 10 years or so, many commissions and panels have identified an alternative analysis as a means of improving analytical processes and decision making. In 1998, the Jeremiah Panel was formed and tasked to identify why the United States was caught unaware when India and Pakistan conducted near simultaneous nuclear weapons tests.[81] The panel lead, Admiral David Jeremiah, stated in his conclusions. "the bottom line is that both the intelligence and the policy communities had an underlying mindset going into these tests that the … newly governing Indian party would behave as we behave."[82] Assuming other parties will think and behave as everyone else does is a common error in policy development, one that red teaming seeks to correct.

The 9/11 Commission asked, "why so little thought had been devoted to the danger of suicide pilots, seeing a 'failure of imagination' and a mindset that dismissed possibilities."[83] Various legislations have also identified similar needs. The 2006 Homeland Security Act for example states, "The Act requires DHS to apply red team analysis to terrorist use of nuclear weapons and biological agents. As terrorists seek to exploit new vulnerabilities, it is imperative that appropriate tools be applied to meet those threats."[84] Red teams have been in existence for a long time. "Commercial enterprises, such as IBM, and government agencies such as Defense Intelligence and the Central Intelligence Agency, have long used them to reduce risks and to improve their problem solving."[85] The literature researched for this thesis identifies the value of such efforts to successful organizations.

---

[81] Roger Z. George, "Fixing the Problem of Analytical Mindsets," In *Intelligence and the National Security Strategist*, ed. Roger Z. George and Robert D. Kline (Lanham, MD: Rowman & Littlefield, 2006).

[82] Ibid.

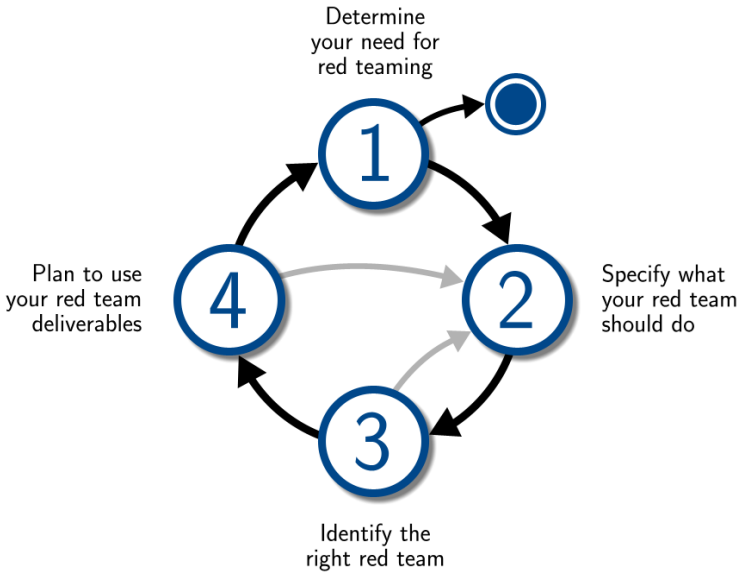
[83] National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission on Terrorist Attack upon the United States*, 334.

[84] FY2006 Homeland Security Authorization Act, Sec. 214, 9.

[85] UK Ministry of Defense, *Red Teaming Guide*, 1–1.

At the strategic level, red teaming is… "an intellectual approach used to analyze the organizations planning cycle and assumptions."[86] By providing an alternative analysis from an outside perspective, red teams add to, rather than replace, existing analytical efforts. Red teaming is an organizational process "undertaken by a flexible, independent, and expert team that aims to create a collaborative learning relationship by challenging assumptions, concepts, plans, operations, organizations, and capability through the eyes of adversaries in the context of a complex security environment."[87] As seen in Figure 1, the development of a red teaming effort can be tailored to an agency's specific needs and evolves within a continuous loop cycle.

Figure 1. Red Teaming Program Development Cycle



Source: "Red Teaming for Program Managers," 2009, http://www.idart.sandia.gov/methodology/RT4PM.html.

The UK Ministry of Defense proposed definition of red teaming is "the independent application of a range of structured, creative and critical thinking techniques

[86] Joint Task Force Games (Games Red Team), *Final Report: Vancouver 2010 Olympic and Paralympic Winter Games* (Vancouver, Canada: Joint Task Force Games (Games Red Team), 2010), 8.

[87] Lauder, "Red Dawn: The Emergence of a Red Teaming Capability in the Canadian Forces," 31.

to assist the end user make a better-informed decision or produce a more robust product."[88]

A red cell is a specific element, distinct from overall red teaming. The UK Ministry of Defense describes red cells in the traditional military opposing forces manner. "Red cells generally play the adversarial role(s) in wargaming or debate undertaken to assist decision making during the planning process … The red cell uses established red teaming techniques to achieve their role, but their terms of reference are much more specific than those of the red team."[89]

Red teaming is a process by which an organization conducts an analysis from an adversary's perspective. It is effective at countering a large organization's tendency to minimize the problem set(s) they focus upon, and the tendencies such organizations have towards groupthink. "Clearly, the majority of failures to anticipate strategic surprise can be correlated with conceptual rigidity and a high incidence of perceptual continuity."[90]

Red teaming can support organizational decision making in a number of ways. In its "Red Teaming for Program Managers," Sandia National Labs provides the following list of red teaming benefits:

- Understand adversaries and operational environments, and assess threats
- Anticipate program risk, identify security assumptions, and support security decisions
- Explore and develop security options, policy, process, procedures, and impacts
- Establish in-house red team
- Identify and describe consequential program security requirements
- Identify and describe consequential security design alternatives
- Measure security progress and establish security baselines
- Understand how system defeats adversaries

---

[88] UK Ministry of Defense, *Red Teaming Guide,* lexicon.

[89] Ibid., 4–2.

[90] Michael I. Handel, *War, Strategy, and Intelligence* (London: Frank Cass, 1989), 270.

- Explore security of future concepts of operation
- Test and train operations personnel response to attack
- Identify and describe surprise, unintended consequences[91]

As documented in the aforementioned list, red teaming is a support function to policy development and decision making. It provides organizations and decision makers information not normally considered, the point of view of the adversary. This perspective can be highly valuable in countering human tendencies towards groupthink and other trends associated with large organizations. "Analysts (and to a lesser extent, political and military leaders) should be encouraged to consider alternative interpretations of data and new evidence, and continuously to reevaluate their concept while avoiding dogmatic adherence to given concepts."[92]

Red teaming is also useful in defining organizational processes. "The common feature in all of these (red teaming) examples is the adversary's or skeptic's outlook taken on by an independent group. This shift in perspective recognizes the powerful psychological force that exists in all organizations not to challenge the way problems are framed—something that can lead to disaster."[93] The integration of red teaming into an organization's decision-making process can counteract the tendencies towards neglecting alternatives in favor of standard practices.

Red teaming can also be a valuable tool for reviewing decisions and policy. "A red team is especially useful to review decisions with large scale and complexity. This is because the momentum needed to launch such projects can lead to a feeling that team loyalty requires supporting them, and because the tendency to get lost in the many details leads people to overlook project risks as a whole."[94] Red teaming can assist in countering these tendencies by identifying risks from the adversarial perspective and weaknesses that would otherwise not be identified.

---

[91] "Red Teaming for Program Managers."

[92] Handel, *War, Strategy, and Intelligence*, 270.

[93] "Definition of Red Team," accessed January 11, 2015, http://lexicon.ft.com/Term?term=red-team.

[94] Ibid.

Some red teaming techniques are of value from a tactical perspective as well. Military and business organizations use red teaming as a means to identify vulnerabilities within their plans and defenses. "Technology giants like Microsoft and Apple use red teams to try to hack their own software, knowing that if they relied on software producers to judge this they would overlook many holes and vulnerabilities."[95]

A red teaming effort not properly designed or executed can do more harm than good. The goal of red teaming is to provide an alternative point of view, rather than simply validating an organization's assumptions or decisions.[96] Red teams need support from leadership in an organization to provide that adversaries' point of view, which can be contrary to the culture of an organization.

