NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**THE TOOLS OF PREVENTION:
BUILDING PREVENTION AND DETERRENCE INTO
EXERCISE PROGRAMS**

by

Michael K. Meehan

September 2006

Thesis Advisor:	Christopher Bellavita
Second Reader:	Brady O'Hanlon

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL
POSTGRADUATE
SCHOOL

DUDLEY KNOX LIBRARY.

September 10, 2008

SUBJECT: Change in distribution statement for *Tools of Prevention: Building Prevention and Deterrence into Exercise Programs* – September 2006.

1. Reference: Meehan, Michael K. *Tools of Prevention: Building Prevention and Deterrence into Exercise Programs*. Monterey, CA: Naval Postgraduate School, September 2000. UNCLASSIFIED [Distribution authorized to U.S. Government Agencies and their Contractors].

2. Upon consultation with NPS faculty, the School has determined that the main body of this thesis may be released to the public and that its distribution is unlimited, effective February 15, 2008.

3. Appendices A and B have been re-released under separate cover as a limited distribution document.

University Librarian
Naval Postgraduate School

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** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: The Tools of Prevention: Building Prevention and Deterrence into Exercise Programs			**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael K. Meehan			
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.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT ~~Distribution authorized to U.S. Government Agencies and their Contractors; (Operational Use); (September 2006). Other requests for this document must be referred to President, Code 261, Naval Postgraduate School, Monterey, CA 93943-5000 (or Seattle Police Department) via the Defense Technical Information Center, 8725 John J. Kingman Rd., STE 0944, Ft. Belvoir, VA 22060-6218.~~ Approved for public release; Distribution is unlimited			**12b. DISTRIBUTION CODE** ~~C~~ A
13. ABSTRACT (maximum 200 words) This thesis will briefly explore the questions surrounding why prevention has typically not been incorporated into homeland security exercises and strives to document and demonstrate that prevention can be exercised. It will look at various prevention strategies, most notably, "All-Crimes," Information Sharing, Private Sector Security, Attack Trees, Red-Teaming, and Behavioral Analysis, to determine how these prevention-related tools can be integrated into exercise design and conduct. These tools can be used in exercises individually or in groups. They are, however, not the end-state, as other tools undoubtedly exist. Prevention as a science and a skill is still in its infancy; with additional research, analysis, and practice, maturity will come. This thesis also endeavors to provide a road map for agencies desiring to understand and exercise prevention activities. Understanding that prevention can be practiced and exercised through the use of certain tools is one significant step in having the guidance necessary to begin a prevention exercise, or better, a complete prevention exercise program. Agencies using these tools, working within the Homeland Security Exercise and Evaluation Program (HSEEP) Guidelines, and using technical expertise available from local, national, and federal subject-matter experts, should have that road map.			
14. SUBJECT TERMS Prevention, Deterrence, Crime Prevention, All-Crimes, Attack Trees, Red Teams, Information Sharing Environment Analysis, Behavioral Analysis, Private Sector Security, TOPOFF, Terrorism Exercise Prevention Program, Homeland Security, Terrorism, Exercises, Training			**15. NUMBER OF PAGES** 138 **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 ~~UL~~

THIS PAGE INTENTIONALLY LEFT BLANK

THE TOOLS OF PREVENTION: BUILDING PREVENTION AND DETERRENCE INTO EXERCISE PROGRAMS

Michael K. Meehan
Captain, Seattle Police Department
B.A., University of Washington, 2001

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
September 2006**

Author: Michael K. Meehan

Approved by: Christopher Bellavita
Thesis Advisor

Brady K. O'Hanlon
Second Reader

Douglas Porch, Ph.D.
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis will briefly explore the questions surrounding why prevention has typically not been incorporated into homeland security exercises and strives to document and demonstrate that prevention can be exercised. It will look at various prevention strategies, most notably, "All-Crimes," Information Sharing, Private Sector Security, Attack Trees, Red-Teaming, and Behavioral Analysis, to determine how these prevention-related tools can be integrated into exercise design and conduct. These tools can be used in exercises individually or in groups. They are, however, not the end-state, as other tools undoubtedly exist. Prevention as a science and a skill is still in its infancy; with additional research, analysis, and practice, maturity will come.

This thesis also endeavors to provide a road map for agencies desiring to understand and exercise prevention activities. Understanding that prevention can be practiced and exercised through the use of certain tools is one significant step in having the guidance necessary to begin a prevention exercise, or better, a complete prevention exercise program. Agencies using these tools, working within the Homeland Security Exercise and Evaluation Program (HSEEP) Guidelines, and using technical expertise available from local, national, and federal subject-matter experts, should have that road map.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK A

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

The research for this thesis was conducted in cooperation with the Department of Homeland Security through the National Exercise Program and the Terrorism Prevention Exercise Program (TPEP) in their efforts to implement prevention-oriented exercises.

Special thanks are due to Chris Bellavita, my Thesis Advisor, and Brady O'Hanlon, my Second Reader. I also owe thanks to Jonathan Cleck, Joseph Autera, and the Terrorism Prevention Exercise Program team for their invaluable assistance during the writing of this thesis. Thanks also to "Butch" Colvin, Branch Chief in the National Exercise Program for his advice and assistance, and to Chief of Police Gil Kerlikowske for his support during this effort.

Finally, and most importantly, thank you to my wife and two children for their patience, understanding, assistance, and support in this and every other endeavor.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

Traditionally, homeland security exercises have focused on the activities of first responders. This is not surprising since responder activities are the easiest to conceptualize, the most straightforward to plan and the simplest to objectively document. Moreover, response and recovery plans are relatively easy to test and stress. This usually requires simply pushing more victims at responders until the system can no longer handle the flow. Response exercises, perhaps the most common type, are generally conducted on one of several levels including seminars, workshops, tabletops, games, drills, functional and full-scale. These exercises usually produce concrete information easily reviewable by budget-writers and decision-makers—this is frequently true of mitigation and recovery exercises as well. Additionally, after-action reports, lessons-learned and improvement plans from response exercises are generally clear-cut and relatively easy for other responders to relate to and understand.

Prevention, however, is a more imprecise discipline than response. Certain aspects of prevention, such as target hardening and Crime Prevention Through Environmental Design (CPTED), can produce tangible results, but they are primarily long-term capital investment strategies and do not lend themselves well to the exercise process.

The National Strategy for Homeland Security features prevention prominently although it may be the least understood element of the strategy. Superficially, it is a seemingly simple concept but in relation to homeland security planning, training and exercising, the term is sometimes used ambiguously.

In reviewing lessons learned, agencies focus on what went wrong the last time but spend little effort determining what will go wrong in a future, different event. Prevention is difficult to define or measure. If it works, nothing goes wrong. Moreover, stressing prevention systems can be done by simply overloading the system with information, intelligence, or adversaries to the point that the system is no longer effective. This only

proves, however, that any system can be overloaded. Considering these difficulties, it is therefore not surprising that homeland security drills and exercises have not yet, to any significant extent, focused on prevention-related activities.

At the state and local level, some agencies believe they have been left on their own to craft prevention strategies. This contention is confirmed by a report from the Police Executive Research Forum (PERF), which observed that:

> …on a national level, law enforcement is just beginning to develop comprehensive and detailed strategies for prevention and responding to terrorism and is searching for direction and guidance to inform their development of homeland security plans. PERF says "too many" of these agencies "are unsure of what their part should be" in preventing and responding to terrorism, and local homeland security planning efforts to date consequently have been characterized by a "lack [of] a strong unifying strategy and coordinated approach with other jurisdictions and with agencies at other levels of government." Moreover, PERF said, "even those [agencies] that feel certain of their charges must make significant changes to their structure, policies, procedures, personnel expertise, training and budgets – all with only their own guidelines or standards to ensure success.[1]

Clearly, as prevention is an emerging discipline and not always plainly and uniformly defined, much work remains.

This thesis will briefly explore the questions surrounding why prevention has typically not been incorporated into homeland security exercises. It will also look at various strategies, most notably those concerning traditional crime prevention, intelligence, red teaming, and behavioral analysis, to determine how these prevention-related strategies can be integrated into homeland security exercise design and conduct. Ultimately, this thesis will provide answers to government agencies, primarily at the local and state level, which seek to supplement their traditional response, recovery, and mitigation efforts with the vastly more difficult task of preventing terrorism in the first place.

---

[1] Gwen A. Holden, *Building a Homeland Security Strategy: State and Local Law Enforcement on the Line* (Washington D.C., Branch Office: University of Pennsylvania's Jerry Lee Center of Criminology, 2003), 2.

According to the National Strategy for Homeland Security, prevention is the nation's first homeland security strategic objective.[2] However while most layers of government are trained, practiced, and experienced, to varying degrees, in response and recovery, those same layers are not particularly well trained, practiced or experienced in prevention. Recently, with the TOPOFF (Top Officials) series of national homeland security exercises, and an exercise conducted in 2005 by the Department of Homeland Security and the Upstate New York Regional Intelligence Center, prevention has played a more important, albeit still minor, role than in the past. Fortunately, as the importance of prevention is increasingly acknowledged and accepted, and additional research is completed, we begin to get better at learning about prevention. While exercises can help plan, train and assess response and recovery readiness, they can also be used to plan, train, and assess prevention readiness. This thesis will attempt to provide guidance on improving prevention readiness by exploring various ways to incorporate prevention strategies into homeland security exercises.

To implement a prevention exercise program, individually, or as part of larger, more comprehensive, exercises, state and local jurisdictions need a roadmap that explains the benefits, provides clear direction on how to begin the process, and if possible, provides financial and technical assistance to agencies that require it. This thesis, by detailing specific tools, will attempt to provide some of the guidance necessary to accomplish this task.

Currently, the most widely used and funded exercise methodology for validating and enhancing homeland security capabilities at the local, state, and national levels is the Homeland Security Exercise and Evaluation Program (HSEEP). Recently, DHS released a working draft of HSEEP V, Terrorism Prevention and Deterrence. HSEEP V is modeled after and designed to be consistent with HSEEP Guides I-IV and is intended to be a living document that will evolve along with the emerging disciplines of exercising and prevention.

---

[2] Office of Homeland Security, *National Strategy for Homeland Security* (Washington, D.C.: GAO, 2002), 2.

There are many benefits to exercises. Exercises can improve performance, identify areas in need of improvement, and improve intelligence gathering and sharing capabilities. Most importantly, however, on-going, realistic prevention-oriented exercises may result in actual improvements in society's ability to prevent terrorism.

B. LITERATURE REVIEW

A review of available literature finds that general information on exercises is widely available as is information on the importance of including prevention in plans and strategies. The most prominent of these is the National Strategy for Homeland Strategy, which lists prevention as the first strategic objective of various national strategies. This review also finds that little research has been done on prevention models that can be incorporated into homeland security exercises. *The Homeland Security Exercise and Evaluation Program (HSEEP) Guides I-IV* mentions the importance of including prevention in homeland security exercises many times. For example, HSEEP I suggests that prevention exercises focus on issues pertaining to the following:[3]

1. Information and intelligence sharing
2. Credible threats
3. Surveillance
4. Opposing/adversary force or "red team" activity

Unfortunately, *HSEEP Guides I-IV* provide little specific direction on what these methods and tactics should look like in homeland security exercises, and instead leave much of that detail for readers to determine for themselves. As it is an exercise program, HSEEP generally does not offer tactical-level operational guidance.

This lack of specific guidance is not uncommon. The Office for Domestic Preparedness (ODP) published its *Guidelines for Homeland Security–Prevention and Deterrence* in 2003. Though the document cites exercises twenty seven times, most of the references focus only on the need to include prevention in exercises and not on how this should be accomplished. The *Guidelines for Prevention and Deterrence*, however, was not written to as a 'how-to' guide.

[3] U.S. Department of Homeland Security, *Homeland Security Exercise and Evaluation Guide, ed., Volume I: Overview and Doctrine* (Washington, D.C., 2004), 14.

The U.S. Government Accounting Office (GAO) has issued several reports, which analyze federal level counterterrorist exercises and detail how improvements can be made, including the publications *Combating Terrorism: An Analysis of Federal Counterterrorist Exercises* and *Combating Terrorism: Issues to Be Resolved to Improve Counterterrorist Operations*. These works focus primarily on statistics but also provides some limited guidance on information sharing and cooperation among agencies. Examples of prevention can be found in research conducted by Bach.[4] This work focuses solely on border security; however, his discussion of deterrence strategies such as the Cargo Security Initiative may be instructive. As mentioned previously, the *Department of Homeland Security HSEEP Guidelines* provide specifics on the implementation of an effective exercise program and more limited general direction on the incorporation of prevention into actual exercises. Recently, DHS published the *HSEEP V: Prevention and Deterrence Exercises*, which provide significantly more substantial direction for agencies to follow.

There is recent research and guidance, albeit sometimes peripheral to the author's primary topic, on the overall prevention of terrorism. Longshore, for instance, has written that we must recognize that the prevention of terrorism will not always be a direct result of prevention efforts, but may also be related to other tactics that are more broadly directed at the suppression of crime and other factors.[5] His research, along with that of Docobo, suggests that traditional crime prevention efforts can be applied to homeland security efforts.[6]

Work by Dailey has produced a specific counter-terrorism plan, with accompanying training, for police patrol officers.[7] This is important because if a plan can

---

[4] Robert Bach, "Transforming Border Security: Prevention First," *Homeland Security Affairs* 1, no. 1 (Summer 2005).

[5] David N.M. Longshore, "The Principles of Prevention and the Development of the Prevention Triangle Model for the Evaluation of Terrorism Prevention" (Master's Thesis, Naval Postgraduate School, Monterey, CA, 2005), 38.

[6] Jose M. Docobo, "Community Policing as the Primary Prevention Strategy for Homeland Security at the Local Law Enforcement Level" (Master's Thesis, Naval Postgraduate School, Monterey, CA, 2005), 34.

[7] Thomas J. Dailey, "Implementation of Office for Domestic Preparedness Guidelines for Homeland Security June 2003 Prevention and Deterrence" (Master's Thesis, Naval Postgraduate School, Monterey, CA), 2005.

be trained it can be exercised. Typically, training and exercising contain elements of both learning and practice; however, as used here, training is primarily the act of learning, while exercising is primarily the act of practicing. When you practice, you prepare. One area where both training and exercising have proven more difficult is in the area of intelligence gathering and analysis.

The intelligence function has a significant role in homeland security prevention but there appears to be a tendency to only superficially integrate this discipline into homeland security exercises. This may be understandable because, like prevention, intelligence is difficult. Only recently, during TOPOFF 3 and the prevention exercise held by the Update New York Regional Intelligence Center (UNYRIC) has intelligence begun to play a larger role of terrorism prevention. Pointing the way towards more effective use of intelligence in homeland security exercises will require a review of the progression of the role of intelligence in exercises. Additional literature on the subject includes the aforementioned U.S. Government Accounting Office reports on Federal Counterterrorism Exercises and the U.S. Homeland Security Exercise and Evaluation Program Guidelines.

A final area of research is in the use of red teaming to support prevention in homeland security exercises. Red teaming has long been used in the military. As it applies to homeland security, it involves thinking or acting like a terrorist in an effort to identify security weaknesses and potential targets. Red teaming can be accomplished through field-based physical operations or on an analytical level through discussions. This thesis will address only how best it can be used as a prevention tool in homeland security exercises. Available literature on red teaming is limited. The Department of Homeland Security is writing a red team manual and the U.S. Army is developing a multi-week red teaming course curriculum. Additionally, after-action reports from exercises possessing prevention components are extremely helpful.

The difficulty with pure research is in determining, from this basis alone, whether the nation will be safer because of the implementation of prevention strategies into homeland security exercises. The answer to that question, while intuitively positive, is also, ultimately, unknowable. Like prevention itself, measuring the success of prevention

efforts is difficult. Prevention is a negative quantity. Furthermore, a reduction is some static measure of success, for example, the number of terrorist incidents, may simply mean that terrorists, independently, have decided to focus on fewer, but larger and more damaging attacks. This type of asymmetric change in tactics could hardly be counted as a success. These difficulties are a significant reason for the increasing use of capabilities-based planning. Capabilities can, for the most part, be measured.

C. METHODOLOGY

A full examination of prevention-oriented homeland security exercises will require an understanding of homeland security exercise history, design, and development.

Research for this thesis focuses on the logic, strategy, and success of homeland security exercises, particularly those with after-action analysis and comments. It attempts to identify existing practices that can be incorporated into exercises and used as tools to further prevention efforts. The tools researched and evaluated include 'all-crimes' strategies, information-sharing, red-teaming, attack trees, behavioral analysis, and the incorporation of private sector security into training and exercise programs.

This thesis will establish various best practices for prevention activities from corollary models found in prior and planned future exercises, particularly as they may apply to local and state agencies. Review by subject-matter experts will ensure information is analyzed correctly and recommendations are both sound and realistic. Ultimately, this research is intended to assist in the development of guidelines on how to design, develop, and conduct prevention-oriented homeland security exercises.

D. HISTORICAL CONTEXT

There has been no shortage of emphasizing the prevention of terrorism as the highest priority of the United States in the so-called 'global war on terrorism'. Shortly after the attacks of 9/11, President Bush created the Office of Homeland Security and appointed then Governor Tom Ridge as the Director. The first action of this new office was to draft and publish the National Strategy for Homeland Security. That strategy designated prevention as the nation's first priority. Since then, several legislative and executive actions have further driven this priority. Examples include the U.S. Patriot Act, Executive Orders 13356 and 13388, the Intelligence Reform Act of 2004 and others. To

further support prevention, there have also been various policy initiatives such as the Homeland Security Grant Program, the Law Enforcement Terrorism Prevention Program, and the DOJ and DHS led effort to create Fusion Center Guidelines through the Global Justice Information Sharing Initiative.