Successful red teams must "think like the adversary." Take for example a large U.S. firm competing in the information technology (IT) market with numerous Chinese competitors. "Many U.S. firms find it difficult to understand the way Chinese companies think."[97] With the current globalazation of industry and surge of Chinese influence in those markets, red teams can bring a Chinese perspective to market analysis that is highly sought out.[98]

B. RED TEAMING APPROACHES

The *Financial Times* defines a red team as "an inside group that explicitly challenges a company's strategy, products, and preconceived notions."[99] It further describes red teaming methods as framing a "problem from the perspective of an adversary or skeptic, to find gaps in plans and to avoid blunders."[100] "Red teams are one way to manage the biggest corporate risk of all: thoughtlessness."[101] Red teams conduct alternative analysis from the perspective of the adversary, with the goal of identifying

95 "Definition of Red Team."

96 Ibid.

97 Ibid.

98 Ibid.

99 Ibid.

100 Ibid.

101 Ibid.

potential threats, and weaknesses in policy not identified through traditional assessment techniques.

Red teaming is a common tool within the military. "Red teams assist the commander and staff with critical and creative thinking and help them avoid groupthink, mirror imaging, cultural missteps, and tunnel vision throughout the conduct of operations."[102] The Department of Defense has called for an increased use of red team analysis across the department in both policy and operational plan development processes.[103]

"The most basic level of red teaming is to conduct peer review of plans and policies to detect vulnerabilities or perhaps to simply offer alternative views of scenarios."[104] For the purposes of this thesis, it is helpful to discuss red teaming in two general categories, physical and analytical red teaming.

- Physical Red Teaming

"A physical red team embodies the selected adversary, acting according to the selected group's motivations, capabilities, and intent."[105]

- Analytical Red Teaming

"During analytical red teaming, participants analyze the attack plans and look for indicators and warnings, key decision points, and vulnerabilities in the plan."[106]

According to the Under Secretary for Defense Acquisitions, red teaming functions at multiple levels within the DOD enterprise are:

- Strategic level to challenge assumptions and visions
- Operational level to challenge force postures, a commander's war

---

[102] United States Army, *Field Manual 5-0* (Washington, DC: United States Army, 2010), 1–7.

[103] Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *The Role and Status of DOD Red Teaming Activities*, 17.

[104] Michael Meehan, "Red Teaming for Law Enforcement," *The Police Chief* 74, no. 2 (February 2007), http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=print_display&article_id=1111&issue_id=22007.

[105] Ibid.

[106] Ibid.

- Plan and acquisition portfolios
- Tactical level to challenge military units in training or programs in development[107]

Red teams can take on numerous forms that are dependent upon the desired alternative analysis outputs.

The Department of Defense defines three overall red team constructs, as shown in Table 1.[108]

Table 1. Examples Types of DOD Red Teams[109]

Red Team Method	Function
Surrogate of Adversaries	Expose vulnerabilities, understanding responses available to adversaries
Devil's Advocate	Critiques and alternatives to the enterprise's assumptions
Independent Judgment	Independent advisory boards, other sources of independent judgment

Combined or individually, these red team methods establish a framework for alternative analysis red teaming processes. Red teaming steps can be planned in great detail or be more free flowing in nature. In either case, red teaming functions should define, "who the red team reports to; how it interacts with the management of the enterprise and the owner of the activity it is challenging, and how the enterprise considers and uses its products."[110]

C. SOCIAL IDENTITY THEORY APPLICATIONS FOR RED TEAMING

Social psychology theories and practices have value in understanding the perspectives of others. These concepts can be useful tools for conducting alternative

[107] Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *The Role and Status of DOD Red Teaming Activities*, 2.

[108] Ibid., 3–4.

[109] Ibid.

[110] Ibid., 3.

analysis of terrorist behaviors. "Alternative techniques force analysts to look at their own or peer's work from varying viewpoints with the goal of scrutinizing a plan or thought against previously unforeseen scenarios."[111] Red teaming is a set of alternative analysis processes focused on an adversary's point of view; thereby, conducting analysis from the adversary's perspective. Social psychological concepts can assist a red team in seeing problems from another group's point of view.

These concepts can help in avoiding the more common pitfalls associated with terrorism analysis. This section discusses the value of social identify theory (SIT) to red teaming efforts, and explores concepts of in-groups, and out-groups as a means to assist a red team in avoiding some of the more common analysis hazards. "The modern use of Red Teams has almost exclusively operated around threat replication and security validation, and, therefore, offers very few insights into an enemy's mental model or psychological mindset."[112]

Red teams may offset this analysis weakness by leveraging psychological models and approaches, such as SIT. This theory can assist in gaining an understanding of a terrorist perspective. "SIT postulates that the need for a positive and distinct identity will lead individuals to want to belong to groups that enable their members to fulfill their identity needs."[113] A red team can leverage an understanding of SIT to conduct an analysis through the lens of a terrorist's group membership affiliation, as well as that group's comparison of themselves to another.

"SIT evaluates a person's decisions and actions based on perceived group membership."[114] This theoretical approach can assist red teams in viewing their analysis from that perspective. For example, a red team conducting an assessment of anti-terrorism defenses performs their analysis from an identified attacker's perspective. When a red team fully adopts the concepts of SIT and group membership, they can begin

---

[111] Carter M. Matherly, *The Red Teaming Essential, Social Psychology Premier for Adversarial Based Alternative Analysis* (Charles Town, WV: American Military University, 2013), 4.

[112] Ibid., 2.

[113] Fathali M. Moghaddam, "Multiculturalism and Intergroup Relations," *American Psychological Association*, November 2011, 95.

[114] Matherly, *The Red Teaming Essential*, 20.

to understand a terrorist's perspective. "From the terrorists' point of view, terrorism is a rational problem-solving strategy."[115] Conducting an act of terrorism is to them, a justified means to achieve their in-groups goals.

SIT can provide a structure to understand that perspective for what it truly is, allowing the analyst to filter out the biases of their own in-group to provide a red team an understanding of how a member of an out-group would approach an attack, vice how a member of their in-group perceives that attack would occur. Red team alternative analysis that accounts for this concept can provide unbiased analytical support to decision makers. SIT can provide a means by which a red team can gain an understanding of how other groups perceive the element they are analyzing.

The concepts of in-groups and out-groups are core elements in the approach. "When a social identity is activated, people act to enhance the evaluation of the in-group relative to the out-group and thereby enhance their own evaluation as a group member."[116] According to McLeod, "We divided the world into 'them' and 'us' based through a process of social categorization (i.e., we put people into social groups)."[117] This explanation divides people into two groups, the in-group (us) and the out-group (them).[118] "The central hypothesis of social identity theory is that group members of an in-group will seek to find negative aspects of an out-group, thus enhancing their self-image."[119]

To analyze adequately from the perspective of a terrorist, red teams must gain an understanding of the terrorist's in-group to allow the red teams to view the element they are analyzing from the adversaries' point of view. An understanding how a terrorist

---

[115] Fathali M. Moghaddam, *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy* (Santa Barbara, CA: Praeger Security International, 2006), 2.

[116] John C. Turner, *Rediscovering the Social Group: A Self-Categorization Theory* (Oxford: Basil Blackwell, 1987).

[117] Saul A. McLeod, "Social Identity Theory," *Simple Psychology*, 2008, http://www.simply psychology.org/social-identity-theory.html.

[118] Ibid.

[119] McLeod, "Social Identity Theory."

becomes radicalized and the hermeneutics that make up their in-groups narratives can provide a red team the ability to approach analysis as the terrorist would.

Also needed is an understanding of the concept of the out-group. This concept introduces an approach, which states that individuals view themselves based in part on how they compare themselves to those outside their group. "Membership of the group is important, but not as important as the relationship that emerges as the individual further defines themselves via comparison of a contrasting group known as the 'out-group."[120]

Social physiological theories can further assist red teams in preventing some of the common errors associated with an analysis of terrorists. Table 2 lists some of the mindsets that can lead to errors in an analysis effort. Red teaming, with SIT factored in, can assist an analyst in avoiding some of these pitfalls. Identifying and understanding the underlying factors associated with another's in-group, and out-groups can provide a red team analysis the ability to approach a problem set free of these more common errors.