All of these initiatives recognize the importance of the prevention mission, but also the difficulty in actually doing it. In June 2003, the Office for Domestic Preparedness published the Guidelines for Prevention and Deterrence, which provides some context on how to view this mission area.[8] The guidelines were not written as a 'how to,' but rather to provide aspects to consider when enhancing prevention capabilities. Though the Prevention and Deterrence Guidelines publication helps to frame what the prevention mission might look like, it does not offer guidance on how prevention can be exercised. Even with the guidelines, increased prevention abilities will not come without some operational, technical, and perhaps cultural changes in many organizations at all levels of government, and these skills and abilities will not be realized without training, exercising, and structure.

Currently the most widely utilized and funded exercise methodology for validating and enhancing homeland security capabilities at the local, state, and national levels, is the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP was created in 2003 by examining and integrating parts of numerous legacy exercise programs that supported events such as natural disasters, radiological/nuclear incidents, chemical facility breeches, and even WMD terrorism. Some of these programs included FEMA's Radiological Emergency Preparedness (REP) and Comprehensive Exercise Programs, the U.S. Army's Chemical Stockpile Emergency Preparedness Program (CSEPP), and the Nunn-Lugar-Domenici Act's Domestic Preparedness Program (DPP). Although fundamental similarities existed in each of these programs' exercise methodologies, each was created, implemented, and managed by separate government program offices and their individual contract support teams, not to mention that each was

[8] U.S. Department of Homeland Security, *Guidelines for Homeland Security, Prevention and Deterrence* (Washington, D.C., 2003).

driven by unique federal grants and, in some cases, statutory requirements. Finally, virtually none of these exercise programs placed prevention as its highest priority or, in most cases, even in their list of requirements.[9]

The Nunn-Lugar-Domenici Act (NLD-DPP) was a first of its kind effort by the Federal Government to provide direct preparedness support to state and local governments focused exclusively on the threat of terrorism. The DPP was funded and administered through the NLD Act, first under the Department of Defense, then Department of Justice, and finally the Department of Homeland Security. The Act provided for three exercises in each of the 120 most populated cities in the U.S., according the 1990 census. The exercises consisted of a chemical weapons tabletop, biological weapons tabletop, and a chemical weapons full-scale, each focused exclusively on response operations.

The most valuable effort undertaken to date describing the prevention mission has been by way of presidential directive. *Homeland Security Presidential Directive 8 (HSPD-8),* which tasked the Secretary of DHS to, among other things, develop a National Preparedness System. In response to this directive, a comprehensive effort was undertaken to describe, the homeland security mission in detail. Two products were designed to accomplish this task. The *Target Capabilities List (TCL)* and the *Universal Task List (UTL).* The TCL consists of 37 capabilities and includes descriptions of what is required to sustain the four primary areas (prevention, protection, response, and recovery) that comprise the homeland security mission. Theoretically, if a state or local government can show that it has the ability to fully and effectively sustain these 37 capabilities, then it could argue that it is 'mission-ready', to the maximum extent possible, in regards to homeland security. Along with the TCL is the *Universal Task List (UTL).* Using the previous example, if an organization can show that it has the ability to effectively maintain the 37 target capabilities, that means then that it should be able to perform all of

[9] Significant portions of this section are based on interviews, discussions and correspondence the author had during the period January-August 2006 with Brady K. O'Hanlon, formerly the Program Manager of the DHS Terrorism Prevention Exercise Program (TPEP).

the tasks illustrated in the UTL. This, of course, is only an ideal and no single agency is expected to perform to this level. Five of the 'target capabilities' that specifically relate to prevention are the following:[10]

- Information Gathering & Recognition of Indicators and Warnings;
- Intelligence Analysis & Production;
- Intelligence / Information Sharing & Dissemination;
- CBRNE Detection; and
- Law Enforcement Investigation & Operations

These five capabilities comprise, for all practical purposes, the generally accepted description of what the mission of prevention is today. The products created in response to HSPD-8 hope to offer to the homeland security community, a clear, common, operating picture that describes what prevention should *look like*. From these definitions and tools, the U.S. National Exercise Program (NEP) has drafted HSEEP V–Prevention and Deterrence Exercises. HSEEP V is intended to guide jurisdictions on how to exercise the target capabilities they have worked to attain.[11]

[10] U.S. Department of Homeland Security, "Target Capabilities List-Draft Version Two" (Washington, D.C., 2005).

[11] U.S. Department of Homeland Security, *Homeland Security Exercise and Evaluation Guidelines.*

II. STRATEGIES AND TOOLS

A. ALL-CRIMES

1. Introduction

Crime prevention is one of the most important tasks of law enforcement, and while the prevention of crime is more difficult to accomplish than response, it is of infinitely more value. Of course, the rapid enforcement of crime might also serve as a form of deterrence and therefore prevention. For instance, a suicide terrorist is usually the last link in a long organization chain that involves numerous actors. Once the decision to launch a suicide attack has been made, its implementation requires at least six separate operations: target selection, intelligence gathering, recruitment, physical and 'spiritual' training, preparation of explosives, and transportation of the suicide bombers to the target area. Each of these steps presents itself as a target for prevention efforts.

Law enforcement organizations may take different approaches to terrorism prevention. On one hand, departments may view terrorism in isolation, as a rare occurrence or remote possibility. Based on this view, a department would organize a unique counterterrorism unit, intelligence unit or simply provide staffing to a local Joint Terrorism Task Force (JTTF) and assume that all that can be done is being done. However this narrow perspective would not allow for all of the existing knowledge, skills and abilities of the agency, obtained from decades of experience in fighting traditional crime, to be used in the fight against terrorism. Law enforcement can and should employ tactics that have been effective in fighting crime.

While acknowledging that police departments may take differing approaches to the incorporation of homeland security duties into law enforcement priorities, a preponderance of states and experts believe that a nexus exists between traditional crimes and terrorism.[12] Focus solely and specifically on terrorism can lead to missing clues about terrorism and terrorists that might otherwise be found in cases involving traditional crime.

[12] Council of State Governments, *The Impact of Terrorism on State Law Enforcement* (Washington, D.C., 2005), 19.

A better approach would be modeled after the 'all-hazards' approach common among emergency planners. A report from the Police Executive Research Forum (PERF) states that many in local law enforcement recommend an 'all-crimes' approach to intelligence and information sharing for terrorism and other crimes.[13] There is a further extension of this philosophy that could be described as 'cross-crimes.' Focusing on all crimes indicates that a law enforcement agency will look at any criminal matter as potentially terrorism-related. This would be a tall order for any organization. A more logical and common sense approach would be to focus on those crimes that are more frequently interrelated with terrorism.

The motives of terrorists and other criminals are rarely aligned, however, similarities can be found in the behaviors and methods of terrorists and organized criminals. For example, terrorists operating in cells may not always receive organized or centralized financing and therefore must generate their own. They must acquire funds without attracting the attention of law enforcement. Like traditional white-collar criminals, terrorists also rely on fraud in many of its forms to support themselves and their networks.

Still, traditional criminal organizations are not similar to terrorist organizations in every way. Typically, terrorists are not significantly involved in street level crime. Unlike most street crime, terrorism usually requires careful planning over long periods and involves other actors. Indicators of terrorism such as explosives and extremist literature may not typically be found on non-terrorist criminals. Finally, terrorist activities do not always generate reasonable suspicion and terrorists themselves have typically strived to blend in and to remain relatively anonymous.

2. Crime vs. War

At the macro level, there is an on-going debate regarding the very nature of terrorism. The two schools of thought view terrorism as either criminal in nature or as acts of war. These extremes, however, assume there is no middle ground. Is it not possible that terrorism can involve both war fighting and crime fighting? To be effective,

[13] Police Executive Research Forum, *Protecting Your Community from Terrorism: Strategies for Local Law Enforcement, vol. 5, Partnerships to Promote Homeland Security* (Washington, D.C., 2002), 80.

indeed, to be of any use at all, law enforcement must regard the fight against terrorism as a matter of crime fighting. While many have previous military experience, generally, police officers are not institutionally trained or experienced in war fighting. Conversely, particularly in countries outside of the United States, the skills and resources of the military must see the battle against terror as one that requires war-fighting capabilities. If the national-level struggle is a war, then the state and local level struggle can be criminal. This way, the most appropriate resources address the problem.

Most of the successful efforts in the United Kingdom have been crime-fighting efforts. This is the same as in much of the European Union, which generally focuses on four components: suppressing terrorist financing, legislatively defining terrorism as a crime, strengthening immigration policies, and intelligence collection. In his book *Strategies for Countering Terrorism: Lessons from the Israeli Experience,* Tucker points out that "most countries view terrorism as a crime and believe that retribution for terrorist acts should be pursued through the legal process." Israel may be the only open and democratic society truly fighting terrorism like a war with targeted killings and other military tactics.[14]

Chairman of the Joint Chiefs of Staff General Richard Myers stated in 2004 that, "if you call [terrorism] a war, then you think of people in uniform as being the solution…terrorism is a peacetime problem, which must be about using peacetime remedies." Both he and Secretary of Defense Donald Rumsfeld have expressed a preference for the term 'global struggle against violent extremism' over 'global war on terror.' Even President Bush has referred to the attacks on the World Trade Center in 2001 as both criminal acts and acts of war.

[14] Jonathan B. Tucker, "Strategies for Countering Terrorism: Lessons from the Israeli Experiment," *Journal of Homeland Security* (March 2003), 3.

3. Organized Crime

One avenue for criminal investigators would be to look at organized criminals for links to terrorists. In a recent study, researchers asserted that it is "…well known that terrorists have affiliations with organized crime."[15] If so, then investigations should strive to expose those links.

The same report identifies similarities between the tactics of terrorist organizations and those of traditional organized crime. Both groups commit fraud and theft. Both also are known to traffic in drugs and human beings, and commit extortion and bribery. Terrorists have created shell companies, used chartable organizations, sold counterfeit goods, evaded taxes, and committed immigration and insurance fraud and forgery to generate or hide funds. Finally, both groups also may be involved in legitimate business to aid and conceal their actual motives.

It is not unheard of for ties between criminals and terrorists to be close and collaborative. This situation is more common in developing nations than elsewhere. In more developed countries, terror-crime relationships are more likely to be based on short-term needs and not involve long-term interaction.

Another area that warrants close attention is drug trafficking. Though links between drug traffickers and terrorist organizations are undoubtedly closer in other regions including parts of South America and Asia, a recent FBI bulletin reported that "Drug trafficking represents a significant and possibly growing source of revenue for terror groups…cells may employ drug trafficking to raise funds at a local level. Law enforcement can exploit this possible dependence on drug trafficking by international terrorist cells to detect and disrupt terrorist operations."[16] Considering the size and scope of the illegal drug market in the United States, this would seem a fruitful area for law enforcement attention.

---

[15] Louise Picarelli, John Shelley, Allison Irby, et al., "Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism" (Washington, D.C., U.S. Department of Justice, 2005), 9.

[16] Federal Bureau of Investigation: Counterterrorism Division, "Intelligence Bulletin: Drug Trafficking and International Terrorism," November 16, 2005.

4. White Collar Crime

Perhaps the most obvious and probably the most common nexus between traditional crime and terrorism can be found in the area of white-collar crime. Money is the fuel for most crimes and while the goal of terrorism does not generally involve money, it is used to accomplish larger terrorist goals. The need for secrecy during terrorist planning can require anonymity and the use of deceptions. For example, money may be laundered to hide the source and destination of funds and false identification may be used to enable travel. An FBI brochure called *The Role of Police in Combating International Terrorism*, states, "False documents are the life-blood of the terrorist's covert existence."

An analysis by the National White Collar Crime Center (NWC3) of 100 terror-related federal criminal cases found that every case included charges for some type of white-collar crime falling under one or more of six different fraud categories including document, financial, credit card, immigration, and mail, wire and tax fraud. Table 1 lists the charges filed in the 100 case sample:[17]

Table 1. Charges Filed in Case Sample

White-Collar Crime Category	% of Charges Filed
Identification Document Fraud	54%
Financial Fraud	16%
Immigration Fraud	16%
Credit Card Fraud	10%
Mail and Wire Fraud	4%
Tax Fraud	1%

5. Examples of Terror-Crime Nexus

It is generally well known that several of the 9/11 terrorists, including Muhammad Atta, had been stopped by local law enforcement for various offenses prior to the attacks. There are, however, also examples that illustrate the nexus between traditional crime and terrorism.

[17] John Kane, April Wall, "Identifying the Links Between White-Collar Crime and Terrorism," (Richmond, VA, *National White-Collar Crime Center*, 2005), 3.

One of these crime prevention examples occurred in 1995 in the Statesville and Charlotte areas of North Carolina. An off-duty sergeant from the local sheriff's office observed three Arabic speaking men purchasing a huge amount of cigarettes at a local discounter and paying for it with large amounts of cash wrapped in rubber bands inside shopping bags. His initial suspicions ultimately led to a multimillion-dollar tobacco smuggling ring. That was the case, however. Further investigation revealed that the suspects were actually Hezbollah operatives funneling cash and specialized equipment back to the Middle East. Estimates are that the group generated over eight million dollars before being caught. The money had been used to purchase night vision goggles, mine detectors, blasting equipment, GPS devices, and other paramilitary equipment. Not coincidentally, the group and its members were also involved in a range of other criminal activity including bribery, credit card fraud, identity theft, tax evasion, and money laundering. Though the group was involved in vast numbers of crimes, most of the activities were deliberately kept at a low level and went undetected by local law enforcement. Describing the group, one FBI agent involved in the case stated, "They're best described as part-time terrorists and full-time criminals."[18]

Another example occurred in Colorado in the 1980's. In 1985, after bombings in Detroit and Seattle, investigators began tracking members of a group known as al Fuqra. During the investigation, an Englewood Colorado police sergeant stopped a suspicious vehicle in which the driver was carrying a homemade weapon. A multi-year investigation ensued. In 1989, a search of a storage locker turned up 30 pounds of explosives, pipe bombs and other IED's, shape charges, handguns, documents related to military training, target lists, guerilla warfare, bombing, sniping and surveillance, and evidence of document fraud including 54 blank birth certificates from two different states. Several documents contained plans for the murder of a person living in a mosque in Arizona. Two weeks after investigators identified and interviewed the subject in Arizona, he was found stabbed to death by an unknown assailant. A knife attack was one of the methods described in the documents found in Colorado.

[18] David E. Kaplan, "Homegrown Terrorists: How a Hezbollah Cell Made Millions in Sleepy Charlotte, N.C.," *U.S. News and World Report*, March 10, 2003.

Interestingly, a private security business, Professional Security International (PSI) was associated with a number of al-Fuqra members and was found to have been used to facilitate money laundering and transfers and provide information for terrorist planning. The company was able to negotiate security contracts with the federal government and international airports. al Fuqra had been using PSI and several other security businesses for these activities. Unfortunately, the State of Colorado had no system for regulating the operation of security companies.[19]

6. Methodology to Identify Terror-Crime Interaction

In the previously mentioned report on the links between organized crime and international terrorism, researchers developed what they describe as a "groundbreaking methodology for analysts and investigators to…identify crime-terror interactions more quickly and to assess their importance with confidence."[20]

Researchers noted that terror-crime interaction is frequently discovered only by accident due to close analysis of specific terror groups and their activities. Discoveries of this type preclude the identification of patterns of crime, but are obtained only after specific terror groups have *already* been identified. Based on this finding, the research team developed a methodology to identify positive indicators of terror-crime interaction and further, to eliminate irrelevant data. They call this method preparation of the investigative environment (PIE). See Figure 1.

[19] Kane and Wall, "Identifying the Links," 29.

[20] Picarelli, Shelley, Irby et al., "Methods and Motives," 4.

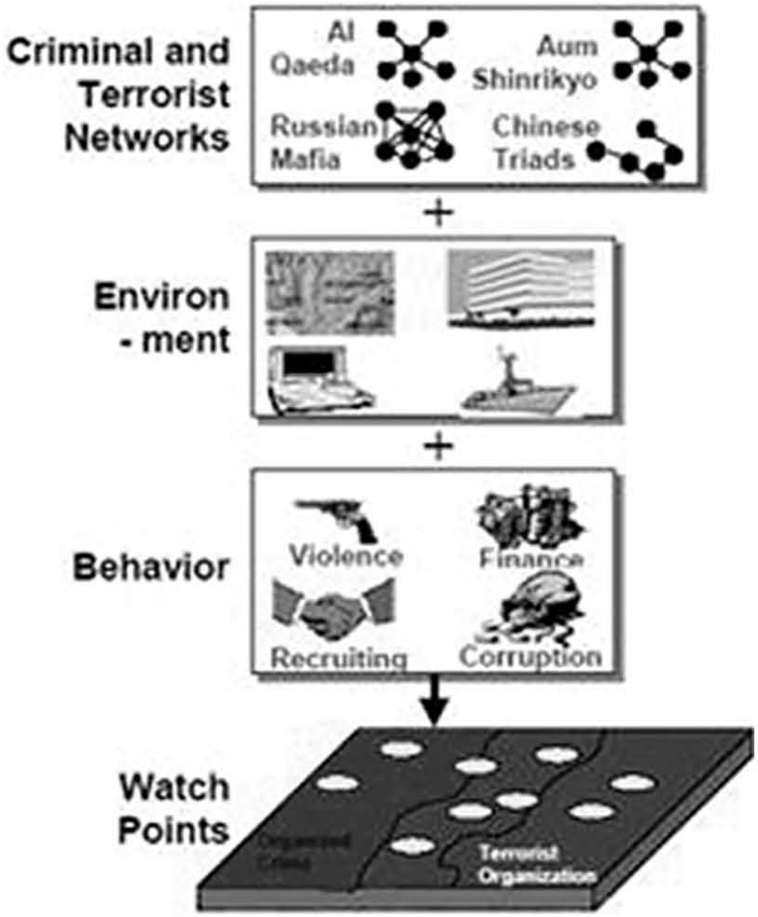

Figure 1. Preparation of the Investigation Environment (PIE)

PIE involves taking existing data and identifying specific examples of terror-crime interaction for the purpose of recognizing and thereby preventing planned terrorist activity. PIE separates data into three analytical components—criminal and terrorist network organization, the environment, and behavior. From these components, researcher selected twelve 'watch points', or indicators, that lead to a level of suspicion that warrants further investigation. The watch points are fully described in Appendix B.

The process begins with identifying areas where associations between traditional crime and criminals and terrorists are most likely to occur. The next step requires analysis of watch points to determine where overlaps are likely to occur. The final step is to collect and analyze information where terrorists and criminals appear to cooperate.

While no known methodology will produce positive results every time, the benefit of any effective system will be to ensure that investigators and analysts are devoting time and resource to areas that objective analysis demonstrates is most likely to lead to valid information and therefore successful intervention and prevention.

7. Conclusion

While an 'all-crimes', or 'cross-crimes', emphasis by law enforcement in dealing with terrorism may be useful, the topical question is whether this approach can be exercised as part of a terrorism prevention scenario. Evidence points to clear and dangerous links between organized crime and terrorists. Furthermore, one axiom among white-collar crime investigators is 'follow the money', and this saying appears to apply equally well to terrorist organizations.

Perhaps the more relevant question is *how* can terror-related crime be exercised. The answer, in part, is that intelligence-oriented exercises can be altered to incorporate a broader range of criminal activity. This can be done at the level of analysis, but prior to that, it can also be done by incorporating indications and warnings of those crimes most frequently linked to terrorist network and cell activities. In addition to intelligence, fusion centers can add crime analysts and exercise their skills and abilities as part of prevention exercises. Finally, using a formal methodology based on empirical data will direct resources to those areas most apt to generate positive results.

Prevention exercises, while not law enforcement exclusive, almost by definition are law enforcement centric. Even if other non-law enforcement collaborators in homeland security efforts accept this viewpoint, it does not lend itself to equal partnerships, and therefore, it may be difficult to obtain as much buy-in from non-law enforcement agencies as may be ideal. Finally, the exercise of prevention is complex and not well understood. This can lead to apprehension on the part of agencies considering the exercise of prevention activities. Having a level of comfort is not an absolute requirement, but a *lack* of comfort should be acknowledged and addressed. Ultimately, providing clear guidelines, useful tools, and technical and financial assistance will help to overcome many of these obstacles, and most of this should come from the federal government.

B. INFORMATION SHARING ENVIRONMENT ANALYSIS

Agencies considering prevention exercises should view intelligence challenges from an 'all-crimes' perspective, which is similar to the 'all-hazards' approach used for most preparedness activities. This approach is becoming more widely accepted with the recognition that terrorism intelligence at the state and local level will likely not be as effective unless analysts have access to traditional criminal information. It is not uncommon for terrorists to be involved in precursor crimes of one kind or another, which could provide analysts additional opportunities to recognize potential threat elements.[21] The Washington [State] Joint Analytical Center (WAJAC) and the recently opened Los Angeles Joint Regional Intelligence Center (JRIC) both recognize the value of the all-crimes approach and have adopted it as part of their core operations.[22]

Exercising state or local capabilities to prevent terrorism is best done in a multi-jurisdictional environment. Terrorists do not recognize borders, therefore, the flow of information and intelligence should not either. Rarely would terrorist planning, surveillance, movement, or other activities all occur in one sector or discipline of our response or civilian communities. In addition, prevention exercises involving the intelligence function of just a single agency would be more similar to training than exercising.

1. Problems with the Current Approach

The field of intelligence is vast, complicated, and after decades of relative secrecy, increasingly well documented. Much of this documentation relates to the many and varied problems in the federal intelligence community; intelligence roles and responsibilities that sometimes conflict; a lack of trust between organizations tasked with sharing information; users having difficulty accessing the information they need; and,

---

[21] One example is the cigarette smuggling case in North Carolina, which involved Hezbollah operatives. More can be found in the following article. Sari Horwitz, "Cigarette Smuggling Linked to Terrorism," *Washington Post*, June 8, 2004, sec. Metro-Crime. A01.

[22] Patrick McGreevy, "L.A.'s Counter-Terrorism Team May Get Permanent Status," *Los Angeles Times*, February 3, 2006.

technological systems that are frequently incompatible.[23] These operational and relational issues are in addition to the need to ensure that legal rulings, polices, and guidelines are followed and in sync with prevention oriented plans and operations.

The problems may be no better at the state and local levels. Law enforcement gets little guidance on what it should be looking for and only the largest police departments devote resources to a potent intelligence and analysis capability[24]

The current information-sharing environment is both overly complex and lacks robustness.[25] In addition, the federal government has not yet defined a clear information-sharing environment path. In their recent report on information and intelligence, the Markle foundation describes the federal effort as being "bogged down by gaps in leadership, policy articulation, turf wars, and struggles over competing…technologies. Indeed, our government seems to have lost its sense of the broader mission."[26]

Another report, this from the U.S. House of Representatives, complains "despite numerous strategy pronouncements, memoranda of understanding, Executive Orders, reports, and promised guidelines for how to "do" information sharing, [federal policymakers] have come up short time and time again."[27]

2. Information Sharing Environment

Looked at broadly, through the federal legal definition, the Information-Sharing Environment is a program, under the Director of National Intelligence, initiated in accordance with the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. It is intended to examine and construct the combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of

---

[23] John A. Russack, "Preliminary Report on the Creation of the Information Sharing Environment" www.ise.gov/PreliminaryReport.pdf. Accessed September 13, 2006, 4-7.

[24] K. Jack Riley, Gregory F. Trevorton, Jeremy M. Wilson, Lois M. Davis, *State and Local Intelligence in the War on Terrorism* (Santa Monica, CA: RAND, 2005), 58.

[25] Russack, "Information Sharing," 2.

[26] Zoe Baird and James Barksdale, "Mobilizing Information to Prevent Terrorism" (New York, NY: Markle Foundation, 2006), 1.

[27] U.S. House Committee on Homeland Security Democratic Staff, "Beyond Connecting the Dots: A VITAL Framework for Sharing Law Enforcement Intelligence Information," 2005, 4.

Federal, State, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration among users to combat terrorism more effectively."[28]

The Information Sharing Environment is also a vision for the revision and implementation of improved polices, cultures or technologies. While initially focused on terrorism, the environment can include all-crimes, and includes information from sources in intelligence, law enforcement, the military, homeland security, and potentially others.[29]

The federal Information Sharing Environment is a legal construct, but it also exists at the local and state levels, even if it is not always referred to as such. For the this thesis, the definition of the information sharing environment is the state and local system by which information and intelligence is collected, exchanged, analyzed and acted upon—frequently using a fusion center at its core. For a successful prevention exercise, this environment must be fully understood.

One strategic role of the federal government is to help guide the process of intelligence development from seeking and sharing information and intelligence to building knowledge. See Figure 1. Ideally, an information sharing environment should be "scalable…distributed, decentralized…so that information flows do not depend on a central information broker."[30]

[28] Information Sharing Environment, "Program Manager Information Sharing Environment," http://www.ise.gov/. Accessed August 7, 2006.

[29] Russack, "Information Sharing," 7.

[30] Baird and Barksdale, "Mobilizing Information," 21.

Figure 2. Advanced Collaboration Cycle[31]

3. Intelligence-Oriented Exercises are Law Enforcement Centric

Intelligence is not the sole purview of law enforcement. State and local enforcement may, however, be "uniquely positioned to augment federal intelligence capabilities by virtue of their presence in nearly every American community, their knowledge of local individuals and groups, and their use of intelligence to combat crime."[32] Intelligence collection for traditional crime prevention and investigation, however, is not the same as that needed for terrorism prevention and investigation. Traditional criminal intelligence tends to be tactically oriented. Counterterrorism intelligence requires significantly more analysis."[33] In addition, traditional criminal investigations usually follow a single path from the crime backwards to the suspect(s). Prevention oriented counterterrorism investigations must look forward at many paths—a much more difficult process of predictive analysis.[34]

[31] LTG Peter A. Kind (Ret.) and J. Katherine Burton, *Information Sharing and Collaboration Business Plan* (Alexandria, VA: Institute for Defense Analysis, 2005), 8.

[32] Riley, et al., "State and Local Intelligence," ix.

[33] Ibid., 38.

[34] Ibid., xv.

This fact, along with the reality that separate intelligence and investigation capabilities are not always the most effective path to prevention is leading to changes in the structure of the intelligence community. For example, the Federal Bureau of Investigation (FBI), through the establishment of Field Intelligence Groups, is working to combine its intelligence and investigative capabilities.[35] Some would argue that, similar to the structures found at the local and state levels, there should be a combining of the many federal enforcement and investigative agencies under one (or at least fewer) umbrellas. While this could be one route to better cooperation among stakeholders, it is not the current reality.

The primary investigative and intelligence agency assigned to the terrorism prevention mission is the FBI, a law enforcement agency. The FBI has approximately 100 Joint Terrorism Task Forces in operation in the U.S.[36] These task forces are intended to facilitate cooperation in the prevention of terrorism.[37] As stated earlier, one problem with the intelligence community and its processes is that they are overly complex. As an example, the FBI alone distributes information in at least nine ways: Weekly Intelligence Bulletins; the Director's Briefing; Intelligence Information Reports; Intelligence Assessments; the Secure Video Teleconference System; Urgent Reports; Quarterly Terrorist Threat Assessments; email messages; and Terrorist Watch List.[38]

Regardless, the purpose of briefly examining the current system is to demonstrate that terrorism prevention is, and will likely remain, not law enforcement exclusive, but law enforcement centric.

---

[35] Suzel Spiller, "The FBI's Field Intelligence Groups and Police: Joining Forces." *FBI Law Enforcement Bulletin* (May 2006): 1.

[36] Riley et al., "State and Local Intelligence," 3.

[37] Ibid., 15.

[38] Ibid., 41.

4. Intelligence Fusion Process

One increasingly recommended path for improving terrorism prevention intelligence is through the creation and maintenance of intelligence fusion. Intelligence fusion is defined as the "overarching process of managing the flow of information and intelligence across levels and sectors of government."[39]

To assist in this process, Fusion Center Guidelines have been jointly developed by the Departments of Justice and Homeland Security. The foundation of the Fusion Center Guidelines is the National Criminal Intelligence Sharing Plan (NCISP) The NCISP is the model or blueprint to follow when building an intelligence function in law enforcement and the Fusion Center Guidelines are intended specifically for the law enforcement intelligence component of fusion centers and fusion centers are designed to fight both traditional crime and terrorism.[40]

The data fusion process is intended to combine uncertain, incomplete data with the goal of improving the value of the information.[41] This ability allows a fusion center to identify terrorism-related leads from crime-related leads and other information sources. In other words, fusion centers focus on all-crimes.[42]

5. Analyzing the Information Sharing Environment in Exercises

The reason prevention exercises require an analysis of the state and local information sharing environment is that prevention exercises can be designed around this environment. It would serve no purpose to exercise the information-sharing environment that agencies wished they had. The exercise must test and validate the actual environment. Of course, prevention exercises can also help determine if future changes are warranted.

The Information Sharing Environment Analysis (ISEA) is a process that serves to "identify the organizations, personnel, activities, programs, networks, and data that

---

[39] U.S. DHS, DOJ, "Fusion Center Guidelines," 2.

[40] Ibid., 2-3.

[41] Ibid., 12.

[42] Ibid., 17.

comprise and support the local antiterrorism mission."[43] The analysis will typically produce an ISEA flow chart (see Figure 3). The flow chart is a graphical depiction of the state and/or (depending on the scale of the exercise) local information-sharing environment. It should include participants in the environment, inputs, outputs, and the flow of information and intelligence though internal and external formal networks. As information can also flow through an almost limitless number of informal networks and channels the analysis should seek to identify the most common ways these may occur within the local information-sharing environment.

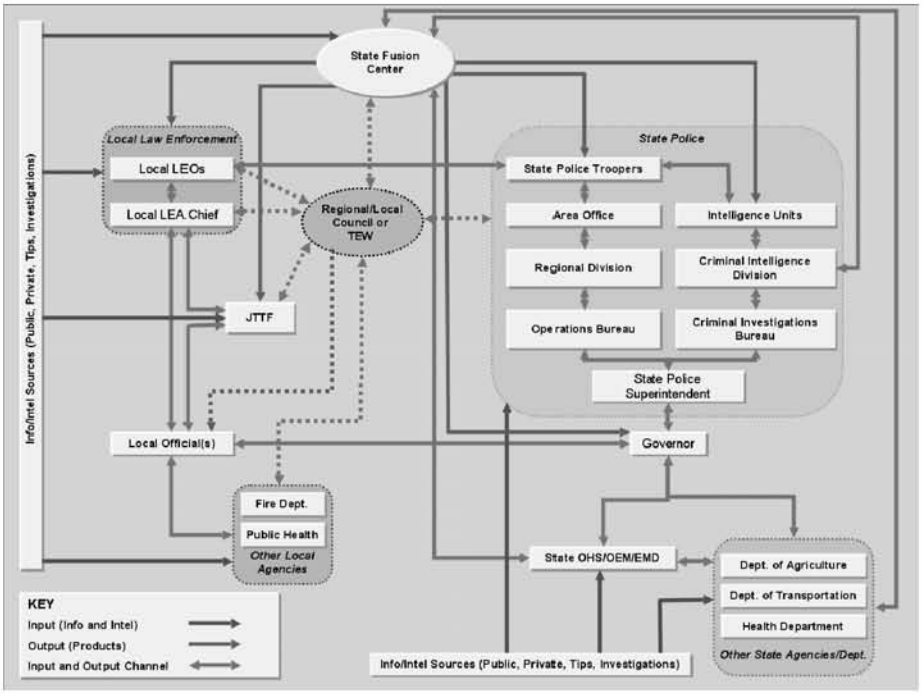

Figure 3. Sample ISEA Flow Chart for a State Exercise

The results of the information sharing environment analysis should be used to tailor exercise objectives, ensure systems are realistically tested, and aid in the development of exercise injects.[44]

One difficulty in exercising intelligence functions, particularly collection and analysis, is that those people responsible for these functions are typically aware they are

[43] U.S. DHS, *Homeland Security Exercise and Evaluation Guidelines*, 2.

[44] Ibid., 3.

participating in an exercise and may be hypersensitive to clues that would not otherwise attract attention. This tendency can invalidate the results of a prevention exercise.

There are ways, at least partially, to mitigate some of these artificialities. One method is to conduct exercises in real-time. This might require that an exercise last for days, weeks, or even months, allowing the intelligence life cycle to play out as it naturally might. This timeframe may be impractical, not to mention expensive and potentially disruptive, for many agencies. Prevention exercises must not always be conducted full-scale but can focus on smaller, specific components of a system, which can allow them to be scaled to more achievable proportions. Another method to mitigate the problem of exercise-related anticipation and awareness is the use of white noise. Intelligence exercises typically employ the use of white noise, or erroneous information, unrelated to the threat, to force analysts to prioritize information and make connections found within large amounts of data and information. Finally, intelligence exercises can be conducted without notice. That is, intelligence collectors, investigators, and analysts do not have to be aware that an exercise is being conducted. Of course, the larger the exercise, the more difficult it is to conceal its existence and this may only work in smaller exercise scenarios.

6. Conclusion

Historically, the American public has viewed intelligence as a feature of foreign security and not something required within the continental United States.[45] For prevention at the local and state level, effective intelligence is the most critical component. Abuses of the past need not be forgotten but lessons learned incorporated into intelligence policies and procedures to ensure that public trust is maintained. Moreover, we cannot ignore that many past intelligence failures have resulted from over reliance on technology. The "human dimension is critically important for information sharing."[46] Personalities and relationships can frequently bridge gaps communication links. There may be truth to the saying it is better to have a friend than a plan.

---

[45] Todd Masse, "Domestic Intelligence in the United Kingdom: applicability of the MI-5 Model to the United States" (Washington, D.C., Congressional Research Service, May 2003), 9.

[46] Baird and Barksdale, "Mobilizing Information," 51.

C. RED TEAMING

Unlike many traditional crimes, terrorism, by definition, is indiscriminate, and therefore, very nearly, unpredictable. Nevertheless, there are ways to anticipate reasonably likely attack scenarios and therefore train and exercise strategies to prevent them. One of the most effective, yet little used, strategies is red teaming.