Table 2. Common Analytical Bias[121]

Bias	Description
Tunnel Vision	Tendency to focus on a small portion of a much larger complex problem
Over Optimism	Assumption that success will occur
Cultural Contempt	Failure to recognize and assimilate importance of differing culture(s)
Mirror Imaging	Applying own attitudes and opinions to a third party
Trends Faith	Blind adherence to trends
Paradigm Bias	Aversion to address/change models that have worked in the past
Current Focus	Failure to anticipate or react

SIT is a valuable tool for red team alternative analysis, which fills a void within many current approaches. "A comprehensive review of the literature suggests that a lack

[120] Henri Tajfel, *Human Groups and Social Categories* (Cambridge, MA: Cambridge University Press, 1981).

[121] University of Foreign Military and Cultural Studies, *Red Team Handbook* (Ft. Leavenworth, KS: Department of the Army, 2011), 6.

of systematic scholarly investigation has left policy-makers to design counterterrorism strategies without the benefit of facts regarding the origin of terrorist behavior—or, worse, guided by theoretical presumption couched as facts."[122]

Red teaming is that specific set of alternative analysis techniques that is based in accounting for an adversary's perspective. Knowledge of the psychology of an adversary is crucial to the development of red team functions, which if meeting requirements, provide a functional representation of an adaptive adversary.[123]

This approach is value added to developing a red teaming system that truly conducts an alternative analysis from the point of view of the adversary. A system, based on social psychological model, "can provide Red Teams the needed insight of the target audience in order to formulate mindsets, perceptions, and bias that can be in turn quantified as a rule set that the team can then base further decisions."[124] With this knowledge and skill sets, red teams can better achieve their primary function to provide an alternative analysis to decision makers from the adversaries' perspective.

If executed correctly, red teaming can break the chain of analytical bias and in-grouping traits among homeland security practitioners. A solid understanding of SIT and an approach that truly comes from an out-group's point of view should be a key skill of a red team member, which is an excellent area for further research and examination.

D. EXAMPLES OF RED TEAMS IN USE

1. Homeland Security Red Teaming- Government of Canada

The Government of Canada does not have a formal anti-terrorism red teaming program. However, Canada has utilized red teaming alternative analysis for major events, the 2010 Vancouver Winter Olympics being a recent example.[125] During the planning

---

[122] Jeff Victoroff, "The Mind of the Terrorist," *Journal of Conflict Resolution* 49, no. 1 (February 2005): 4.

[123] Matherly, *The Red Teaming Essential*, 2.

[124] Ibid., 27.

[125] Alex S. Wilner, "Terrorism in Canada: Victims and Perpetrators," *Journal of Military and Strategic Studies* 12, no. 3 (Spring 2010): 72.

cycle for securing the Olympics, a team was designated specifically to challenge Canadian Forces' (CF) conformity, convention, and orthodoxy in counterterrorism while encouraging "self-discovery and learning" within the ranks.[126]

The team, known as the Games Red Team (GRT), was tasked with conducting an alternative analysis of the Olympic security plan with the goal of gaining an understanding of the high-end threat to the Games. To achieve this goal, the GRT developed an adversary campaign plan based on an imaginary terrorist cell with traits found in open source readings on terrorist groups worldwide.[127] The team conducted an assessment of the terrorist actors' devised scalable threat scenarios from the perspective of a potential adversary that spoke to specifically identified deficiencies in the CF's Olympic plan. The GRT provided an independent peer review of defence planning.[128] This red teaming process has been identified as a best practice and incorporated into future large-scale security event planning efforts.

2. Military Red Teaming—United Kingdom Ministry of Defense

The United Kingdom does have an established red teaming program within its Ministry of Defense. Over the last couple of years, red teaming has become more widely used in UK defense planning, and is now recognized as a major aid to decision making in the planning and policy functions of defense.[129] This concept of red teaming for defense is similar to that of the Government of Canada, and the United States. "Organisations establish red teams to challenge aspects of their own plans, programmes and assumptions. It is this aspect of deliberate challenge that distinguishes red teaming from other management tools, although there is not a sharp boundary between them."[130]

---

[126] Wilner, "Terrorism in Canada: Victims and Perpetrators," 93.

[127] Ibid., 73.

[128] Ibid., 93.

[129] UK Ministry of Defense, *Red Teaming Guide*, 1–1.

[130] Ibid., 1–3.

3. Comparative Analysis of the U.S. Domestic Maritime Anti-Terrorism Programs

The Canadian red teaming approach to the 2010 Vancouver Winter Olympics is a value added example for the U.S.' homeland security event planning. The approach leveraged military officers and red team skill sets and applied them to a homeland security problem set.

The approach was not without its issues. Buy in from law enforcement elements for the alternative analysis was problematic, primarily attributed to the military procedures and approach of the red team. The approach, however, is value added; being able to leverage defense personnel and skills to allow for an independent alternative analysis of homeland security plans and functions. Refinement of the processes to account for differences in approach and clients would add further validity and value to the red team process.

Red teaming by the U.S. homeland security enterprise is not common. For example, red teaming processes were not used during the planning and development of the maritime security plan for the 2011 Asian Pacific Economic Committee conference. This event, hosted by the United States in Hawaii, was the first outside continental United States (OCONUS) national security special event.[131] Each event venue, including the hotels housing over 20 heads of state, had direct maritime perimeters requiring security. Protective security operations were planned for this event utilizing standard methods and activities outlined in the Coast Guard MSRO manual. While deemed an efficient and effective plan at the time, an alternative analysis from an adversary's point of view could have identified weaknesses in the plan along with potential countermeasures. The Canadian red team approach to the 2010 Vancouver Olympics provides a template for an alternative analysis of event security plans and could be adapted for use by the Coast Guard within the domestic maritime domain.

The UK red team approach, while similar to the U.S. model, does differ in some areas. Within the UK model, a red team is formed with the objective of "subjecting an

[131] Derived from authors experience and documents as Operations Section Chief for this National Security Special Event.

organizations plans, programmes, ideas and assumptions to rigorous analysis and challenge."[132] The U.S. model differs from the UK's model, as specific teams are established and tasked with separate functions. Teams are assigned in areas, such as conceptual challenge, wargaming, and technical terms that seek to find gaps and vulnerabilities within a plan. The UK model does not make these distinctions, with the red team identified as the group that addresses these alternative analysis processes as a whole. The UK approach for red teaming for defense could be adapted to meet red teaming needs within the domestic maritime domain. Using this overall system analysis approach shows merit, and would allow the Coast Guard to assess the ability of its programs and policy to address the risks of terrorism while also identifying future risk.

[132] UK Ministry of Defense, *Red Teaming Guide*, 1–2.

IV. DOMESTIC MARITIME DOMAIN TERRORISM RED TEAM PROGRAM

A. INTRODUCTION

Threats from terrorism persist and continue to evolve; attack methods are harder to identify and do not come from any one individual or group.[133] It is critical that Coast Guard policy, plans, and tactics maintain pace with the ever-changing risks associated with terrorism. As both a military and federal law enforcement organization, the Coast Guard faces the broad challenges each of these organizational structures are afflicted with including a lack of creativity for the sake of efficient execution.[134] As with any human system, the organization is fallible; susceptible to beliefs, biases and constraints that may skew decision making and analysis.[135] The domestic maritime security enterprise must account for this ever-changing environment and address the uncertainty, which frames anti-terrorism pragmatic decisions.[136]

The Coast Guard's domestic maritime anti-terrorism program is generally efficiently executed and managed. An alternative analysis point of view identifying future threat streams and gauging the domestic maritime security regime's ability to address them would increase the ability of the Coast Guard to define and address terrorism risk. All decision makers and their teams are subject to bias, emotion, and the need to simplify complex problems by the use of assumptions and models.[137] These realities lead policy developers to generally limit the problem sets they seek to address. Red teaming programs are designed to counter these inherent factors. Such a program within the domestic maritime domain would challenge current maritime security doctrine, identify potential weaknesses in anti-terrorism policy and plans, and offer solutions by which to lower the risks of a terrorist attack.

---

133 "Preventing Terrorism and Enhancing Security."

134 UK Ministry of Defense, *Red Teaming Guide.*

135 Ibid., 1–1.

136 Mark Mateski, "Why We Red Team: The Tyranny of Uncertainty," *Red Team Journal*, November 2014.

137 UK Ministry of Defense, *Red Teaming Guide*, 1–3.

This chapter discusses and defines a proposed alternative analysis red teaming program executed by the Coast Guard in the mission space of domestic maritime terrorism. The paragraph discusses the domestic and international nexus of maritime terrorism, and defines the program elements.