The deployment of a trained adversary provides an essential move-countermove element not available in response exercises. As it applies to homeland security, it involves thinking or acting like a terrorist in an effort, for example, to identify security weaknesses and potential targets. Red teaming can be accomplished through field-based physical operations or on an analytical level through discussions. Adversaries, as portrayed by red teams, should accurately represent whatever the most probable threat facing the jurisdiction. If it is not an accurate reflection, and the jurisdiction measures its capabilities against it, the jurisdiction stands the chance of developing a false sense of security, or worse yet, inappropriate counter-measures.

The Department of Homeland Security has developed a program called the Universal Adversary (UA), to assist with this requirement. The UA essentially collects real-world threat group information and sanitizes it into usable materials in unclassified exercises for all levels of government. The UA also has the capability to manifest itself into the physical deployment of any of its threat group by way of a Red Team.

Unfortunately, while red teaming can be a tool of significant value, it also carries with it the greatest amount of risk. For this reason, only trained, experienced, and disciplined professionals should be used as red team adversaries. This will help avoid both inaccurate portrayal of an adversary, and, more importantly, the potential for personal injury to exercise participants.

The *National Strategy for Homeland Security* states that "employing 'red team' techniques" is a major initiative within the intelligence and warning mission area…[47] The Congressional Research Service, in its report, *Border and Transportation Security: Possible New Directions and Policy Options*, also recommends the expanded use of red teams.[48]

1. Definitions

Red teaming is a relatively new term that describes a variety of exercise activities. The most basic level of red teaming, if it can be called that, is to conduct peer review of plans and policies to detect vulnerabilities or perhaps to simply offer alternative views of scenarios.

There are a number of definitions of red teaming, each differing primarily in scope but otherwise similar in content. One definition is that red teaming is an iterative, interactive process conducted during crisis action planning to assess planning decisions, assumptions, processes, and products from the perspective of friendly, enemy, and outside organizations.[49] Red teaming has also been described as the "capability-based analytical or physical manifestation of an adversary, which serves as an opposing force…"[50]

Red teaming can be a form of risk assessment and mitigation, with the key difference that red teaming involves the presence of an adversarial condition. Red teaming is not intended to be used as an oversight function. For the purpose of this Chapter, red teaming refers to having the role of an active, thinking, and importantly, adaptive, opponent in an exercise. Adaptive opponents allow exercise participants to engage in both prevention and protection-related activities simultaneously.

As indicated by the name, red teaming involves the use of teams, the most important of which is the red team itself. According to the Homeland Security Exercise

---

[47] Office of Homeland Security, *National Strategy,* viii.

[48] Congressional Research Service, "Border and Transportation Security: Possible New Directions and Policy Options" (Washington, D.C.: March 2005), 19.

[49] Col Timothy G. Malone and Maj Reagan E. Schaupp, "The 'Red Team': Forging a Well-Conceived Contingency Plan," *Aerospace Power Journal* XVI, no. 2 (Summer 2002).

[50] DHS, *Homeland Security Exercise and Evaluation Program.*

and Evaluation Program, a red team is a "group of subject matter experts with various appropriate disciplinary backgrounds, that provide an independent peer review of plans and processes, acts as a devil's advocate, and knowledgably role-plays the enemy using a controlled, realistic, interactive, process during operations planning, training, and exercising."[51]

Table 2. Typology of Activities with Embedded Red Team Approaches

	ACTIVE	PASSIVE
STRUCTURED	Force Protection Vulnerability Assessment Computer Security Penetration Testing Physical Penetration Testing of Facilities Readiness Exercises Military Wargaming	Tabletop Exercises Models & Simulations Military Decision-Making Process Adversary Analyses
UNSTRUCTURED	Naval Special Warfare Development Group Opposition Forces	Analysis of Competing Hypotheses Red Cell Activities

Red teaming has long been used in the military. The Defense Science Board states that there are three types of counterforce training. Surrogate adversaries and competitors intended to sharpen blue team skills, expose vulnerabilities, increase understanding of options and response plans; devil's advocates who provide critical analysis to critique plans and strategies, etc; and independent sources of judgment such as general advisory boards.[52] Red teams evaluate a target or tactic, but not the likelihood that a particular target will be attacked. Red team members are strategists who identify what to attack and

[51] DHS, *Homeland Security Exercise and Evaluation Program.*

[52] U.S. Department of Defense, Defense Science Board, "The Role and Status of DoD Red Teaming Activities" (Washington, D.C., September 2003).

domain experts who identify how. Non-military red teams should not be, however, solely target-focused. Red teams can also be used to engage and cause reaction to allow agencies to deploy systems such as the intelligence life cycle.

Red teaming also involves other participants, each of which can be part of a team. Blue teams represent defenders at all levels. The role of the blue team is to think about how surprise attacks might occur, identify indicators and warnings of those attacks, collect intelligence on those indicators, and adopt defenses against the most likely possibilities or at least provide early warning.[53] Partners and neutral forces represent green team members. White team members frame, execute and evaluate the exercise, facilitate and mentor team members, and otherwise ensure the exercise continues. Using a nomenclature that color codes each team is optional for all participants except the red team itself.

While there are potentially many levels of red teaming, two of the most common are physical red teaming and analytical red teaming. Physical red teaming involves individuals portraying actual, realistic, adversary moves and countermoves in an exercise. A physical red team embodies the selected adversary, acting according to the selected group's motivations, capabilities, and intent. Physical red team operators plan, prepare, and leave signatures. Using a sliding level of realism, they act out and execute the steps dictated by known terrorist tactics, techniques, and procedures, and provide the means for the blue team players to interact with an adversary in an exercise setting.[54]

A second form of red teaming is referred to as analytical red teaming. The benefit of analytical red teaming is that it can be conducted by agencies possessing almost any level of capability, at a lower cost, over a shorter time, and with fewer personnel. Of course, using fewer personnel presents both positive and negative aspects since fewer participants also means that fewer people are trained. Analytic red teaming provides a potential adversary's view of threats, vulnerabilities, and countermeasures. Without testing the physical limitations of antiterrorism measures, analytical red teaming can offer

[53] CRS, "Border and Transportation Security," 19.

[54] DHS, *Homeland Security Exercise and Evaluation Program*, 6.

insight to challenge prevailing views, prevent surprise, allocate resources, and expand the bounds of imagination. Analytical red teaming can occur as part of a discussion-based exercise or as a stand-alone activity.[55]

Red teaming can be conducted on multiple levels and used in different types of exercises. Discussion-based and tabletop exercises, for example, may, in some cases, be preferable to field exercises, primarily due to these types of exercises being much simpler and less expensive to conduct. According to a report from Sandia National Laboratories, however, field red teaming has significant strengths when compared to simple analytic exercises and is "most likely a preferable approach…in some settings." The report states that field-based games lend realism to the process, add real-world complexities and that red team dynamics add a joint sense of ownership to problems.[56] Ultimately, the type of exercises to conduct will be determined by costs, resource availability, knowledge, skills, and abilities of the participants, training culture of the organization, and the intended purpose of the exercises.

2. Background of Red Teaming

The value of any exercise rests on how realistically it is carried out. The Battle of Midway is a good example. On May 1, 1942, six months after Japan attacked Pearl Harbor, the Japanese Combined Fleet HQ conducted a four-day series of war games to test the operations planned for the upcoming Battle of Midway. War gaming and red teaming are functionally similar endeavors. Unfortunately for the Japanese, the war game had serious defects in both its approach and its methodology.

First, game planners and controllers assumed that the Imperial Navy could execute all operations without difficulty. Much of this was due to the arbitrary interference of the Rear Admiral presiding over the game. He would countermand the ruling of game umpires whenever their determination adversely affected the Japanese side.

---

[55] DHS, *Homeland Security Exercise and Evaluation Program*, 14.

[56] Judy Whitley, John Moore, Rick Craft, *Red Gaming in Support of the War on Terrorism: Sandia Red Game Report* (Albuquerque, NM: Sandia National Laboratories, January 2004), 25.

Second, there was a serious lack of familiarity with the plan by the operational commanders responsible for the conduct of the game.

Finally, many of the officers of the operational force were dissatisfied with many aspects of the plan, in particular the underestimation of the enemy capabilities. They did not voice their reservations, however. The problems that were identified and the underlying (and flawed) assumptions were never challenged.[57]

Though other factors, including poor luck by the Japanese and superior signals intelligence by the Americans, contributed to heavy losses by Japan (four aircraft carriers, three thousand sailors and strategic advantage in the Pacific), poor planning, training and exercising did nothing to improve their chance of success.

Later in the war, the allies more effectively used exercising when they successfully war-gamed the deception plan for the invasion of Europe to ensure they could counter German attempts to discover the deception.[58]

More recently, the Nuclear Regulatory Commission conducted 81 red team exercises at nuclear power plants from 1991-2001. In 37 of those exercises, teams were successful in 'attacking' their target. This exposed serious security weaknesses and led to improvements.

Currently, Sandia National Laboratories is doing extensive red teaming research, much of which is related to cyber threats, as red teaming is relatively common in the area of cyber-security.

The U.S. Department of Defense views red teaming as a "valuable, but underutilized" exercise strategy.[59] Red teaming conducted by the U.S. Army in 1996, though, was less than successful. Opinions varied on their value as many of the exercises were apparently scripted only to validate existing operational concepts. The army has

[57] Defense Science Board, "Role and Status of DoD Red Teaming Activities," 35.

[58] Colonel Gregory Fontenot, U.S. Army, Retired, "Seeing Red: Creating a Red-Team Capability for the Blue Force," *Military Review* (September-October 2005): 6.

[59] Defense Science Board, "Role and Status of DoD Red Teaming Activities."

typically used red teams in an ad hoc manner with no established doctrine or methodologies. Additionally, military red teams lack shared tactics, techniques, and procedures.[60]

This may soon change, however, as the U.S. Army, through their University of Foreign Military and Cultural Studies, is developing an education, training, and practical experience curriculum for red teams. The program hopes to publish a red teaming best practices handbook and consists of an eighteen-week course for red team leaders, six week course for red team members, and two week course for mentors and subject matter experts assigned to red teaming operational support.[61]

3. Benefits of Red Teaming

The benefits of red teaming are many. Perhaps most importantly, successful red teaming offers a hedge against surprise and inexperience and a guard against complacency. It tests the fusion of policy, operations, and intelligence. It can be used to imitate attackers, other agencies, even Murphy's Law. Red Teaming can yield a closely synchronized planning staff, drive more complete analysis, and deliver a better plan. Red teams can highlight deviations from doctrine, reveal overlooked opportunities, and determine how well an agency understands its own plans and procedures. It can also improve both contingency and deliberate planning.[62]

As one researcher has determined, red teaming "provides a means to build intellectual constructs that replicate how the enemy thinks [because the constructs] rest on a deep intellectual understanding of his culture, [the] ideological (or religious) framework through which he interprets the world…and his possible and potential strategic and operational moves."[63] This is important because carefully and accurately imitating the enemy (or whatever function is being tested) is what lessens the likelihood an agency will be caught by surprise and left unprepared. This requires that agencies

---

[60] Fontenot, "Seeing Red," 6.

[61] Ibid.

[62] Malone and Schaupp, "Red Team," 11.

[63] Williamson Murray, *Red Teaming: Its Contributions to Past Military Effectiveness* (McClean, VA: Hicks and Associates, September 2002), 58.

practice against threats that are specific to the geographical areas being tested. We can better prioritize prevention and response plans when we better understand the culture and objectives of potential attackers.

Red teaming can increase opportunities by challenging aspects of plans, programs, and assumptions. It allows organizations to model missions, assets, and operating environments and to then assess these systems through the eyes of an enemy. Perhaps most importantly, it can assist organizations to prepare for the unexpected.[64]

In addition, effective red teaming can define a threshold of detection, suspicion, and action. It can and should cause blue team exercise players to recognize suspicious behavior, investigate networked resources, share information, and/or any number of other steps to prevent or deter a particular attack. Specific examples of these behaviors might include attempts to purchase weapons or pre-cursors for weapons and inquiries made to private sector security, law enforcement, or others regarding security measures or infrastructure vulnerabilities. Red teaming, however, should not include potentially dangerous activities such as driving erratically, physical threats, or foot and vehicle chases.[65]

Finally, Fontenot argues that red teaming can reduce risk, perturb a stagnant organization, avoid predictability, overcome bias, and improve flexibility and response. At the macro level, red teaming expands problem definitions, challenges assumptions, and provides an independent view of vulnerabilities; it also provides a better understanding of potential enemies, can identify the secondary and tertiary effects of plans, and can reveal opportunities and provide alternative courses of action.[66]

4. Impediments to Effective Red Teaming

Unfortunately, in addition to the benefits, there are also numerous possible impediments to conducting effective and helpful red teaming. Culpepper classifies impediments into situational and organizational. Situational impediments include the

---

[64] DoD Defense Science Board, "Role and Status of DoD Red Teaming Activities," 14.

[65] DHS, *Homeland Security Exercise and Evaluation Program*, 51.

[66] Fontenot, "Seeing Red," 5.

chosen scenarios, the selection and training of members and the conditions. Organizational impediments depend on the organization and include red team interactions with the blue team, organizationally imposed constraints and the interpretation, distribution and reception of the resultant lessons learned.[67]

The Defense Science Board has compiled an even more detailed and thorough inventory of what makes for successful, and unsuccessful, red teaming. Among the more common reasons for failure include red teams not given enough latitude, not approaching the task with gravitas or conversely, not being taken seriously by the organization, not accurately capturing the culture of potential adversaries, and team members of poor quality or lacking in adequate training. The board identified elements of effective red teaming that address some of the reasons for failure. In addition, they add that red team success requires an organizational culture that values constructive criticism and provides top cover for exercise participants, meaning independence with accountability and accepting and acting upon red team recommendations.[68] Fontenot adds that organizations should value intellectual preparation as seriously as physical preparation.[69] This is perhaps the most important factor in conducting successful red teaming.

Another hindrance is that organizations may not want to share information and thereby limit not only the ability to effectively carry out the exercises but also the usefulness of lessons learned. Furthermore, if red team play is overly scripted, it can limit the training value by taking the realism out of what should be a realistic exercise. Conversely, play that lacks sufficient scripting can lead to unexpected and undesired outcomes, make assessment more difficult, and increase safety risks.

Finally, there have been demonstrated historical difficulties in creating and sustaining red teaming and therefore, based on this experience, it is possible that new red teaming initiatives will not provide expected values.

---

[67] Anna M. Culpepper, "Effectiveness of Using Red Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack" (Master's Thesis, Naval Postgraduate School, Monterey, CA, 2004), 11.

[68] DoD Defense Science Board, "Role and Status of DoD Red Teaming Activities," 6.

[69] Fontenot, "Seeing Red," 6.

5. Methodology for Using Red Teaming in Exercises

There are a number of steps involved in the development of red team exercises. The hosting or lead organization must determine the objectives and/or desired results which may include: liaison with governmental and/or private partners, determine the scale and type of exercise, the type of scenario, the method of evaluation and the documentation plan, develop the scenario, identify and train the appropriate participants, conduct and evaluate the exercise, prepare thorough documentation, evaluate the performance, develop the improvement plan, make required and desired improvements, and finally, exercise again. This basic outline applies to virtually all exercises, not just red teaming, and many of the steps are intuitive. However as it may be more expedient, less costly or simply reduce the potential for embarrassment, some organizations may choose to omit steps in the process. This is not recommended.

Addressing red teaming specifically, Malone, et al. have developed a detailed checklist for red team exercise preparation:

1. Establish Secure Locations Away from Distractions
    a. Privacy, secure network, maps and overlays (generally open-source), and office supplies
2. Gather Necessary Reading Material and Data
    a. Appropriate policies, directives and other orders, general guidance, message traffic (intelligence reports, etc.), relevant briefing documents produced in the planning process, relevant publications, organizational charts, location studies, etc.
3. Prepare to Role-Play the Enemy and Other Adversaries
    a. Review location studies, study enemy doctrine and capabilities, determine enemy's probable actions, study the political environment
4. Understand the Overall Situation and Blue Planning Process
    a. Review assessments, orders, messages, and other products, identify blue team assumptions, etc.[70]

This checklist, however, particularly bullet point 4, "Understand the Overall Situation and Blue Planning Process," may be more appropriate for military red teams.

[70] Malone and Schaupp, "Red Team," 5.

For example, adversaries (whether real world or red team) would not typically have access to governmental or private sector assessments, assumptions, messages, etc. This type of information should only be available to red teams if it would be available to real world adversaries. Also not mentioned by Malone, but supremely important, is the integration of effective and redundant safety measures.

A red team exercise should be an action-reaction-counteraction game prompting move and countermove analysis. Red team operations should affect the actions of the blue team (in other words, be realistic but noticeable), potentially affect other red team actions (e.g., a change of plans), and provide data and information that will stress the system and drive exercise play.[71] Real value can be obtained by using red teams at varying suspicion thresholds. For example, a team can be activated and conduct operations in the least suspicious manner possible, presenting few indicators and warnings on which blue teams can react. If they are not discovered, continue to send them in, each time increasing some level of suspicious behavior until the prevention system engages. This allows the threat detection system to be tested and evaluated more precisely ensuring specific training needs are identified.

To generate new ideas, red team members should be subject matter experts and represent a balance between skilled permanent staff and shorter-term transient members. The key is there should be a variety of opinions and ideas. The risk in not using people fully trained in red team operations or not fully understanding the mind of the adversary is that an agency could end up developing a false sense of security or devising inappropriate countermeasures based on unrealistic threats. The resources available to the organization will be a factor.

[71] U.S. Department of Homeland Security, *Prevention Exercise Training Course: Participant Handbook* (Washington, D.C., March 2006), Module 4.

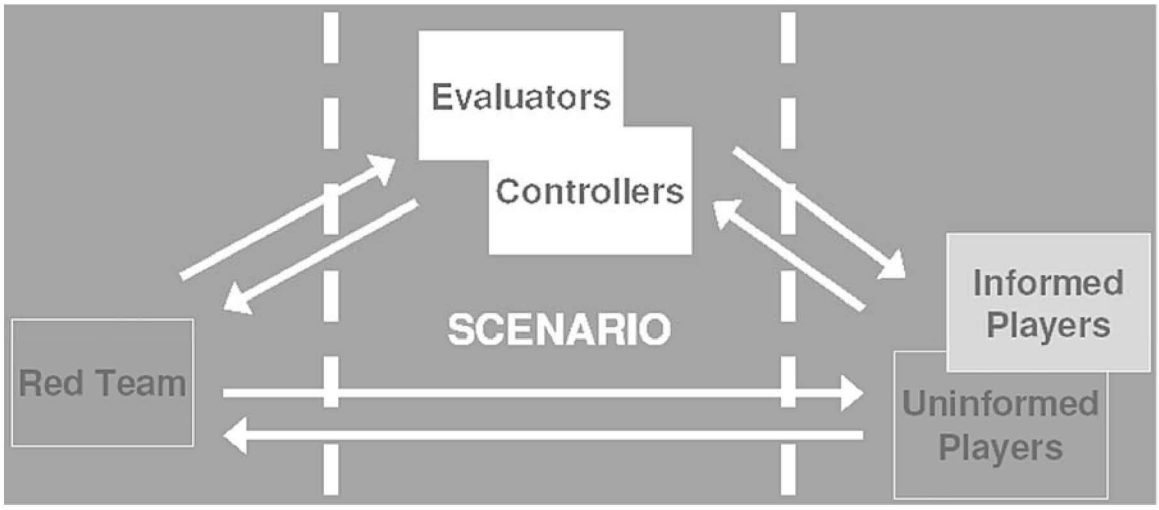

Figure 4. Red Team Participant Interactions

The red team scenario should be a general outline, not a detailed script and should be based on historical threats or known current threats. An example scenario outline might include an adversary profile, objective, target, weapon, location, and timeline. Furthermore, as mentioned earlier, red teams should only have access to information that real-world adversaries could access. In Figure 4 above, the vertical dotted lines represent information firewalls or filters. To drive exercise play, information must flow between the red and blue teams, just as it would in the real world. For example, red teams may observe (and adapt to) increased security at an intended target. The red team typically would not, however, have additional information about the cause of the increased security unless interactive play between the teams has allowed the information to be obtained. In short, the firewalls or filters are designed to ensure that information possessed by red and blue teams is as realistic as possible.

Creating the adversary scenario is dependent on knowledge of the adversary otherwise, the scenario may not reflect real world threats. Choosing a plausible adversary for a specific geographic location, however, can be sensitive if it is too closely based on actual threats. To avoid the need to use or release actual threat information, organizations can use a predetermined ‘universal adversary’ (UA), as developed by the U.S. Department of Homeland Security for use in replicating actual terrorist adversaries. The most important aspects of the universal adversary to consider for an exercise are

ideology, motivation, tactics, capability, and objectives. A shorter variation of these adversary aspects still includes academic, ideology, and operations (tactics, techniques, and procedures). The universal adversary data enables exercise players to simulate intelligence gathering and analysis and ensure realistic representation of the hazards posed to the personnel, procedures, and/or target being exercised. Local or regional intelligence background information can serve as the foundation for the selection of the universal adversary and its target(s).[72]

Red team members can use targeting information developed internally by the exercise planning team or, alternatively, may use information collection methodologies that the chosen adversary might use including the internet, other publicly available records, surveillance and planted insiders.[73]

As stated earlier, there are two general types of red team exercises, physical and analytical. In physical red team exercises, the red team operationally portrays adversaries in the field. To minimize the risks inherent with this type of exercise, red teaming must always keep safety as the foremost consideration. Without adequate safety measures there can be no exercise. Accidents, in addition to causing harm to our most valuable resource, our personnel, can lead to negative perception of exercise play and players, and cause leaders to reconsider the value of red team exercising. Red teaming does involve increased risks, however, and organizations need to make informed decisions.

Physical red teaming requires careful planning and safe execution. To abet this, exercise documentation should include a red team handbook. The handbook is a collection of all red team documentation. The purpose of the handbook is to aid in conducting safe activities and assist red team controllers in understanding their roles and responsibilities. The handbook should include a profile of the adversary, the type of threat posed by the adversary, rules of exercise play, operational safety requirements,

[72] DHS, *Homeland Security Exercise and Evaluation Program*, 11.

[73] Ibid., 13.

detailed scenario information, description of each red team operation, target information, communications plan, contact information, red team members unique identification and credentialing.[74]

Safety can be achieved by establishing clear and consistent rules of exercise play, ensuring red team members are properly selected, adequately supervised, have unique identification and sufficient training. The rules of exercise play should define the boundaries of exercise play and include guidance on the use of force, weapons, in and out of bounds areas, personal safety, hazardous environments, and others.[75] Other rules should include no real weapons; red team actions conducted within the law, and, in a prevention-oriented exercise, the final attack should not be simulated. Additionally, all props must be safe, levels of force set at pre-defined levels, protective equipment sufficient for the scenario and type of exercise, exercise sites are checked for hazards, warning signs are posted, where appropriate, and first aid is available.[76]

Red team safety controllers should be able to observe and monitor red team operators and operations without interfering or drawing unnecessary attention to their presence. Finally, every action of the red team should be observed by at least one evaluator.[77]

Analytical red teams portray an adversary but do not involve actual field play. Analytical red teaming adds value to simple discussion-based exercises and can range from basic peer review to near-real-time (notional) force on force interaction, as in games or simulations.[78]

Generally, analytical red team participants' need not all be subject matter experts but must have a strong working knowledge of their organizations plans, policies, and procedures. However, at least one red team expert should participate and have an

---

[74] DHS, *Homeland Security Exercise and Evaluation Program,* 32.

[75] Ibid., Appendix B.

[76] Lynch, "Developing a Scenario-Based Training Program," 7.

[77] DHS, *Homeland Security Exercise and Evaluation Program,* 4.

[78] DHS, *Prevention Exercise Training Course,* Module 4.

operational, academic, and most importantly ideological understanding of the portrayed adversary. The red team expert should help develop the scenario and adversary profile and assist with facilitation and team member indoctrination in the chosen adversaries ideology, motivation, capability, objective, and tactics.

During analytical red teaming, participants analyze the attack plans and look for indicators and warnings, key decision points, and vulnerabilities in the plan. Participants should assess whether their current plans, policies and procedures would be able to successfully repel an attack and, if not, work to modify and improve plans, policies and procedures to enable them a better opportunity for success.

6. Limitations of Red Teaming

While past behavior might be the best predictor of future behavior, it will not necessarily identify a future, never before seen, method of attack. There will never be enough information to predict all possible means of attack. Typically, red team exercises are based on prior events and are less likely to anticipate new, unplanned or never before seen events. In addition, attackers may look at whole systems, or multiple targets and it is not possible to exercise every area.[79] "Red teaming will not prevent surprises. But, [it] can prepare…organizations to deal with surprise. In particular, it can create the mental framework that is prepared for the unexpected."[80]

Red teaming is difficult to do and even more difficult to do well. Nor is red teaming a perfect or foolproof method of improving prevention capabilities. Red teaming is also not well suited to developing solutions to problems so much as raise issues and explore potential responses that can be explored in more detail.[81] Even the Defense Science Board's extensive research could not find agreed upon red team capabilities, functions, or means to ensure quality. Finally, there will always be some things that are tainted or influenced in some way by the fact that the red teams are not really attackers, but simply doing their best to mimic potential attackers.

---

[79] Toby Eckert, "U.S. 'Red Teams' Think Like Terrorists to Test Security," *San Diego Union-Tribune*, August 20, 2002.

[80] Culpepper, "Effectiveness of Using Red Teams," 59.

[81] Richard Brennan, "*Protecting the Homeland*" (Arlington, VA: RAND, 2002), viii.

One researcher has concluded, "Where red teams existed in active and vigorous forms…organizations have almost invariably out-performed their opponents…"[82] If done correctly, red teaming is realistic, near real world, training. Unlike traditional response operations, which begin after attackers have succeeded, prevention operations must begin before and during the planning stages of an attack. Red teaming may be one of the few reasonably effective methods to exercise those prevention tactics. As the Homeland Security Institute has said, "Red teaming must be advanced in order to aid in the understanding and anticipation of the adaptive and complex nature of the adversary."[83]

Attackers will adapt to our plans and our responses. We must also continually adapt and improve. Plans and procedures need to be stressed and once stressed, must evolve and improve. Progress does not need to be dramatic; it can be a series of incremental improvements over time. The key is that strategic, operational, and tactical planning and exercising is an iterative and evolving process.

D. THE ATTACK TREE

Attack trees are sometimes referred to as threat trees and are similar in structure to the fault trees used in system safety analysis and other areas. Bruce Schneier, a computer security expert, first introduced the concept in 1999. An attack tree is a graphical collection of boxes (nodes) laid out in a hierarchical fashion. They are designed to analyze possible attacks in a structured and systematic way and are intended to model the human decision process. A reasonably complete attack tree would illustrate all of the potential paths that an attacker could take to achieve a certain goal. For example, in an exercise, this might be an improvised explosive device (IED) attack. Each step required of or available to the attacker is modeled including decision points in the planning,

[82] Williamson Murray, "Thoughts on Red Teaming" (McClean, VA: Hicks and Associates, May 2003), 2.

[83] Shelley Kirkpatrick, PhD, Shelley Asher, Catherine Bott, "Staying One Step Ahead: Advancing Red Teaming Methodologies through Innovation" (Arlington, VA: Homeland Security Institute, 2005), 1.

preparation and attack phases, though in a prevention exercise, this would not include the attack itself. In essence, an attack tree shows a path through an exercise highlighting the various available steps, options, and decision-points of an adversary.[84]

While attack trees are a relatively new concept, they are well known in the area of cyber security. For example, American Electric Power, one of the largest electric utilities in the United States uses attack tree modeling to evaluate cyber and physical security risks.[85] One use of fault-tree based modeling is in Model Based Vulnerability Analysis or MBVA. MBVA is a form of analysis that combines network, fault, event, and risk analysis into a single methodology for conducting analysis on critical infrastructure vulnerabilities.[86]

1. Benefits of Attack Trees

Classic threat and vulnerability assessments are conducted annually or when required to generate or maintain funding. With a computerized attack tree model, information is linked and as one part of the model is updated, related parts are updated. Furthermore, models can be used to test procedures and processes for effectiveness in advance, without having to devote large numbers of resources each time. Scientific models are more advanced and detailed than simple, probabilistic, models, which generally tend to involve a greater degree of randomness. Though a model cannot substitute for an actual, physical test, it is a quick, cost-effective way to test selected system components and to determine what may or may not require further, more detailed, testing.

Typically, security systems are built on expert opinion and not on scientific evidence. They are formed over time as reactions to perceived weaknesses or attacks.

---

[84] U.S. Department of Homeland Security, "*Homeland Security Exercise and Evaluation Guidelines Volume V, Chapter One, Prevention and Deterrence Exercises, draft*" (Washington, D.C., 2006). 15.

[85] North American Electric Reliability Council, "*Risk-Assessment Methodologies for Use in the Electric Utility Industry*" (Princeton, New Jersey, September 2005), 526.

[86] Professor Ted Lewis, "*Module 5 Learning Objectives*," Center for Homeland Defense and Security, Naval Postgraduate School, https://www.chds.us/courses/mod/resource/view.php?id=364/ (Accessed July 16, 2006).

Interestingly, models are frequently used as an analysis tool—except in security.[87] Models are designed to forecast or predict what might happen based on certain 'what-if' scenarios. Additionally, they are useful to illustrate complex information in a more comprehensible manner. This is a benefit to practitioners. A thorough, well-designed, attack tree provides profiles that can characterize a broad range of attacks and is a tool to assist with the automation of threat analysis.[88] It can be especially effective in assessing risks from intelligent adversaries.[89]

Attack tree models can be modified, reused, and shared among individuals or organizations that have similar needs. This is important because complex attack trees can require significant investments in time and energy and are not simply built, but built upon. A multifaceted tree can be added to or improved upon by any number of people. They can be built over time by different people from many different disciplines. They can model dynamic changes such as new attackers, methods, motives, or resources. Attack trees can include other information such as costs, values, time, and impacts in terms of time or costs, physical or legal risks assumed by attackers, etc.[90] This ability allows it to be a potentially potent tool during prevention exercises. The information in the attack tree allows exercise planners to "develop plausible scenarios and master scenario events list (MSEL) injects, minimize artificialities, and portray accurate timelines, all of which are essential elements of an effective prevention and deterrence exercise."[91]

2. Constructing an Attack Tree

The first step in constructing an attack tree is to identify possible attack goals and plot each goal on a separate tree. Each possible attack is then deconstructed into all the steps it would take to make it happen. Each step in the process becomes a node on the

---

[87] Amenaza Technologies Limited, "*Creating Secure Systems through Attack Tree Modeling.*" www.amenaza.com/downloads/docs/5StepAttackTree_WP.pdf. Accessed September 20, 2006.

[88] Sjouke Mauw, Martijn Oostdijk, "*Foundations of Attack Trees*" (Netherlands, Eindhoven University of Technology, 2005), 1.

[89] Amenaza Technologies Limited, "*Creating Secure Systems through Attack Tree Modeling.*" www.amenaza.com/downloads/docs/5StepAttackTree_WP.pdf. Accessed September 20, 2006.

[90] Robert J. Ellison, "*Attack Trees*" (Pittsburgh, PA, Carnegie Mellon University, September 2005), 2.

[91] U.S. Department of Homeland Security, "*Homeland Security Exercise and Evaluation Guidelines Volume V, Chapter One, Prevention and Deterrence Exercises, draft*" (Washington, D.C., 2006). 15.

An attack tree can be based on historical and anticipated attack data.[92] As a tree is built, new methods or previously unconsidered paths of attack may present themselves thereby making the construction of an attack tree a prevention tool for both newer, imaginative attacks and real-world prevention activities.

Attack trees are typically represented graphically though they can be either graphical or textual. A graphical illustration is based on a tree structure. A textual illustration usually follows a numeric outline.[93] The benefit of a textual outline style of attack tree is that it may flow more logically when viewing very long or complex attack patterns.[94]

An attack tree can highlight possible paths of attack, but it can also assist by eliminating unlikely paths. For example, if an attack costs more to produce that the expected benefit, it can be reasonably assumed that it is unlikely (or at least less likely) to take place. Conversely, the higher the reward (meaning the greater destructive value of a target) compared to the cost (whether financial, logistical, human, or other), the greater the motivation. Attacks that require more resources than an attacker is known or presumed to have are not considered.

Looking at an attack tree, it may appear intuitive that weaknesses or vulnerabilities higher in the tree (closer to the root goal) should be mitigated first. This may sometimes be true, and while this may make sense in some cases, changes in one node may have implications for continued operations elsewhere.

Attack tree construction takes practice and an analytical, detail-oriented mind—even if constructing with the aid of attack tree software. Moreover, attack tree construction and analysis is better informed if planners represent a variety of disciplines, e.g., fire, health, etc. Having a variety of disciplines is most helpful when those

---

[92] Andrew Ellison, Robert J. Moore, Richard C. Linger, "*Attack Modeling for Information Security Survivability*" (Pittsburgh, PA, Carnegie Mellon University, March 2001), 20.

[93] Michael S. Pallos, "*Attack Trees: It's Jungle Out There*" (Beverly Hills, CA, The Business Forum, 2003), 2.

[94] Bruce Schneier, "*Attack Trees,*" http://www.schneier.com/paper-attacktrees-ddj-ft.html.,Accessed September 13, 2006.

disciplines are in a position to take some type of action during specific phases of the attack planning.

In an exercise, it may be easier to construct an attack tree if it is focused solely on the planned prevention exercise scenario rather than all possible means of attack. In an exercise attack tree, the actual path of attack, as determined by planners, is called the critical path.

3. The Critical Path

The planned critical path is the adversary's path through the exercise. From the prevention, or blue team, perspective, the critical path is a graphical roadmap of opportunities that are available to prevent the attack precursors shown in the attack tree. During an exercise, both attack and prevention activities can be plotted on the attack tree. This allows for evaluation of prevention activities that were useful in countering or changing attack strategies. The planned critical path can be compared to the resultant exercise critical path and any deviations noted. These deviations may represent where prevention actions were successful in pushing an adversary off their planned attack path and therefore may be indicators of successful prevention. This does not necessarily signify that where an adversary is forced to change tactics or strategies due to some intervention, that the actual attack has been prevented. Forcing an attacker to deviate from some point of their planned attack path may simply mean that the attacker has been forced to adjust to the deviation and, absent further preventative measures, returns to their planned strategies further up the attack tree or elsewhere on the threat continuum.

That said, in a prevention exercise, success should not be solely measured by the complete prevention of an attack and the apprehension of all attackers. Any prevention activity that forces attackers to change strategies or delays or diverts an attack is a partial success and should be analyzed for lessons learned that may be applicable to real world plans and procedures.[95] More importantly, though, is the identification of tactics or strategies that more or less permanently impair an attacker's ability to conduct specific attacks.