B. INTERNATIONAL MARITIME TERRORISM AND PIRACY

The global economy relies heavily on international maritime shipping to move goods and people around the world. As economic trends shift, so do the demands upon the maritime transportation system. An effective red teaming program must factor in global maritime security trends to provide value-added alternative analysis assessments.

A trend in the literature has been establishing a linkage between international piracy and maritime terrorism. Somalia's coastal waters have been at the center of much of this activity. While the motivation for most of these situations has been purely economical, the actions provide terrorists an excellent case study in target selection. That is to say, piracy activity has proven that large commercial vessels are highly vulnerable targets for terrorists.

Al Qaeda and other terrorist organizations have shown both interest and a history of attacking large vessels, both commercial and military. In January 2000, al Qaeda attempted and failed to attack the USS SULLIVANS docked in Yemen via a boat bomb. Having learned from the first attempt, the organization successfully attacked the USS COLE in October of that year. In 2002, Al Qaeda attacked the French oil tanker LIMBURG, and during that same year, Moroccan officials disrupted an al Qaeda plot against British and American tankers in the Strait of Gibraltar.[138]

Maritime terrorist attacks have not been limited to al Qaeda. In 2004, Abu Sayyaf conducted a bombing attack on a large ferry in the Philippines that sank the SUPERFERRY 14 and killed 116 people.[139] This attack showed that an attack on a large passenger vessel has the potential for inflicting mass casualties in a single successful

[138] Gal Luft and Anne Korin, "Terrorism Goes to Sea," *Foreign Affairs*, November/December 2004.

[139] Simon Elegant and Kuala Sepetang, "Dire Straits," *Time*, November 29, 2004.

attack. In 2009, Pakistani bureau chief, Syed Saleem Shahzad, reported that an emerging priority for al Qaeda was precisely the disruption and destabilization of sea routes between Somalia and Yemen,[140] and in May 2009, al Qaeda issued direction to its followers to attack strategic maritime chokepoints as a way to destabilize the global economy.[141] In July 2009, Egyptian authorities arrested over 20 individuals, which they claim were an al Qaeda cell. During the raid explosives, electronic devices, and diving equipment were seized. The men are charged with planning attacks on ships traveling within the Suez Canal.[142] These maritime threats highlight the relevance of alternative analysis red teaming programs to identify potential attack methods and security programs' ability to address maritime attacks

A red teaming program could provide the current Coast Guard MSRAM quantitative data on the abilities of would-be terrorist actors within the domestic maritime domain, as well as identify potential future attack scenarios. Specifically, an alternative analysis program focusing on red teaming concepts to identify and define would be attackers' abilities, and potential attack methods would directly support the current MSRAM process. Red teaming would reduce the Coast Guard MSRAM programs singular reliance on SME judgments for calculating would-be terrorists abilities, as well as integrating within the current risk assessment system vice replacing it. A third policy analysis component would round out a red teaming progam by assessing anti-terrorism polices from an adverasiral point of view.

[140] Syed Saleem Shahzad, "Al-Qaeda Sniffs Opportunity in Gaza," *Asia Times*, January 7, 2009.

[141] Peter Chalk, "Assessing the Recent Terrorist Threat to the Malacca Strait," *CTC Sentinel* 3, no. 4 (2010): 8–10.

[142] "Egypt Arrests 25 in 'Suez Plot,'" *BBC*, July 9, 2009.

C. PROGRAM ELEMENTS

The domestic maritime anti-terrorism red team program would be comprised of three components:

- A physical red teaming component. This element identifies the capabilities of would-be attackers to conduct elements of a terrorist attack within the maritime domain. The program's outputs would be quantifiable data elements incorporated into the existing MSRAM program.
- The identification of future attack scenarios. This element assesses emerging technologies and their potential application for terrorist attacks within the domestic maritime domain. The program's outputs would include the descriptions of the technologies, application within the domestic maritime domain, and potential countermeasures.
- A policy red teaming component. This element assesses the level which policy meets the strategic goals. Specifically, how Coast Guard domestic maritime anti-terrorism policies reduce the risk of terrorist attacks.

1. Physical Attack Abilities

This program assesses physical abilities of would-be terrorist actors within the domestic maritime domain. Following accepted steps in the development of a red teaming process, such as those identified by Sandia National Labs,[143] both physical and virtual red teaming protocols provide a baseline and continual assessment of potential attackers' ability to execute the various steps of identified attack scenarios. This assessment captures adversaries' abilities to execute potential techniques, but not their intent. The program provides a continual update on potential attack methods, and identifies the possible use of new technologies and methods by would-be attackers. The assessment results are both qualitative and quantitative in nature and are transferable directly into the Coast Guard MSRAM risk analysis program.

Table 3 provides a set of attack scenarios and methods for specific targets to assess an adversary's abilities.

[143] "Red Teaming for Program Mangers."

Table 3. Physical Attack Red Team Program[144]

Conduct Surveillance	Identify Targets	Establish Logistics	Establish Staging	Gain Access	Conduct Attack
Identify areas that provide the capacity to observe and intended target for extended periods and conduct surveillance of security activities and critical functions. Remain undetected while conducting surveillance. Collect data in open public areas while remaining undetected	Translate surveillance data into targets selection criteria	Acquire equipment to conduct stages of an attack. Train for all phases of an attack undetected Conduct trial runs of attack scenarios and collects intelligence on security procedures	Identify and procure housing for support and attack teams Identify and procure equipment Identify storage areas for all equipment, vehicles, weapons	Identify primary and secondary ingress routes for various attack methods Use concealment to remain undetected during ingress Avoid or bypass intrusion detection systems Overcome personnel and item screening systems Overcome obstacles to ingress both natural and manmade; fences, vehicle barriers	Execute physical attack procedures

2. Future Attack Scenarios

This program assesses emergent technologies, social constructs, and other factors to identify and capture data on future attack scenarios within the domestic maritime

[144] Adapted from U.S. Coast Guard Port Security Evaluation Team, *Indicators of Terrorist Activity Handbook* (Washington, DC: Port Security Assessment Office, 2006).

domain, as shown in Table 4. This alternative analysis program provides value to the Coast Guard's anti-terrorism program by providing an "examination of the tools and tactics available to terrorists, it is possible to establish intelligence profiles and threat indicators to warn of potential attacks and other operations."[145] This information is mostly qualitative in nature, and provides direction for the physical and policy red teaming programs.

Table 4. Future Scenarios Functions[146]

Assessment	Analysis
Highlight unidentified Attacks Scenarios	Insight into adversaries intentions, perceptions, and decision making methods
Identification of future technologies potential exploitation by an adversaries	Identification of adversaries alternative actions and responses to situations or inputs

3. Policy Assessment

This program assesses the Coast Guard's policies ability to meet anti-terrorism goals and objectives. The program reviews policy to identify gaps and vulnerabilities from an adversarial perspective. An excellent example of such a program is the 2010 2010 Winter Olympic Games efforts of the Government of Canda described previously. The efforts of the GRT offer an example of how to leverage red teaming in planning and policy development. Similar to the GRT program, a domestic maritime red teaming policy program focuses on "discovery learning"; an intellectual approach to analyze planning cycles, assumptions, and policy.[147] In doing so, the policy red team seeks to "challenge … conformity, convention, and orthodoxy while encouraging self-discovery and learning"[148] within the policy development ranks.

[145] Anna Culpeper, "Effectiveness of Using Red Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack" (master's thesis, Naval Postgraduate School, 2004), 59.

[146] Developed by author, pre-decisional information, October 2015

[147] Wilner, "Terrorism in Canada: Victims and Perpetrators," 93.

[148] Ibid.

Applying alternative analysis techniques to security planning helps identify atypical threats, exemplified by 9/11, and allows analysts and decision makers to stretch their understanding of emerging threat environments.[149] Playing Devil's advocate is a form of red teaming derived from alternative analysis well suited for policy assessment, as presented in Table 5. Devil's advocate techniques include "critiques of, and in some cases alternatives to, the enterprise's assumptions, strategies, plans, concepts, programs, projects, and processes. At the program level, the objective of this type of red team is to provide critical analysis in order to anticipate problems and avoid surprises."[150]

Table 5. Policy Red Teaming Functions[151]

Alternative Policy Review	**Alternative Analysis**
Existing Policies	Problem Sets
Developmental Policies	Metrics
Doctrine	Trends
	Effectiveness Standards

[149] Fishbein and Treverton, "Rethinking "Alternative Analysis" to Address Transnational Threats," 2–3.

[150] Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *The Role and Status of DOD Red Teaming Activities*, 4.

[151] Developed by author, pre-decisional information.

THIS PAGE INTENTIONALLY LEFT BLANK

V. IMPLEMENTATION CONSIDERATIONS

A. MINIMAL VIABLE PROGRAM FOR GOVERNMENT AGENCIES

In business terms, a startup is described as "a human institution designed to create a new product or service under conditions of extreme uncertainty."[152] A key component within the startup framework is a minimal viable product. "A Minimum Viable Product is that version of a new product which allows a team to collect the maximum amount of validated learning about customers with the least effort."[153] In other terms, a minimum viable product is "the smallest thing you can build that delivers customer value (and as a bonus captures some of that value back)."[154] Another trait of a startup is entrepreneurship. "Anyone who is creating a new product or business under conditions of extreme uncertainty is an entrepreneur whether he or she knows it or not and whether working in a government agency, a venture-backed company, a nonprofit, or a decidedly for-profit company with financial investors."[155]

Startup concepts can apply to government as well. Policy development can be executed in a similar manner. Terms, such as beta testing or pilot programs, are commonly used, and are in fact, examples of startup approaches within federal government. As policies and programs are generally the core products government agencies produce, it is suggested in this thesis that the product of a startup in the federal government can be described as a minimal viable program. The author defines a minimum viable program as the collection of initial policy, TTP, and tools entered into a learning loop to establish a program, while improving and developing its elements to meet the strategic objective(s) of an agency.

---

[152] Ries, *The Lean Startup: How Today's Entrepreneurs use Continuous Innovation to Create Radically Successful Businesses*, 26.

[153] Ibid., 70.

[154] Maurya, "Minimum Viable Product."

[155] Ries, *The Lean Startup: How Today's Entrepreneurs use Continuous Innovation to Create Radically Successful Businesses*, 27.

The Coast Guard recently developed a policy in such a manner, developing and deploying what is known as risk based maritime security response operations (RBMSRO). The program updated existing policy and tools, and transitioned domestic maritime security activity requirements to a risk-based planning and reporting program for domestic maritime anti-terrorism efforts.

The program was run as a government startup; a small development team with a minimal budget developed an experimental policy and a prototype planning and reporting tool. The program was tested at a handful of seaports, took input, and adjusted both policy and the tool over the course of 12 months. The system was continuously evaluated and updated during the process, with an end result of having the program up and running at every seaport, and across the Coast Guard within 12 months of starting. Results and development were encouraging, and built a basis for risk-based resource management with an approach flexible enough to transition to other mission spaces.

The 12-months period acted as both a development cycle and proof of concept. The policy and tool won acceptance and funded. It is currently undergoing an integration phase leading to becoming the Coast Guard program of record for maritime anti-terrorism programs. This minimal viable program approach could be replicated with other programs, including the alternative analysis red teaming concepts proposed in this thesis.

Using RBMSRO implementation as an example, a maritime security alternative analysis red team program can be implemented via a minimal viable program approach. This approach allows for rapid implementation, scalability, and the ability to react and pivot to meet new demands and challenges. The following paragraphs discuss some challenges and proposed solutions for implementing an alternative analysis red teaming program for the domestic maritime domain.

B. CONSIDERATIONS FOR IMPLEMENTING A DOMESTIC MARITIME ANTI-TERRORISM RED TEAMING PROGRAM

Programs must be nurtured to survive within the bureaucracy of the federal government. A program leader must have the skills and knowledge to maneuver with and through government circles and protocols to ensure success. This chapter discusses some

of challenges and opportunities in implementing a domestic maritime anti-terrorism red team program.

In a democratic system, it simply is not possible to pay off a select few people to ensure they remain in power. Rather, it is essential to keep a larger population's favor; normally, by the development of good and popular public policy.[156] The proposed set of programs within this thesis will depend on two groups of people to "remain in power." The first is the existing domestic maritime terrorism risk analysis enterprise currently in place within the Coast Guard. Moreover, the second is the senior leadership who make up the "ruling coalition"[157] of the Coast Guard.

Leaders will be dependent on the first group to execute and continue to develop the program. Their willingness to do so depends on two factors, first that the program provides value to the existing terrorism risk analysis construct, and secondly, that the program is supported by senior leadership (the identified second group). Senior Coast Guard leadership, the second group, will support this program if it provides a cost effective means to articulate the threats of terrorism within the domestic maritime domain.

Of concern is the relatively small pool of people upon which the program will be dependent. The group of people who work within the current terrorism risk analysis enterprise is relatively small when compared to other Coast Guard programs. Additionally, the group of senior leaders who directly influence these programs is relatively small as well. To offset the associated risks, the program must focus on expanding the pool of supporters from senior leaders Coast Guard-wide.

To implement and sustain the proposed set of red teaming programs, it will be important to have those working within, and customers of Coast Guard terrorism risk analysis, dependent upon these red teaming programs. To accomplish this dependency,

---

[156] Bruce Bueno De Mesquita and Alastair Smith, *The Dictator's Handbook: Why Bad Behavior Is Almost Always Good Politics* (New York: Public Affairs, 2011), 41.

[157] Diana T. Richards et al., "Good Times, Bad Times, and the Diversionary Use of Force a Tale of Some Not-So-Free Agents," *Journal of Conflict Resolution* 37, no. 3 (1993): 504–535.

the programs must provide some early "wins" by showing unique perspectives in the arena of terrorism risk analysis.

As compared to other programs, Coast Guard terrorism risk assessment and mission policy development does not have a large budget. However, anti-terrorism activities equate to about 1/3 of all Coast Guard resource hours, which are allocated across 11 mission areas.[158] Providing value-added information upon which to base budgetary and policy decisions will encourage senior leaders from across the organization to support red teaming programs. Those involved in the programs are "paid" when leadership values their analysis, and bases organization-wide decisions upon it. Currency by which to "pay off" those who will keep this program in power, or even started, is in providing a value added alternative assessment that supports senior leader decision making.

Having a set of programs that define terrorist abilities, identify potential future risks, and evaluate current policy from an adversaries' point of view are powerful tools for senior level decision making. It will be imperative for these red teaming programs to focus on providing unique, value-added analysis that cannot otherwise be provided by existing programs. It will both strengthen the programs' value, as well as narrow the number of elements they are dependent upon to remain viable.

For such a program to be sucessful, it must leverage support from a wide-ranging group, or the "nominal selecotate pool."[159] According to De Mesquita, leaders must identify those within this pool whose support is truly influential. A leader, organization, or program is dependent upon various groups to remain sucessful. "A simple way to think of these groups is: interchangeables, influentials, and essentials."[160]

The interchangeables for the proposed red team programs are the Coast Guard program managers associated with anti-terrorism policy management. The influentials are made up of the office chiefs in these policy areas; namely, the Office of Maritime

[158] Derived from author's policy development research.

[159] Bueno De Mesquita and Smith, *The Dictator's Handbook: Why Bad Behavior Is Almost Always Good Politics*, 4–5.

[160] Ibid.

Security Response Policy, and the Office of Port Security Assessment. Finally, the essentials are the senior leaders who have oversight in anti-terrorism efforts.

The set of red team programs this thesis proposes will provide value-added analysis to a wide Coast Guard audience. Current terrorism risk analysts will benefit from qualitative and quantitative assessments of terrorist abilities within the domestic maritime domain, and future attack scenarios. Senior leadership will likewise benefit from those programs' input to the decision-making processes. Additionally, the entire organization will benefit from a policy of the red teams' ability to identify weaknesses in the policies' abilities to meet the goals of the organization.

A "winning coalition" for Coast Guard terrorism red teaming would be comprised of elements across the organization. Red team programs would be ingrained into the Coast Guard terrorism risk enterprise, with red team analysis interwoven into decisions regarding attack scenarios and target selection. Senior leadership would be dependent upon, and factor in, red team analysis into policy, budget, and acquisition decisions for the organization.