[95] U.S. Department of Homeland Security, "*Homeland Security Exercise and Evaluation Guidelines Volume V, Chapter One, Prevention and Deterrence Exercises, draft*" (Washington, D.C., 2006). 8.

As each tree is a model, it can be adjusted and fine-tuned as more and better information and intelligence becomes available. Excluding the very simplest of attacks, they are never necessarily complete.

As explained earlier, each attack goal must be put on a separate attack tree. This can lead to many differing trees. However, attacks may be consolidated into attack classes where the methods and resources used by an attacker would be similar. This allows for a reduced number of trees.

Attacks may or may not be a single event. They may consist of a series of sequential or concurrent, related events. Attack trees may not be as effective for these types of events. Furthermore, unexpected interactions in attack or prevention planning may cause failure in unanticipated areas. Future attacks might be focused on these interactions rather than on single point vulnerabilities.[97] Attack tree modeling is not a model for all security but a single tool to model specific attacks. They tend to focus on individual component failure and generally cannot account for human or organizational failures.[98]

Security is only as strong as its weakest links; fortunately, adversaries do not typically know what the weakest links are. In many cases, neither do we. Predicting human behavior is an extremely complex problem—attack trees offer a scientific approach to this problem. Security is a process, not a product. Attack trees form the basis of understanding that process.[99] The attack tree serves as a roadmap or guide to the options, actions, and decisions involved in carrying out a terrorist attack.

E. BEHAVIORAL ANALYSIS

Behavior surveillance in analysis and screening is a technique designed to detect potential threats through observation of behaviors, mannerisms, and interviews. It is based on factors, other than race, that may cause an elevated or reasonable suspicion. Behavioral analysis is based on the theory that "a person engaged in deception or in an

---

[97] Robert J. Ellison. "*Attack Trees*" (Pittsburgh, PA, Carnegie Mellon University, September 2005), 4.

[98] Nancy Leveson, "*A New Accident Model for Engineering Safer Systems*" (Cambridge, MA, Massachusetts Institute of Technology, April 2004), 27.

[99] Schneier, "*Attack Trees*", 3.

act in which the person fears being discovered will suffer mental stress, fear, or anxiety that is manifested through involuntary physical and physiological reactions that serve to dissipate the stress, fear, or anxiety."[100] Behavioral surveillance looks for behaviors that may be more common to terrorists and other criminals but is just one of many tools that may be used in exercises to identify these behaviors.

1. Limitations of Using Technology in Exercises

There are many new and interesting technologies in development that, over time, should enhance society's ability to identify potential threats. Many systems, in use or in development, are based on biometric identification. Some examples include facial recognition, iris and retinal scans, hand geometry, voice recognition, gate (walking) analysis, and DNA identification. Other new tools include Radio Frequency Identification (RFID) Systems, Automatic License Plate Recognition (ALPR) Systems, and others.

Automated License Plate Recognition systems are an interesting, and relatively more mature, example. License plate recognition was developed in the United Kingdom in the early 1980's largely as a response to repeated IRA bombings. In 1993, the technology was adapted for more routine law enforcement purposes, principally auto theft reduction. The technology has evolved to the point that, while not intended to replace the observation skills of law enforcement officers, a long-term goal of the United Kingdom's Home Office is to fully transition the technology into a mainstream tool of policing. A major step in that direction is taking place now as a nationwide system of over 2,000 fixed-mount cameras is currently being deployed in Britain. This follows the installation of mobile license plate recognition systems in all forty-three police forces throughout England.

Fingerprinting is the oldest and most common identification system. In fact, the largest biometric database in the world is the FBI's Integrated Automated Fingerprint Identification System (IAFIS) with over 47 million subjects classified. This sizable database is possible because the first systematic use of fingerprint in the United States began in 1902. It is the only biometric identification system that has been in wide use for

[100] Jim Metzger, "*Behavior Oriented Screening System*" (Philadelphia, PA, SEPTA Transit Police, 2005), 78.

more than the last 10 or 15 years.[101] Furthermore, NCIC 2000, a national database of criminal justice records, allows police patrol officers to both send and receive data from the field with laptop computers, portable fingerprint scanners, and digital cameras.[102]

Yet another part of the NCIC 2000 network is the Violent Gang and Terrorist Organization File (VGTOF). This database is designed to assist law enforcement with the identification of gang and terrorist organizations and their members.[103] Of course, names must already be known and then run through these watch lists and databases for them to be of use. The repeated failures of the intelligence community to watch-list two 9/11 conspirators, al-Mihdhar and al-Hazmi, were seen as "crucial lost opportunities" by a congressional Joint Inquiry.[104]

Many of these technologies can be used in exercises to assess authorities' ability to detect and apprehend potential threats. Most of them, however, whether those in extensive use, like fingerprints, or in development, like many of the others, are designed to identify *known* subjects. They are far less useful when the goal is to detect, deter, or prevent *any* possible threat from succeeding. Finally, these technologies continue to be developed and improved, tend to be too expensive for most agencies to deploy in significant numbers, and are not always accepted by populations apprehensive about technology that enhances surveillance and detection, therefore, their value during exercises may be limited, at least for the near future.

2. Behavioral Indicators and Warnings

Many of the above technological advances may still be years away from widespread use but they can offer some degree of prevention potential. Even so, we should use caution when placing too much reliance on technology. As the 9/11

---

[101] Federal Bureau of Investigation, "*Integrated Automated Fingerprint Identification System or IAFIS*," http://www.fbi.gov/hq/cjisd/iafis.htm. Accessed July 11, 2006.

[102] William J. Krouse, "Terrorist Identification, Screening, and Tracking under Homeland Security Presidential Directive 6," (Washington, D.C., Congressional Research Service, 2004), 31.

[103] Indiana Data and Communications System, "*IDACS 2000 Full Operator's Lesson Plan*" (Indianapolis, January 2004), 204.

[104] U.S. Congress, "*Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*" (Washington, D.C., December 2002), 148.

Commission Report noted when investigating the September 11th terrorist attacks, "...virtually all information regarding possible domestic threats came from human sources."[105]

One type of human intelligence is behavioral recognition, analysis, and screening. A number of agencies have identified common behavioral indicators that may warrant further investigation by law enforcement officers. For the purposes of this section, the referenced indicators are behavioral, and not the same as those indicators and warnings listed in the Department of Homeland Security's *Target Capabilities List*, which refers to the recognition of indicators, and warnings that are found in gathered intelligence reports and data.

The observation of behavioral indicators is a form of street-level intelligence, which requires authorities (or whomever is involved in the exercise) to be observant for potentially significant behaviors. These behaviors may indicate that an individual presents a threat or is at least suspicious enough to warrant further investigation, however, they offer no guarantee of success. They are merely indicators that should cause observers to focus their attentions more closely and may perhaps increase the odds of successful prevention or intervention.

Traditionally, police officers wait for intelligence. To be preventative, however, authorities must actively seek information and intelligence, and actively search for persons who may be suspicious—not simply respond to calls of suspicious persons or circumstances.[106] Police officers should seek to assess threats that may not rise to a level of suspicion that police would traditionally use to justify arrest or detention. Police officers are and should be willing to talk to individuals that warrant further inquiry but may be reluctant to make contact with people unless they meet the reasonable suspicion standard. For the most part, this is how police officers are trained. Not every contact by law enforcement requires that this standard be met, however. For example, voluntary interviews can be useful tools and do not require reasonable suspicion, much less

[105] National Commission on Terrorist Attacks upon the United States, "*The 9/11 Commission Report*" (Washington, D.C., 2004), 535.

[106] Metzger, "*Behavioral Screening,*" 7.

probable cause, before police officers can initiate them. The U.S. Supreme Court, in Florida V. Bostick, ruled that the "4th Amendment permits police officers to approach individuals at random in…public places to ask them questions and to request consent to search…so long as a reasonable person would understand that he or she could refuse to cooperate." In other words, law enforcement officers are permitted to ask questions and request identification without making a "seizure," as defined by the Fourth Amendment.

Behavioral analysis focuses specifically on just that—behaviors. Basing proactive investigation on race or ethnic appearance is not a reliable, or legal, indicator of terrorist or other criminal behavior. For example, Spc. Ryan Anderson (a Caucasian male and a member of the U.S. National Guard in Ft. Lewis, Washington) was charged with attempting to provide intelligence to Al-Qaeda in 2004. John Walker Lindh, the 'American Taliban, was a Caucasian male. Jose Padilla a Hispanic male. Jaradat Hanadi, involved in a 2003 suicide bombing in Israel, was a female. There are no fixed profiles of terrorists and therefore, behaviors are much better prevention tools than race or ethnicity.[107]

Behavioral analysis is not a foolproof method of detection—nothing is. There are, however, examples of behavioral analysis successful use. Once case involved a U.S. Immigration Inspector named Jose Melendez-Perez. A month before 9/11, based on suspicious behaviors, Melendez-Perez turned away Muhammed Al Kahtani, who was believed to be the planned '20th hijacker.' On the same day, at the same airport, Mohamed Atta was allowed into the country by another screener despite paperwork showing evidence of fraud.[108]

There is no single, accepted, analysis model, as behavioral analysis is an inexact and evolving science. One reasonably well developed example is the Behavioral Oriented Screening System developed by Lt. Jim Metzger for the SEPTA Transit Police Department in Pennsylvania. This system uses a 'Terrorist Characteristic Template'

[107] Metzger, *Behavioral Screening*, 69.

[108] Ibid., 99.

developed by U.S. military intelligence officers based on analysis of characteristics of 130 persons engaged in radical Islamic Jihad terrorist attacks or who had been arrested on terrorism charges.[109]

Another example was developed by New Mexico Tech for their class Prevention and Response to Suicide Bombing Incidents (See Appendix A). They have identified the nine stages of an attack. Accompanying the nine stages are pre-attack indicators for each stage and potential intelligence collection and/or enforcement actions that may help to identify and prevent a potential attack. The stages with the most likely use in a prevention exercise are those that include "potential law enforcement collections actions." New Mexico Tech's nine stages is just one behavioral analysis tool that can be used during prevention-oriented exercises.

Unfortunately, while this type of information is frequently marked sensitive and/or for limited distribution, much of it can be found on the internet. For example, the FBI's Terrorism Quick Reference Card, which lists pre-incident indicators, can be found on the websites of the New Jersey Self Storage Association, U.S. Attorney for Hawaii, and many others.[110] While it is important for individuals to be aware of potential common indicators, publication of them also provides potential threats the ability to adjust and adapt their behaviors based on known or established behavioral profiles. Unlike some criminals, terrorists are an evolving adversary, but they are not perfect. There are most likely going to be some repeating and perhaps necessary steps to carrying out attacks. For example, in looking at recent events, there is a trend towards attacking soft targets, particularly transit (e.g., Madrid in 2004, London in 2005, and Bombay in 2006). It would seem reasonable that transit security professionals focus on the most common characteristics, at least as much as they can be discerned, and use those characteristics in their security planning, training, and exercising.

Behavioral analysis is a proven, albeit imperfect, prevention tool. In the absence of effective and widespread technology, and even then, it can be a valuable and low cost

[109] Metzger, *Behavioral Screening*, 52.

[110] See http://www.njssa.org/2004%20winter.pdf and http://www.usdoj.gov/usao/hi/atac/terrorisminformation.pdf for two examples. Accessed July 13, 2006.

method of prevention. It has the added benefit of potentially applying to a wide range of other criminal behaviors and can be incorporated into training and exercise programs.

F. PRIVATE SECTOR SECURITY

"Private sector preparedness is not a luxury; it is a cost of doing business in the post 9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security." So said the 9/11 Commission Report in 2004.[111] The importance of incorporating the private sector into homeland security strategic planning, training and exercising activities is widely recognized and even formalized in many national strategies and directives including *Homeland Security Presidential Directive (HSPD) 7, HSPD 9,* the *National Preparedness Standard on Disaster/Emergency Management and Business Continuity,* the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets,* the *Intelligence Reform and Terrorism Protection Act of 2004,* the *National Response Plan,* the *National Incident Management System* and the *National Strategy for Homeland Security.*

Unfortunately, this mandate, if it can be called that, appears to be not well understood nor widely followed. Statements suggesting the integration of the private sector into prevention, preparedness, mitigation, response and recovery planning can be widely found throughout homeland security literature. Clarity on how this can be accomplished, however, particularly in the area of prevention, is less common. Moreover, where information does exist on merging the prevention efforts of the public and private sectors, specific examples of sustained, successful, and equal collaboration are even harder to find. For example, one Lessons Learned Information Sharing (LLIS) "Best Practice" on public-private partnerships in training states, "Public-private partnerships can enhance emergency prevention…efforts through cross-sector…training, and interdependency exercises." However further into the report, under the section on conducting those same joint exercises, the report drops prevention and states only "public-private partnerships can exercise established response and recovery plans and

[111] National Commission on Terrorist Attacks upon the United States, "*The 9/11 Commission Report*" (Washington, D.C., 2004), 398.

procedures."[112] In another Lessons Learned Information Sharing (LLIS) report, public-private partnerships in emergency preparedness are identified as a best practice, but the report provides only general information and guidelines on building and supporting these partnerships.[113] This paucity of specific examples also applies to private security. Unfortunately, little research, particularly when compared to the research devoted to public law enforcement, has been conducted on private sector security.

This section will not attempt to review the private sector in its entirety, but will specifically address the state of private sector *security*. It will examine the role of private security and the benefits of collaboration to both the public and private sectors. It will review the various problems that have, to date, constrained most efforts at integration into homeland security exercises and will conclude by offering several possible solutions.

Prior to 1844, when New York City started the first local governmental police force in the United States, private security was the sole provider of policing services in the United States. During the Civil War, the original Pinkerton detective agency, working for the Union Army, investigated counterfeiting cases and was given responsibility for security and counterintelligence in Washington, D.C. Pinkerton was the first organization to use rap sheets and mug shots.[114]

Determining the number of private security officers in the past is difficult. By 1970, however, the number of private security officers in the nation was estimated to be approximately equal to the number of police officers. Current estimates of private security vary significantly but the difference is generally estimated at between two and three times that of governmental law enforcement. The following table is from the Congressional Research Service.[115]

---

[112] Lessons Learned Information Sharing, "*Public-private Partnerships for Emergency Preparedness: Education, Training, and Technical Assistance*," http://www.LLIS.gov/. Accessed May 3, 2006.

[113] Lessons Learned Information Sharing, "*Public-private Partnerships for Emergency Preparedness: Overview*," http://www.LLIS.gov/. Accessed May 3, 2006.

[114] Jack Kelly, "Safety at a Price: Security is a booming, sophisticated, global business. *Post-Gazette*, February 13, 2000.

[115] Paul W. Parfomak, "Guarding America: Security Guards and U.S. Critical Infrastructure Protection," *Congressional Research Service* (Washington, D.C., 2004), 6.

Table 3. Private Security Officers in the United States

	Private Facilities	Government Facilities	Airports (Screeners)	Total
Contract	531,000		2,000	533,000
Staff	351,000	85,000	53,000	489,000
Total	967,000		55,000	1,022,000

Another estimate from the U.S. Bureau of Labor Statistics states that approximately 12,000 firms employ over one million private security officers, however, this estimate does not include 'in-house' security such as private investigation, private corrections, and others, which would add hundreds of thousands more to the estimate. Even these numbers are not necessarily definitive, however. Yet another report from the IACP and the USDOJ COPS office put the numbers closer to 90,000 private security firms and two million private security officers.[116] Interestingly, while the number of private security officers fell 124,000 between 1999 and 2003, from 2004 to 2014, U.S. private security officer employment is forecasted to grow from between nine and seventeen percent.[117] The earlier decrease is unexplained but may have been due to the economic recession in the U.S. following 9/11. Finally, perhaps the comprehensive and authoritative reports on private sector security are volumes I and II of the government-sponsored, Hallcrest reports. Unfortunately, the more recent volume II is now sixteen years old. One of the more current works on the state of private security is the *ASIS Foundation Security Report: Scope and Emerging Trends* released in 2005.

Private sector security and public law enforcement have similar goals, but also, different approaches and vastly different spheres of influence.[118] Though authority can and does vary by jurisdiction, generally, private security has similar authority to that of ordinary private citizens.[119] Listing the duties of private security, a Congressional

[116] IACP/COPS, "*Private Security/Public Policing, Vital Issues and Policy Recommendations*" (Alexandria, VA, 2005), 2.

[117] U.S. Bureau of Labor Statistics, *Occupational Outlook Handbook, 2006-07 Edition* (Washington, D.C.: Government Printing Office, 2004).

[118] IACP/COPS, "*Vital Issues*," 1.

[119] Parfomak, "*Guarding America*," 4.

Research Report stated that these duties include "protecting people and property from accidents and crime…monitor, patrol and inspect property to protect against…illegal activity…enforce laws…conduct incident interviews, prepare incident reports, and provide legal testimony…use radios to call for assistance…[and be] armed, as required by specific duty assignments."[120] While these responsibilities do not differ greatly from that of governmental law enforcement, there are, of course, distinctions in the roles of public and private security. Traditionally, the government has taken primary responsibly for intelligence gathering and other prevention efforts, (i.e., counter-terrorism) while the private sector has assumed responsibility for reducing their own risks and vulnerabilities, (i.e., anti-terrorism), or in simpler terms, the outside versus the inside. It is debatable whether these historical, and artificial, distinctions provide the nation with the greatest preventative benefit.