Many companies have failed when "confronted with disruptive changes in technology and market structure."[161] At its core, red teaming provides analysis to inform senior leaders of potential, or normally, unseen disruptive events. Additionally, red team programs must be able to detect and account for disruptive trends that could threaten their viability in an organization. To remain worthwhile, red team programs must strive to provide analysis that is functionally valuable and digestible by the decision-making mechanisms of an organization, including the approaches of senior leadership.

In conclusion, the red team programs the author has proposed within this thesis can provide value-added analysis to the Coast Guard. To succeed, and remain of value, these programs must be integrated into the existing Coast Guard terrorism risk analysis enterprise, provide digestible analysis to senior leadership, and support the overall goals

[161] Clayton M. Christensen, *The Innovator's Dilemma: The Revolutionary Book that Will Change the Way You Do Business* (New York: Collins Business Essentials, 1997), 2.

of the organization. Failure to achieve and sustain these efforts would put considerable strain on a red team analysis system to remain a viable program within the Coast Guard.

1. Potential Road Blocks to Implementation

Two groups have been identified as potential inhibitors to the implementation of the programs. The first is described as the "status quo" group. These individuals, many of them long-time employees, generally consider the current terrorism risk analysis constructs within the Coast Guard meet the current analysis demand. They generally focus on efforts that add controls and management oversight elements to existing programs.

The second group is identified as the "legacy mission" group. These individuals place little value on programs that are not part of the suite of Coast Guard "pre-DHS" missions. They would view a terrorism red team analysis program as just another unneeded effort within the organization. They generally focus on efforts that expand upon the Coast Guard's non-homeland security missions.

2. Program Support

The USCG Commandant's strategic intent for 2015–2019 states, "Risk management and hazard prevention across the Maritime Transportation System (MTS) will remain essential to accomplishing our objectives of safety and security."[162] An alternative analysis red teaming program would directly support this approach and directly support one of the Commandant's strategic intents. Program alignment with leadership strategic intent drives support for the programs at the highest levels of the organization. These facts point to the two primarily policy development offices within the Coast Guard Headquarters, the Office of Response Policy, and the Office of Prevention Policy as the primary supporters for these programs.

The most direct means by which to offset potential roadblocks to successful acceptance of the programs is to produce early gains by providing an early on value

[162] United States Coast Guard, *Commandant's Strategic Intent 2015–2019* (Washington, DC: United States Coast Guard, 2015), https://www.uscg.mil/seniorleadership/DOCS/2015_CCGSI.pdf.

added alternative analysis that contributes to senior leadership decision making. Annual budget decisions and resource allocation are two primary areas in which these early wins could be accomplished within the annual planning cycle.

To support these decisions, the Coast Guard must have in place a suite of accepted risk assessment and analysis programs. As a fellow maritime security professional once stated and often continues to state, "In the absence of emotion and political influence, risk is where risk is."[163] Alternative assessment, in the form of red teaming, is a missing component within the Coast Guard's terrorism risk assessment and analysis programs. "The key to security, domestic or otherwise, is the continuous evaluation of the security environment while mitigating the risk of the decisions made to counter threats."[164]

C. LOGISTICS OF IMPLEMENTATION

It is proposed in this thesis that the current domestic maritime anti-terrorism analysis and policy directorates within the Coast Guard would execute each of the elements of a domestic maritime anti-terrorism red teaming program, as seen in Table 6. Red teaming cycles would be annual, and align with current terrorism risk assessment and analysis schedules.

[163] Brady Downs, "Maritime Security Risk Analysis Model (MSRAM), Balancing Resources to Risk," presentation for the Critical Infrastructure Protection Workshop, The Center for Homeland Defense and Security, presented by LCDR Brady Downs, USCG, Domestic Port Security Evaluations Division, U.S. Coast Guard Headquarters, Washington, DC, June 2008.

[164] Culpeper, "Effectiveness of Using Red Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack," 62.

Table 6. Proposed Coast Guard Domestic Maritime Anti-Terrorism Red Teaming Programs[165]

Program	Office	Outputs	Achievability
Physical Red Team Program	Office of International & Domestic Port Assessment	Qualitative and Quantitative injects into MSRAM	Medium effort now new emphasis for program
Future Red Team Program	Intelligence Coordination Center	Qualitative and Quantitative injects into threat reporting and MSRAM	Medium effort now new emphasis for program
Policy Red Team Program	Office of Strategic Analysis	Annual assessment of domestic maritime anti-terrorism policy	Significant effort 2–3 years new structure needed

The physical red teaming program could be implemented by leveraging existing terrorism risk analysis structure within the Coast Guard, as well as leveraging local, regional, and headquarters risk assessment staffs. Led by The Office of International & Domestic Port Assessment, it is envisioned that the program would be managed by PSA-2, which executes the MSRAM program for the Coast Guard.

Likewise, the future attack scenario red teaming program could leverage existing terrorism risk analysis structure within the Coast Guard; specifically, the ICC. The program would integrate into the ICC's annual MSRAM threat data processes and align efforts along the existing annual assessment cycles. As a new concept, the policy red team program would need further study to define its position in the organization. It is suggested that the program be established within the Coast Guard Office of Strategic Analysis.

D. USE OF COAST GUARD CADETS FOR RED TEAMING

To further leverage current Coast Guard resources, this thesis examines the use of Coast Guard Academy Cadets within the proposed alternative analysis red team programs as both red teaming members and program developers. The Coast Guard Academy is the only service academy with direct linkages to homeland security and resides within a

[165] Developed by author, pre-decisional information.

component of the DHS. "The Coast Guard Academy is also the only U.S. service academy with focused coursework and a continuum in Strategic Intelligence Studies."[166] Uniquely positioned, this institution can support Coast Guard red teaming programs and establish itself as the DHS red teaming center of excellence.

The study of alternative analysis red teaming, matched with the actual red teaming programs discussed within this thesis, would provide the Coast Guard, and DHS overall, with a value added program currently missing within the area of domestic maritime security. Inserting this course of study into the Coast Guard Academy has the added benefit of providing a steady stream of skilled officers with red teaming skill sets to the homeland security enterprise. A precedence does exist for the Coast Guard Academy educational program to provide value to and address Coast Guard challenges and efforts in the field. Coast Guard Academy operations research capstone project programs,[167] strategic intelligence studies,[168] and government security studies concentration are all areas of study with direct linkages to an alternative analysis red teaming concepts.

The Coast Guard should consider the continuous pool Academy Cadets as red teaming elements. This untapped resource represents a useful demographic of technology savvy individuals with basic maritime skill sets. By leveraging current risk assessment and analysis processes and incorporating Coast Guard Academy cadets as red teaming subjects, this program has the potential for the establishment with a minimal additional expenditure of funds of a homeland security center of excellence in an area of analysis that currently is nonexistent. This subject merits further research.

E. CONCLUSIONS

The domestic maritime domain is a complex system of transportation, recreation, and essential services linked by the waters of the United States. This operational domain

166 "Why Study Intelligence?" accessed July 21, 2015, http://www.cga.edu/academics.aspx?id=328.

167 "Operations Research and Computer Analysis Capstone Projects," accessed July 21, 2015, http://www.cga.edu/academics2.aspx?id=3096.

168 "2481 Intelligence and National Security Policy," accessed July 21, 2015, http://www.cga.edu/academics2.aspx?id=329.

can benefit from an alternative analysis red teaming program. "Red teaming is a white light that takes on various characteristics as it shines through the prism of different organizations."[169] Understanding the terrorist risk within the domestic maritime domain, through the eyes of those who would do harm is value added. "Successful red teaming offers a hedge against surprise and inexperience and a guard against complacency. It tests the fusion of policy, operations, and intelligence."[170]

For the Coast Guard, red teaming can directly support the organization's existing terrorism risk analysis enterprise with qualitative and quantitative assessments of terrorists physical attack abilities in the domestic maritime domain. Red teaming can further support risk analysis and policy development by identifying previously unidentified and future attack scenarios. Red teaming can further provide value by providing an analysis of current and under development policy from the adversarial point of view. "By using the red team concept, enterprises can draw on the perspective of the adversary to challenge their assumptions and their countermeasures."[171]

Doctrine, practices, and procedures for providing homeland defense and security are based upon science and analysis, "however, Defence (and security) is an organization founded on a set of people with a specific culture, and way of thinking and operating."[172] These foundations are powerful management tools. However, as discussed, they can also blind an organization to potentially hazardous risks. As stated by Sun Tzu, "…if ignorant of both your enemy and yourself you are bound to be in peril…."[173]

To support these decisions, agencies must have in place adequate and accepted risk assessment and analysis programs. As a fellow maritime security professional once stated and often continues to state, "In the absence of emotion and political influence, risk

---

[169] Brendan Mulvaney, "Don't Box in the Red Team," *Armed Forces Journal*, November 1, 2012, http://www.armedforcesjournal.com/dont-box-in-the-red-team/.

[170] Meehan, "Red Teaming for Law Enforcement."

[171] Culpeper, "Effectiveness of Using Red Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack," 62.

[172] UK Ministry of Defense, *Red Teaming Guide*, 1–1.

[173] Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1963).

is where risk is."[174] Decision makers must take into account the risks associated with terrorism and base their actions upon those risks despite the political and other pressures aimed at them. This charge is placed upon homeland security professionals. "The key to security, domestic or otherwise, is the continuous evaluation of the security environment while mitigating the risk of the decisions made to counter threats."[175]

The research conducted for this thesis highlights a role for social identity theory in red teaming. It can be leveraged to define functions of red teaming, as well as assist in the avoidance of some of the more common pitfalls and biases of analysts. This subject warrants further research and development.

It is recommended that an alternative analysis program red teaming program be established within the Coast Guard. The program elements should define would-be attacker abilities and potential attack methods. The output of these programs are structured to allow for direct incorporation into the Coast Guard MSRAM terrorism risk assessment program. As the lead federal maritime security agency, the Coast Guard is the ideal organization to lead and manage this program. Leveraging its regulatory authorities, as well as its responsibilities within the maritime transportation sub-sector, the Coast Guard has the authorities and responsibility to execute such a program.[176]

It is envisioned that this program would include two types of red teaming approaches, analytical and physical. The analytical focuses upon an alternative analysis of policies and programs, while the physical focuses its efforts on the tactics and techniques of terrorist actors within the domestic maritime domain. The domestic maritime security red teaming program described in this thesis should be integrated with the existing Coast Guard intelligence and terrorism risk assessment and analysis programs to support senior decision makers and maritime security policy developers.

---

[174] Downs, "Maritime Security Risk Analysis Model (MSRAM), Balancing Resources to Risk."

[175] Culpeper, "Effectiveness of Using Red Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack," 62.

[176] "Office of Counterterrorism & Defense Operations Policy (CG-DOD), Ports, Waterways & Coastal Security (PWCS), Introduction," last modified October 31, 2014, http://www.uscg.mil/hq/cg5/cg532/pwcs.asp.

Through this red team program, Coast Guard anti-terrorism programs will continue to evolve and keep pace with future threats to the domestic maritime domain.

LIST OF REFERENCES

American Association of Port Authorities (AAPA). "U.S. Port Industry." Accessed December 8, 2014. http://www.aapa-ports.org/industry.

Brewer, Gary, and Martin Shubik. *The War Game: A Critique of Military Problem Solving*. Cambridge MA, Harvard University Press, 1979.

Bueno De Mesquita, Bruce, and Alastair Smith. *The Dictator's Handbook: Why Bad Behavior Is Almost Always Good Politics*. New York: Public Affairs, 2011.

Bunker, Robert. *Terrorists and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications*. Carlisle, PA: The United States Army War College Strategic Studies Institute, 2015.

Chalk, Peter. "Assessing the Recent Terrorist Threat to the Malacca Strait." *CTC Sentinel* 3, no. 4 (2010): 8–10.

Christensen, Clayton M. *The Innovator's Dilemma: The Revolutionary Book that Will Change the Way You Do Business*. New York: Collins Business Essentials, 1997.

Committee on the Marine Transportation System. *National Strategy for the Marine Transportation System: A Framework for Action*. Washington, DC: The Secretary of Transportation, 2008.

Cox, Louis Anthony. "Some Limitations of Risk= Threat x Vulnerability x Consequence for Risk Analysis of Terrorist Attacks." *Risk Analysis International Journal* 28, no. 6 (December 2008): 749–1761.

Craft, Richard. *A Concept for the Use of Red Teams in Homeland Defense*. Livermore, CA: Sandia National Laboratories, 2002.

Culpeper, Anna. "Effectiveness of Using Red Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack." Master's thesis, Naval Postgraduate School, 2004.

Cupp, Shawn, and Michael G. Spight. *A Homeland Security Model for Assessing U.S. Domestic Threats*. Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2007.

Department of Defense and Homeland Security. *National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security*. Washington, DC: Department of Defense and Homeland Security, 2005.

Department of Homeland Security Homeport. "Maritime Transportation Security Act." Accessed December 8, 2014. https://homeport.uscg.mil.

Department of Homeland Security. *DHS Announces Grant Guidance for Fiscal Year (FY) 2014 Preparedness Grants*. Washington, DC: DHS Press Office, 2014.

———. *Safety, Security and Stewardship*. Washington, DC: Director of Strategic Management and Doctrine, U.S. Coast Guard Headquarters, 2011.

Department of the Navy. *Naval Doctrine Publication 2: Naval Intelligence*. Norfolk, VA: Naval Warfare Development Command, 2008. http://www.nwdc.navy.mil/content/Library/Documents/NDPs/ndp2/ndp20007.htm.

Downs, Brady. "Maritime Security Risk Analysis Model (MSRAM), Balancing Resources to Risk." Presentation for the Critical Infrastructure Protection Workshop, The Center for Homeland Defense and Security. Presented by LCDR Brady Downs, USCG, Domestic Port Security Evaluations Division, U.S. Coast Guard Headquarters. Washington, DC, June 2008.

Elegant, Simon, and Kuala Sepetang. "Dire Straits." *Time*, November 29, 2004.

FEMA. "Building Design for Homeland Security." Accessed December 8, 2014. http://www.fema.gov/pdf/plan/prevent/rms/155/e155_unit_v.pdf.

Financial Times. "Definition of Red Team." Accessed January 11, 2015. http://lexicon.ft.com/Term?term=red-team.

Fishbein, Warren, and Gregory Treverton. "Rethinking "Alternative Analysis" to Address Transnational Threats." Occasional Papers, *Sherman Kent Center, Central Intelligence Agency* 3, no. 2 (October 2004). https://www.cia.gov/library/kent-center-occasional-papers/vol3no2.htm.

George, Roger Z. "Fixing the Problem of Analytical Mindsets." In *Intelligence and the National Security Strategist*, edited by Roger Z. George and Robert D. Kline. Lanham, MD: Rowman & Littlefield, 2006.

Greenberg, Michael D., Peter Chalk, Henry H. Willis, Ivan Khilko, and David S. Ortiz. *Maritime Terrorism, Risk and Liability*. Santa Monica, CA: RAND, 2006.

Handel, Michael I. *War, Strategy, and Intelligence*. London: Frank Cass, 1989.

IBISWorld. "Business Environment Profiles—Total Import." March 2014. http://clients1.ibisworld.com.nduezproxy.idm.oclc.org/reports/us/bed/default.aspx?entid=1533.

Joint Task Force Games (Games Red Team). *Final Report: Vancouver 2010 Olympic and Paralympic Winter Games*. Vancouver, Canada: Joint Task Force Games (Games Red Team), 2010.

Kutz, Gregory, and John Cooney. *Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process: Testimony before the Committee on Oversight and Government Reform, House of Representatives.* (GAO-08-48T). Washington, DC: U.S. Government Accountability Office, 2007.

Lauder, Matthew. "Red Dawn: The Emergence of a Red Teaming Capability in the Canadian Forces." *Canadian Army Journal* 12, no. 2 (2009): 25–36.

Luft, Gal, and Anne Korin. "Terrorism Goes to Sea." *Foreign Affairs*, November/ December 2004.

Malone, Timothy, and Reagan Schaupp. "The Red Team, Forging a Well-Conceived Contingency Plan." *Aerospace Power Journal* XVI, no. 2 (Summer 2002).

Mateski, Mark. "Why We Red Team: The Tyranny of Uncertainty." *Red Team Journal*, November 2014.