Some private security firms have assumed traditionally governmental roles. Firms have been hired to police communities, run prisons, and conduct traffic control. Additionally, private security has access to many resources including investigators, biometric readers, bomb detection equipment, and vehicle barriers.

Private security, while assuming additional responsibilities, has also assumed more risk. In August 2004, The U.S. Department of Homeland Security (DHS) issued a terror alert for financial institutions in three cities, New York, Washington, DC, and Newark, NJ. Reports stated that terrorist surveillance included the location, weaponry, and activity of private security officers at those institutions.[121]

There is no reason for private sector security to wait for an event to happen, to be, trained, exercised, and therefore prepared only for that eventuality. In fact, the major responsibility of a security officer is prevention *before* an incident/offense occurs.[122]

---

[120] Parfomak, "*Guarding America*," 4.

[121] Ibid.

[122] State of California, Bureau of Security and Investigative Services, "*Power to Arrest Training Manual*" (West Sacramento, CA. November 2005), 12.

1. Benefits of Collaboration

Ideally, true collaboration would lead to benefits for both law enforcement and private security. While any specific effort may result in more or less benefit, to be successful, interested parties need to believe they are getting at least something close to what they are putting in. In other words, a cost-benefit analysis would demonstrate that the partnership is providing value to the agency and/or company.

Considering the potential resources, in addition to the sheer number of people available in the private sector, the benefits to the public sector would seem apparent. In addition to assisting public sector agencies with emergencies after the fact, private security can also assist with providing low or no cost training and sharing equipment and office space. Private security can assist with identifying and locating evidence in criminal investigations, (e.g., witness statements, records, etc.). In New York City, certain private security officers search for and lift fingerprints. They have also assisted in compiling an inventory of CCTV camera locations to assist follow-up unit investigators. Private security can assist with the collection and analysis of information and intelligence. Private security also employs specialists in various areas including CCTV, physical and facility security, computer security, biometric identification, and others. These efforts can have a positive effect not only on terrorism, but also other types of crime, and may serve to reduce calls for service and duplication of efforts. In this, private security appears to want to be an active partner. According to former ASIS International Chairman Regis Becker, "As an industry, we are prepared and willing to play a greater role in crime control..."[123] Sharing the burden of anti-terrorism and counterterrorism with the private sector not only frees up resources in the public sector, it also makes those efforts more comprehensive and effective.

There are benefits to private security as well. Increasing collaboration with the public sector, in addition to helping to develop and improve personal and professional relationships, can assist the private sector in receiving more frequent and detailed threat information as well as information about developing patterns and trends that might effect

[123] Christopher John Hetherington, "Private Security as an Essential Component of Homeland Security" (master's thesis, Naval Postgraduate School, Monterey, CA, 2004), 15.

individual businesses. It can assist in developing strategies for the protection of vital records. Collaboration would also help law enforcement better understand the corporate needs of private security. Public sector law enforcement, like private security, also has areas of expertise that can be shared. For example, police agencies have skilled interviewers, investigators, and crime analysis and crime prevention specialists. Joint operations, training, and exercises, can reduce workplace violence and improve employee safety. This increased training can help to maintain customer and shareholder confidence in the professionalism and capabilities of a company's security force. Over the long term, improved relationships would allow for the sharing of research and best practices, even the tracking of legislation of interest to public and private security.

Unfortunately, many of the current collaboration efforts, even where successful, are not done at both the managements and street levels. Additionally, many programs tend to be police-driven.[124] While there are clearly benefits to both law enforcement and private security, ultimately, the nation as a whole benefits from effective, institutionalized, public-private collaboration.

2. Problems in the Private Sector

Private security officers have been referred to as real first responders or sometimes, 'first preventers.' On 9/11, many police officers and firefighters lost their lives but less well known is that some three-dozen private security officers were also killed.[125] The value of public/private partnerships does not appear to be in dispute. Unfortunately, there are many difficulties restricting and inhibiting the ability of the public and private sectors in working more closely, and many of these problems rest with the private sector.

One significant, and perhaps justified, fear from both the private and public sectors is in the area of sharing information. Law enforcement officials may fear information sharing with companies that are foreign owned, (e.g., the two largest private security companies operating in the U.S. are both owned by firms located outside of the

[124] Bureau of Justice Assistance, U.S. Department of Justice, "*Operation Cooperation: Partnership Profiles*," (Washington, D.C., 1999), 27.

[125] IACP/COPS, *Vital Issues*, 13.

U.S.). Additionally, there may be legal restrictions on the sharing of certain types of information, particularly as it relates to the sources of information and methods used to obtain it. Sources and methods, however, are not commonly shared by the federal government with local and state law enforcement either and even when that type of information is shared, it is greatly restricted. In any event, information itself, not sources and methods, is typically what is most important.

Companies reporting crimes may fear that criminal investigators may need to seize company assets as part of their investigation. They may fear that information shared with law enforcement may become part of the public record or that sensitive information may get into the hands of competitors.

Private sector groups frequently share information about suspicious activity and other threats with industry peers and the federal government through various networks including the critical infrastructure ISACs. That same information is not always shared with state and local public safety partners.[126] In fact, information is not always shared from private security management to the private security officers on the ground. According to a 2004 survey, private sector security directors in Manhattan were reluctant to share sensitive information with subordinates due to a lack of trust.[127]

Most private security officers work under one of two employment structures—private security companies who hire out services under contract and private security officers working directly for employees as part of regular staff. Either private security structure may be used at private or public faculties. Within these structures, private security is not always a unified function. It may be part of other services including parking and others. In addition, approximately 14% of all private security officers, and more in the contract realm than the staff employee realm, are part-time employees.[128] A

[126] Lessons Learned Information Sharing, "*Public-private Partnerships For Emergency Preparedness: Information Sharing*," http://www.LLIS.gov/. Accessed May 3, 2006.

[127] Hetherington, "*Private Security*," 29.

[128] Security Magazine, "*Security's Top Guarding Companies*," January 2004.

the state. Some reported having no training of any kind. Even more alarming, many cases were uncovered where private security firms employed unlicensed security officers, many who had committed crimes in other states or whose fingerprints were never sent in to be checked, as required. Half of the 868 companies audited were referred for disciplinary action.[136]

This lack of training is not uncommon. In a 2002 survey, over one fifth of private security officers in California, Texas and Florida reported they had received no training of any kind either pre-or post hire. This occurred despite state laws mandating certain minimum training standards.[137]

This poor record on training also applies to the use of drills and exercises. In the 2002 California survey, only 52% of private security employers had conducted emergency drills and just 33% had conducted bomb-threat drills. Another survey in 2004, this one of hazardous chemical storage facilities, found in the preceding 12 months, 68% had provided emergency response training. 59% had conducted response drills, and 38% had improved training and procedures to "*prevent* possible terrorist attacks." What was also discovered was that over one-half of the private security officers in the three-state survey had never participated in an emergency drill of any kind.[138] Encouragingly, the recent *ASIS Foundation Report* noted that over half of ASIS Security Services companies believed that cross training of personnel with law enforcement is either moderately or very important. Over eighty percent believed that education regarding security and police roles is important.[139]

---

[136] Betsy Gotbaum, "*Undertrained, Underpaid, and Unprepared: Security Officers Report Deficient Safety Standards in Manhattan Office Buildings*" (New York: Public Advocate for the City of New York, 2005), 6.

[137] Peter D. Hart Research Associates, "A Post-September 11 Report on Surveys of Security Officers in California, Texas, and Florida" (Washington, D.C.: Prepared for the Service Employees International Union (SEIU), 2002).

[138] Carolyn Said. "Security Lapse: Private Guards Get Little Training and Low Pay, Study Says." *San Francisco Chronicle*, June 11, 2002.

[139] ASIS Foundation, "Security Report: Scope and Emerging Trends" (Alexandria, VA, ASIS Foundation, 2005), 40.

Private security officers may be armed or unarmed but most commonly are unarmed. Companies may not see a business need for security to have improved weaponry and protective equipment, or there may be a fear of the increased liability associated with armed security officers. With training and education standards so low and inconsistent, there may be some validity to this viewpoint. However similar fears were one of the reasons the U.S. Marines assigned to barracks security in Lebanon in 1984 were unarmed and therefore unable to stop the suicide bombing attack that killed 241 soldiers. Legitimate reasons may exist for security to be unarmed, but lack of training and the resultant fear of liability should not be among them as lack of training is a problem readily identified and easily remedied.

Arming private security officers, or even providing better training, will not always provide better prevention because not all threats are guardable. Moreover, increasing the number of human guards (whether police or private security) does not always equate to increased security at a given site and in some cases, might even cause a facility to be *less* secure. For example, no amount of human security on the ground would stop an attack from the air.[140] Additionally, larger numbers of security officers, particularly if they are not properly screened, leads to greater access which would increase the opportunity for infiltrators or other less than trustworthy private security forces to inculcate themselves into a given location or operation.

3. Solutions to Problems in Private Sector Security

On the most basic level, there are issues of trust between the sectors. One reason for this distrust is the lack of screening among private security employers. The *National Strategy for Homeland Security* states, "Time-efficient, through and period back screening…is an important tool for protecting against 'insider threat."[141] The *Intelligence Reform and Terrorism Prevention Act of 2004* allows for criminal background checks of private security officers every twelve months but also allows for states to opt-out of this requirement. Furthermore, there is no widely accepted certification process or national standards for private security officers. Considering the wide variety of security officer

[140] Parfomak, "*Guarding America*," 12.

[141] Ibid., 15.

roles and duties, however, a national standard may be too broad. For example, there is also no single national standard for law enforcement, though regulation at the state level and the impact of case law has created a de-facto, albeit non-uniform, standard.

The *National Strategy* states, "there is an urgent need for ongoing training of security personnel…"[142] The largest private security association in the world, ASIS International, has proposed minimal selection and training standards for use by regulating bodies and companies.[143] ASIS recommends that security officers receive 48 hours of training within their first 100 days of employment. In addition, their guidelines recommend that training topics include information sharing and crime prevention. The ASIS foundation report found that the only condition that law enforcement survey respondents not rated as good or very good was the training received by private sector security.[144]

A number of private security responsibilities can be exercised. Some of these prevention type activities include access-control, screening, intrusion detection, general monitoring of suspicious activity and the safeguarding of information, (e.g., blueprints, security schedules and routines, sensitive information, etc). While each area relates to general prevention, much of it is also facility or location specific.

Police departments regularly meet with local community members including business associations but tend not to meet with private security officials in any systematic way.[145] A summit of public law enforcement and private security leaders indicated that only 5-10% of law enforcement chief executives had partnerships with private sector security.[146] This can change if both public and private stakeholders identify clear benefits for each. Law enforcement administrators tend to spend time putting out fires and focusing on those who make the most noise. Working more closely with the private

---

[142] Parfomak, "*Guarding America*," 17.

[143] ASIS International, "Private Security Officer Selection and Training" (Alexandria, VA, 2004).

[144] ASIS Foundation. "Security Report: Scope and Emerging Trends" (Alexandria, VA, ASIS Foundation, 2005), 42.

[145] IACP, COPS, *Vital Issues*, 12.

[146] Ibid.

sector would require strategic planning and on-going commitment. It can be done. In Israel, for example, there is a "profound amount of intelligence sharing between the private security officers…and the police."[147]

The New York City police department has created the Area Police Private Security Liaison (APPL) program. This program allows information to be shared with private security and includes liaisons with specific private security organizations including hotels, jewelers, retail, contract security, and others. Modeled after APPL, the Nassau County New York Police Department has created the Security Police Information Network (SPIN), a voluntary information-sharing network that includes both vetted and non-vetted members of the private sector. Vetted members require background checks and include members associated with corporate security, critical infrastructure, hospitals, schools, and others. Non-vetted members include those associated with chambers of commerce, civic associations, etc. To prevent overload, a well-designed network would send out information only to those in the network who should receive it. The SPIN also allows for members of private security to feed back into the information-sharing network.[148] Another good example of information sharing can be found in the Critical Infrastructure Information Sharing and Analysis Centers (ISAC). ISAC's are private sector organizations designed to gather, analyze, and disseminate information about their respective critical infrastructure sectors. There are, unfortunately, many impediments to better information sharing between the public and private sectors. It may not be realistic for these to be addressed in any thorough and systematic way, though, until the many difficulties with information sharing *within* government are first addressed.

---

[147] *Security Management*," Training in Israel for Terrorism in the U.S.," (Alexandria, VA, ASIS International, November 2005).

[148] Matthew J. Simeone, "The Power of Public-Private Partnerships: P3 Networks in Policing," (Quantico, VA, *National Academy Associates*, January/February 2006).

Some other positive examples exist. In New York City, the police department conducts threat assessments on private properties on request. Their assessment team will produce a written report, which will include security suggestions. This serves to reduce risk and is, therefore, a form of prevention.[149]

In England, the City of London Police have developed a program called Project Griffin which entails training private security in, among other things, terrorism planning and emergency services command and control. Griffin also has a "bridge call" plan, which allows the sharing of threat and crime trend information with security managers. Finally, Griffin allows for the deployment of security officers working alongside police officers on cordon control in major incidents.[150]

4. Conclusion

While it may be counter to current thinking, and though there are undoubtedly exceptions, private sector security does not appear ready for full and complete incorporation into public sector training and exercise programs. This conclusion is reached not due to a lack of desire or from bias; but it is apparent that private sector security needs to make significant structural changes to its profession. While a uniform national private security officer standard may or may not be necessary or even the most efficient manner to regulate private security officers nationwide, the social benefit of increased preparedness in the private sector may outweigh the private sector costs associated with the tasks required to accomplish it. Unfortunately, to this point, the private sector has appeared to invest relatively little additional capital in increased security.[151]

The business community has not yet created an adequate foundation for prevention. This foundation would allow for the training and exercising of private sector prevention efforts. For example, in a report on private sector crisis preparedness written

---

[149] Craig Horowitz, "The NYPD's War on Terror," *New York Magazine*, (New York, February 3, 2003).

[150] City of London Police, "Project Griffin," http://www.cityoflondon.police.uk/countering-terrorism/terrorism-griffin.html/. Accessed April 4, 2006.

[151] Congressional Budget Office, "Homeland Security and the Private Sector," (Washington, D.C., 2004. 1.

by the Business Roundtable, in a section on smart practices, the only type of exercise listed is evacuation. The report also briefly mentions that the private sector should review lessons learned from governmental exercises and real-world events. Interestingly, the report includes a list from the Department of Homeland Security on what should be done at various threat levels, and many of these recommendations include the testing of plans and procedures, but there appears to be little information about *how* to conduct those tests.[152]

Compounding the problem, there appears to be little desire on the part of government to address the shortcomings. A 2006 Colorado review addressing the need for state regulation of private security concluded that "the potential for harm is almost intuitive" but that since they did not have examples of actual harm they conclude that "the absence of regulation [of private security officers and companies] has not harmed [and based on this logic, apparently cannot and will not harm] Colorado citizens." The report states that increasing professionalism in the [private security] industry is "irrelevant to public protection." From these seemingly contradictory opinions, the state of Colorado has concluded that regulation of private security is not justified. In fact, their analysis concluded that regulation (consisting of licensing, training, and background checks) for private security would be an *unnecessary* barrier to entry.[153] The authors apparently believe that the current lack of meaningful entry requirements provides sufficient protection.

At the federal level, a bill introduced in 2004 called the "Private Sector Preparedness Act of 2004" would have amended the *Homeland Security Act of 2002* to direct the Department of Homeland Security to "develop and implement a program to

[152] Business Roundtable, "A Private-Sector Crisis Preparedness Guide," (Washington, D.C., March 2005), 28.

[153] Colorado Department of Regulatory Agencies, "Private Security Companies and Private Security Guards" (Denver, CO, 2006), 32.

enhance private sector preparedness for emergencies and disasters, including acts of terrorism." The bill would not have applied to staff private security officers and did not include a prevention component. It never became law.[154]

The private sector security industry is marked by low pay, few benefits, little, if any training, few, if any, standards, high turnover, and almost no governmental oversight. Nearly anyone walking down the street can be hired, given a uniform, badge, and keys to a building, and are then trusted with security. This is security in name only. The full inclusion of private sector security into homeland security prevention exercises would not be without risk. Most encouragingly is that the largest professional private security organizations, including ASIS International, recognize the need for increased training and heightened standards and are working towards that goal.

Clearly, many tools exist that can and will be useful in the area of prevention, and many, if not most, of these, can also be tested through the exercise process. Focusing on all-crimes and using behavioral analysis are tools that can and should be used both in the real world, and in prevention exercise scenarios. Private sector security can be incorporated into exercises, provided there is understanding of the risks and limitations inherent in doing so. Information Sharing Environment Analysis, Red Teaming, and Attack Trees are relatively new tools, however, the Department of Homeland Security in its Terrorism Exercise Prevention Program is piloting their use. Additionally, intelligence exercises are not uncommon.

Furthermore, the TOPOFF series of national exercises is increasingly incorporating intelligence and prevention into its design. The following section describes several exercises that involved varying levels of intelligence and other prevention components.

154 "Private Sector Preparedness Act of 2004," http://www.theorator.com/bills108/hr4830.html. Accessed May 1, 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PREVENTION EXERCISE EXAMPLES

As stated earlier, prevention measures have been incorporated, to varying degrees, into homeland security exercises. While examples are still few, it is apparent that it can be done. Following are several examples of recent prevention exercises or exercises with prevention components.