Matherly, Carter M. *The Red Teaming Essential, Social Psychology Premier for Adversarial Based Alternative Analysis.* Charles Town, WV: American Military University, 2013.

Maurya, Ash. "Minimum Viable Product." LeanStack. Accessed July 21, 2015. http:// practicetrumpstheory.com/minimum-viable-product.

McGannon, Mike. "Developing Red Team Tactics, Techniques and Procedures." *Red Team Journal*, April 2004.

McLeod, Saul A. "Social Identity Theory." *Simple Psychology*, 2008. http://www.simply psychology.org/social-identity-theory.html.

Meehan, Michael. "Red Teaming for Law Enforcement." *The Police Chief* 74, no. 2 (February 2007). http://www.policechiefmagazine.org/magazine/index.cfm? fuseaction=print_display&article_id=1111&issue_id=22007.

Moghaddam, Fathali M. *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy*. Santa Barbara, CA: Praeger Security International, 2006.

———. "Multiculturalism and Intergroup Relations." *American Psychological Association*, November 2011.

Moore, Judy, John Whitley, and Rick Craft. *Red Gaming in Support of the War on Terrorism: Sandia Red Game Report*. (SAND2004-0438). Albuquerque, NM and Livermore, CA: Sandia National Laboratories, 2004.

Mulvaney, Brendan. "Don't Box in the Red Team." *Armed Forces Journal*, November 1, 2012. http://www.armedforcesjournal.com/dont-box-in-the-red-team/.

National Commission on Terrorist Attacks upon the United States. *Final Report of the National Commission on Terrorist Attack upon the United States*. Washington, DC: National Commission on Terrorist Attacks upon the United States.

Nettles, A. Bentley. "The President Has No Clothes: The Case for Broader Application of Red Teaming within Homeland Security." Master's thesis, Naval Postgraduate School, 2010.

Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics. *The Role and Status of DOD Red Teaming Activities*. Washington, DC: Department of Defense, 2003.

Oxford Dictionaries. "Risk Management." Accessed January 14, 2015. http://www.oxforddictionaries.com/us/definition/american_english/risk-management.

Red Team Journal. "Red Teaming and Alternative Analysis." Accessed January 11, 2015. http://redteamjournal.com/about/red-teaming-and-alternative-analysis/.

Ressler, Steve. "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research." *Homeland Security Affairs* 2, art. 8 (July 2006). https://www.hsaj.org/articles/171.

Richards, Diana, T. Clifton Morgan, Rick K. Wilson, Valerie L. Schwebach, and Garry D. Young. "Good Times, Bad Times, and the Diversionary Use of Force a Tale of Some Not-So-Free Agents." *Journal of Conflict Resolution* 37, no. 3 (1993): 504–535.

Ries, Eric. *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses*. New York: Random House LLC, 2011.

Risk Steering Committee. *DHS Risk Lexicon 2010 Edition*. Washington, DC: U.S. Department of Homeland Security, 2010.

Sandia National Labs. "Red Teaming for Program Managers." 2009. http://www.idart.sandia.gov/methodology/RT4PM.html.

Shahzad, Syed Saleem. "Al-Qaeda Sniffs Opportunity in Gaza." *Asia Times*, January 7, 2009.

Shelley, Kirkpatrick, Shelly Asher, and Catherine Bott. *Staying One Step Ahead: Advancing Red Teaming Methodologies through Innovation*. Arlington, VA: Homeland Security Institute, 2005.

Social Research Methods. "Qualitative Data" Last revised October 20, 2006. http://www.socialresearchmethods.net/kb/qualdata.php.

Tajfel, Henri. *Human Groups and Social Categories*. Cambridge, MA: Cambridge University Press, 1981.

Trujilo, Mario. "FAA Bolsters Drone Outreach with New Hires." *The Hill*, September 2015.

Tuchman, Barbar. *The Guns of August*. New York: Macmillan Publishing Co., Inc., 1962.

Turner, John C. *Rediscovering the Social Group: A Self-Categorization Theory*. Oxford: Basil Blackwell, 1987.

Tzu, Sun. *The Art of War*. Oxford: Oxford University Press, 1963.

U.S. Coast Guard Port Security Evaluation Team. *Indicators of Terrorist Activity Handbook*. Washington, DC: Port Security Assessment Office, 2006.

U.S. Department of Homeland Security. "National Infrastructure Protection Plan, Transportation Systems Sector." Accessed December 9, 2014. http://www.dhs.gov/xlibrary/assets/nipp_transport.pdf.

———. "Preventing Terrorism and Enhancing Security." Last published August 26, 2015. http://www.dhs.gov/preventing-terrorism-and-enhancing-security.

U.S. Government Accountability Office. *COAST GUARD Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*. (GAO-12-14). Washington, DC: U.S. Government Accountability Office, 2011.

———. *Ferry Security Measures Have Been Implemented, but Evaluating Existing Studies Could Further Enhance Security*. (GAO-11-207). Washington, DC: U.S. Government Accountability Office, 2010.

———. *Testimony Before the Subcommittee on Emergency Management, Intergovernmental Relations, and the District of Columbia, Committee on Homeland Security and Government Affairs, U.S. Senate, National Preparedness—FEMA Has Made Progress, But Additional Steps Are Needed to Improve Grant Management and Assess Capabilities* (Statement of David C. Maurer, Director Homeland Security and Justice). (GAO-13-637T). Washington, DC: U.S. Government Accountability Office, 2013.

———. *Testimony Before the Subcommittee on Transportation Security and Infrastructure Protection, Homeland Security Committee, House of Representatives, Risk Management, Strengthening the Use of Risk Management Principles in Homeland Security* (Statement of Norman J. Rabkin, Managing Director, Homeland Security and Justice). (GAO-08-904T). Washington, DC: U.S. Government Accountability Office, 2008.

UK Ministry of Defense. *Red Teaming Guide*. 2nd ed. London: UK Ministry of Defense, 2013.

United State Coast Guard. “U.S. Coast Guard Port Waterways, and Coast Security.” Last modified October 31, 2014. http://www.uscg.mil/hq/cg5/cg532/pwcs.asp.

United States Army. *Field Manual 5–0*. Washington, DC: United States Army, 2010.

United States Coast Guard Academy. “2481 Intelligence and National Security Policy.” Accessed July 21, 2015. http://www.cga.edu/academics2.aspx?id=329.

———. “Operations Research and Computer Analysis Capstone Projects.” Accessed July 21, 2015. http://www.cga.edu/academics2.aspx?id=3096.

———. “Why Study Intelligence?” Accessed July 21, 2015. http://www.cga.edu/academics.aspx?id=328.

United States Coast Guard. *Commandant’s Strategic Intent 2015–2019*. Washington, DC: United States Coast Guard, 2015. https://www.uscg.mil/seniorleadership/DOCS/2015_CCGSI.pdf.

———. “Maritime Security, Risk Analysis Model.” Accessed January 14, 2015. http://aapa.files.cms-plus.com/PDFs/MSRAMBrochureTrifold.pdf.

———. “Office of Counterterrorism & Defense Operations Policy (CG-DOD), Ports, Waterways & Coastal Security (PWCS), Introduction.” Last modified October 31, 2014. http://www.uscg.mil/hq/cg5/cg532/pwcs.asp.

University of Foreign Military and Cultural Studies. *Red Team Handbook*. Ft. Leavenworth, KS: Department of the Army, 2011.

———. *The Applied Critical Thinking Handbook (formerly the Red Team Handbook*. Ft. Leavenworth, KS: University of Foreign Military and Cultural Studies, 2015. http://usacac.army.mil/sites/default/files/documents/ufmcs/The_Applied_Critical_Thinking_Handbook_v7.0.pdf.

Victoroff, Jeff. “The Mind of the Terrorist.” *Journal of Conflict Resolution* 49, no. 1 (February 2005): 3–42.

Werman, Marco, and Drake Bennet. “Holy Ship! Triple E—The Biggest Container Ship in the World.” *PRI The World*, September 9, 2013. http://www.pri.org/stories/2013-09-09/holy-ship-triple-e-biggest-container-ship-world.

Wilner, Alex S. “Terrorism in Canada: Victims and Perpetrators.” *Journal of Military and Strategic Studies* 12, no. 3 (Spring 2010): 72–99.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California