A. NEW YORK STATE PILOT PREVENTION EXERCISE

The New York State Pilot Prevention and Deterrence Exercise was conducted June 1-23, 2005 in New York State. The exercise, conducted by the New York State Police, New York Office of Homeland Security, Upstate New York Regional Intelligence Center, FBI, DHS Office for Domestic Preparedness, and many local law enforcement agencies statewide, had the potential to reach over 200 organizations including ten private sector organizations.[155] New York State hosted the exercise as they have made significant progress in creating a workable intelligence fusion center and was keenly interested in exercising their capabilities. The purpose of the 23-day exercise was to evaluate processes to recognize, collect, analyze, and disseminate criminal information and intelligence.

The objectives of the exercise were to assess capabilities in three prevention-related competencies from the *Target Capabilities List:* Information Collection and Threat Recognition, including the ability to identify indicators and warning signs; Intelligence Fusion and Analysis, including the ability to glean relevant intelligence encompassed in 'white noise'; and, Information Sharing and Collaboration, including the ability to communicate both vertically and horizontally.[156]

The exercise was unclassified and largely unscripted, and was based on realistic threats to the Nation and the New York State area. There was no media play. The 23 day exercise timeline was a compression of 365 days of exercise-related intelligence and

[155] U.S. Department of Homeland Security, "HSEEP Newsletter" (Washington, D.C., August 2005). 5.

[156] U.S. Department of Homeland Security, ""New York Prevention and Deterrence Pilot Functional Exercise with Red Team - Exercise Plan" (Washington, D.C., 2005), 1-2.

For the exercise, the red teams were prohibited from interacting with senior elected or appointed officials, minors, geographic areas outside the designated areas of play, and any sites not specifically allowed for red team play.[159]

As part of the after-action review process, exercise planners learned of the importance of closely synchronizing red team play with Master Scenario Events List (MSEL) injects. Additionally, the prevention exercise timeline was not fully understood by all players and required more detailed briefings and training. The exercise plan also called for intelligence to be front-loaded, however, participants believed it would have been preferable if intelligence had been injected continuously rather than on pre-selected days. Finally, it was determined that expected player actions and possible contingency injects (particularly those related to red team play) should be scripted in the MSEL to ensure that exercise play flows properly and that controllers and evaluators have benchmarks with which to work.[160]

B. L.A. COUNTY TERRORISM EARLY WARNING EXERCISE[161]

This multi-agency, discussion based, group tabletop, prevention and deterrence exercise, was conducted on June 21, 2005 in Montebello, California. The exercise was the third in a series of exercises conducted as part of Los Angeles County's 2005 Chimera exercise program. Los Angeles County's three-year exercise goals are as follows:

- Prevent acts of terrorism
- Reduce Los Angeles County's vulnerability
- Minimize damage from attacks

Los Angeles County conducts it's exercise program in accordance with the Department of Homeland Security's *Homeland Security Exercise and Evaluation Program* (HSEEP) guidelines. The County's exercise strategy is built on a series of

[159] U.S. Department of Homeland Security, "New York Prevention and Deterrence Pilot Functional Exercise with Red Team - Exercise Plan" (Washington, D.C., 2005), 3-3.

[160] U.S. Department of Homeland Security, Prevention and Deterrence Exercise Support Team, "[New York State] Pilot Exercise Internal AAR and IP," (Washington, D.C., 2005), 1-4.

[161] Except as otherwise noted, all references to the Chimera exercise are from the Los Angeles County Operational Area Exercise Program, "Operation Chimera 2005 Terrorism Early Warning Group Tabletop Exercise After-Action Report" (Los Angeles, CA, 2005), 1-A3.

Investigation. There were a total of 33 players, one observer, and 12 controller/evaluator/facilitators. Health Departments represented 44% of the total exercise participants.

The TEW exercise was specifically designed to enhance participant understanding of the TEW concept and operations. The exercise objectives, taken from the *Target Capabilities List*, were to:

- Identify procedures for determining indicators & warnings, increasing surveillance, exploiting real-time intelligence resources dealing with suspicious outbreak of disease, and
- Identify procedures for sharing intelligence information

Exercise participants were given an overview of the TEW Epidemiological Intelligence Cell, which consist of five components: active/syndromic surveillance, passive surveillance, psychological threat assessment, human intelligence, and open source intelligence. Participants were also given information on the TEW Bio Terrorism Playbook. The Playbook is a guideline for the TEW's response in an actual event. The purpose of the Playbook is to provide essential information and recommended courses of action. The prevention (pre-release) element of the exercise lasted approximately one hour. This demonstrates that prevention exercises can be of short or long duration.

C. TOP OFFICIALS (TOPOFF) EXERCISE SERIES

TOPOFF is a congressionally mandated, biennial, exercise program, which conducts a functional exercise in the first year and a full-scale exercise in the second year, with continuity provided by a series of seminars. The TOPOFF exercise series is the cornerstone of the National Exercise Program. While TOPOFF is not specifically oriented towards prevention and deterrence, over time, these exercises have increasingly incorporated intelligence and prevention actions into the scenarios. TOPOFF 2000, the first in the series, did not include a prevention component but is included here for accuracy and completeness in describing the evolution of prevention in the TOPOFF exercise series.

1. TOPOFF 2000

TOPOFF 2000 was conducted from May 17-23 in 2000 at a cost of about 3.5 million dollars. The exercise was hosted by two localities, Denver, which exercised a bio-

terrorism (Pneumonic Plague) release, and Portsmouth, Hew Hampshire, which exercised a chemical (Sulfur Mustard) attack. The exercises involved approximately 6000 participants and were co-chaired by the Department of Justice and the Federal Emergency Management Agency. There was no international component and only limited play by the medical community. The exercise did not have a prevention and deterrence component and was designed to assess the nation's crisis and consequence management capability.[163]

TOPOFF 2000 was mandated and advertised to be a "no-notice" event and the actual scenario was unclassified, but restricted. The "dates, times and content of the exercise, however, were known to many outside the planning group well in advance of the exercise."[164] Additionally, The TOPOFF 2000 After-Action Report stated, "logistical and scheduling considerations for a no-notice national exercise are exceptionally challenging [and]...the no-notice requirement should be reconsidered."[165] One difficulty with the information being so readily available was that not all participants treated the information as private. The After-Action Report also stated, "some agencies came to the exercise with choreographed responses knowing exactly what the exercise was going to require from them."[166]

The scenario involved a member of a fictional terrorist group being arrested in London, causing the [terrorist group's] original attack timetable to be moved forward.[167] This information was used to enable the exercise scenario to move forward with a realistic foundation, not necessarily for the specific use of participants during the

[163] National Response Team, "Exercise TOPOFF 2000 and National Capital Region After-Action Report: Final Report" (Washington, D.C., August 2001), 1.

[164] Federal Emergency Management Agency, Department of Justice, "Top Officials (TOPOFF) 2000 Exercise Observation Report" (Washington, D.C., April 30, 2002), A-3.

[165] FEMA, DOJ, "*TOPOFF 2000 Report*," EX-31.

[166] Ibid., EX-48.

[167] Ibid., 1-21.

exercise. According to the FBI, "pre-exercise simulated intelligence was satisfactory…Agents collected the necessary information and did not need extensive pre-event background information."[168]

One of the FBI's exercise objectives in TOPOFF 2000 was "collecting, analyzing, prioritizing, and dissemination intelligence…at the on-site locations and at the national level."[169] In addition, the FBI was to "conduct threat assessments and pre-event intelligence for jurisdictions."[170] Intelligence information during the exercise was intended primarily to locate and apprehend the involved suspects, and not to prevent an attack from occurring. This was consistent with the exercise design and objectives.

There were many, candid, after-action comments by participants. Perhaps the most interesting was that TOPOFF 2000 did not have sufficient participation by top officials.[171]

2. TOPOFF 2

TOPOFF 2 (T2) was the second in the congressionally mandated TOPOFF exercise series and was conducted the week of May 12-16, 2003. The full-scale portion of the exercise involved approximately 8500 participants and was the largest peacetime exercise (up to that time), ever sponsored by the Department of Homeland Security or the Department of State.[172] The exercise cost approximately 16 million dollars and was intended, according to then Secretary Tom Ridge, as a test of "strategies, responses, and protocols [to enable participants to] learn a lot about...response capabilities."[173]

---

[168] FEMA, DOJ, "*TOPOFF 2000 Report,*" 1-46.

[169] Ibid., A-2.

[170] "TOPOFF Exercise Planning Conference Final Report: May 21, 1999," http://www.gnyha.org/eprc/general/nbc/chemical/200202_ChemGuidebook.pdf. Accessed August 12, 2006.

[171] U.S. Department of Homeland Security, "TOPOFF 2 After-Action Report" (Washington, D.C., August 18, 2003), 219.

[172] U.S. Department of Homeland Security, "Exercise T2 Evaluation Plan (EVALPLAN)" (Washington, D.C., May 2003), 2.

[173] John Mintz, Edward Walsh, "Huge Homeland Security Drill Planned," *Washington Post*, May 5, 2003.

Unlike TOPOFF 2000, T2 was, depending on the participant, either a limited or a full-notice event. Participants were allowed to review much of the scenario, if they so desired. Many chose to avoid exposure to scenario information to make the event a more realistic challenge. TOPOFF 2 exercise designers "deliberately erred in favor of maximizing continuous learning rather than sequestering the scenario."[174]

TOPOFF 2 involved sixteen major exercise activities conducted for 103 federal, state, local, and international departments and agencies.[175] The exercise also involved extensive media coverage from both the real media and exercise player media. T2 was also the first exercise in the series to be conducted after the creation of the Department of Homeland Security, National Response Plan, National Incident Management System, and the Homeland Security Advisory System (HSAS). In addition, TOPOFF 2 was the first time the HSAS threat condition was raised to red (whether real or exercised).[176]

This second TOPOFF involved two full-scale response exercises: A Pneumonic Plague (Yersinia pestis) release in several Chicago metropolitan area locations and a radiological dispersal device explosion in Seattle. It also involved one of the largest hospital mass casualty exercises every conducted (64 hospitals in the Chicago metro area).[177]

Prevention and deterrence played a slightly greater role than in TOPOFF 2000. Neither venue (Seattle or Illinois), however, listed prevention or intelligence as one of its exercise objectives. Moreover, only four percent of federal agency participant objectives related to intelligence.[178]

---

[174] U.S. Department of Homeland Security, "TOPOFF 2 After-Action Report" (Washington, D.C., August 18 2003), 218.

[175] Select Committee on Homeland Security - U.S. House of Representatives, "Statement of C. Suzanne Mencer" (Washington, D.C., July 8, 2004), 4.

[176] U.S. DHS, "*TOPOFF 2 AAR*, 230.

[177] U.S. DHS, "*TOPOFF 2 AAR*, 231.

[178] U.S. Department of Homeland Security, "Exercise T2 Evaluation Plan (EVALPLAN)" (Washington, D.C., May 2003), 11.

The following section is from the TOPOFF 2 After-Action Report:[179]

> T2 intelligence play was purposefully designed to provide background support to drive the exercise scenario. For simplicity, T2 did not provide an opportunity for analytical review and development of intelligence. Several comments suggested including enough depth and complexity of notional intelligence processing to allow analysis play in real time. Such intelligence play should enable and promote the intelligence buildup at exercise commencement, and continue as a robust element of play throughout the event. The intelligence community should provide answers to requests for information, including the production of "tear-lines" so that DHS can produce press releases based on product produced. This concept would support the concept of prevention, an important aspect of homeland security.

The full-scale exercises in both states involved active opposition forces. This part of the scenario, however, was limited in scope to "tactical support by Seattle Police Department SWAT, U.S. Coast Guard, FBI SWAT in Seattle and in Illinois to the Illinois State Police and the FBI Hostage Rescue Team (HRT).[180]

Like TOPOFF 2000, intelligence was primarily used to drive exercise play. Unlike TOPOFF 2000, however, T2 involved "significant pre-exercise intelligence play."[181] The "[full-scale exercise] de-emphasized attribution issues by making it relatively easy for authorities to discover that the attack was undertaken by GLODO (the fictionalized adversary). The exercise did less than it could have to test how the intelligence…machinery deals with a terrorist attack."[182] The scenario involved a "swift and effective response by [law enforcement]." Terrorist's safe houses were scripted to be identified within 36 hours of the initial attack.[183]

---

[179] U.S. DHS, "*TOPOFF 2 AAR*," 226.

[180] U.S. DHS, "*TOPOFF 2 AAR*," 213-215.

[181] U.S. Department of Homeland Security, "Top Officials (TOPOFF) Exercise Series: TOPOFF 2 -- After Action Summary Report for Public Release" (Washington, D.C., December 19, 2003), 2.

[182] Institute for International Studies Center for International Security & Cooperation, "Final Report: Top Officials 2 Full Scale Exercise, May 11-15, 2003" (Palo Alto, CA: Stanford University, 2003), 37.

[183] John Mintz, Edward Walsh, "Huge Homeland Security Drill Planned," *Washington Post*, May 5, 2003.

Following is the timeline used in the Washington State portion of the exercise: [184]

D-60: Global indicators and warnings

D-6: Increase in hostile cyber-activity; threat condition elevated from yellow to orange. U.S. intelligence picks up credible threats related to a notionalized terror group

D-3: Credible threat against Columbia Generating Station

D+1: Two terrorist suspects captured

D+2: Terrorists attempt to flee the area and cross the U.S. Canadian border.

One informal after-action comment about the Seattle full-scale exercise by an observer in the health field was that threats were not shared with the Department of Health and Human Services or other local authorities outside of law enforcement.[185]

3. TOPOFF 3

The most recent TOPOFF exercise was TOPOFF 3 (T3), conducted April 4-8 2005. Eight states and one territory applied to host the exercise before the States of Connecticut and New Jersey, along with jurisdictions from the United Kingdom and Canada, were selected to play. New Jersey exercised a biological release of pneumonic plague and Connecticut exercised a chemical explosion. International travelers were notionally exposed to the biological agent, which facilitated play with the United Kingdom and Canada.

T3 was another limited-notice exercise. It involved approximately 22,000 participants, 27 federal Departments and Agencies, 30 state, and 44 local departments and agencies, in addition to 156 private sector organizations across 4 separate venues. This exercise was billed as the largest, most complex, comprehensive, dynamic, and ambitious, counterterrorism exercise ever conducted in the U.S. it incorporated many

[184] U.S. Department of Homeland Security, "Exercise T2 Evaluation Plan (EVALPLAN)" (Washington, D.C., May 2003), 14-15.

[185] Andy Stevermer, Capt., "TOPOFF 2 in Seattle: Lessons and Challenges" (Seattle, WA: Presentation given August 2003, http://depts.washington.edu/nwcphp/siphp2003/summerinst.html)/. Accessed August 12, 2006.

more elements, roles and participants that in previous exercises. The exercise cost over 21 million dollars.[186] Thirteen countries participated as observers.[187]

TOPOFF 3 involved the following cycle of activities:[188]

- Command Post Exercise (May, 2004)
- Seminars and Planning Events
- Advanced Distance Learning Exercises (January, 2005)
- Simulated intelligence activities (March, 2005)
- Full-Scale Exercises (April, 2005)
- Large-Scale Game (May, 2005)
- After-Action Conference (June, 2005)

Prevention was an underlying theme in TOPOFF 3. Nationally, the exercises focused on four critical areas, one of which was intelligence/investigation, to test the flow, handling, and sharing of time-critical information. The State of Connecticut listed seven overarching objectives, one of which was to "examine interagency intelligence sharing processes required to prevent terrorist attacks."[189] The State of New Jersey listed twelve over arching goals, one of which was to "explore the multi-level, operational coordination of intelligence and investigative authorities."[190] Therefore, for the first time in a TOPOFF exercise, a significant prevention element was included.

Unlike previous TOPOFF exercises, in T3 the adversary was fictionalized but based on real world terrorist groups. Exercise designers planned a simulated stream of

---

[186] U.S. Department of Homeland Security, Office of Inspections and Special Reviews, "A Review of the Top Officials 3 Exercise" (Washington, D.C., November 2005), 76.

[187] U.S. Department of Homeland Security - Press Release, "Transcript of Press Conference with Secretary of Homeland Security Michael Chertoff on the TOPOFF 3 Exercise" (Washington, D.C., April 4, 2005), 1.

[188] U.S. Department of Homeland Security - Press Release, "TOPOFF 3 Exercise Program Press Kit" (Washington, D.C., April 4, 2005), 1.

[189] College of Continuing Studies University of Connecticut, Homeland Security Education Center, "State of Connecticut TOPOFF 3 After-Action Report: Summary of Key Findings" (Storrs, CT, January 2006), 5.

[190] New Jersey Domestic Security Preparedness Task Force, "2004/2005 Progress Report" (January 2006), 71.

intelligence involving "all intelligence agencies"[191] The goal of the intelligence was to influence player actions, create decision-making avenues, and provide participants with an opportunity to exercise against a realistic and adaptive adversary with the intent to test law enforcement and intelligence capabilities to detect, disrupt, and react to ambiguous and changing information as early as possible. The prevention aspect was intended to allow law enforcement and intelligence to fully deploy their operational procedures, engage their analysts, and provide vital information to exercise participants.[192] Unlike TOPOFF 2, the intelligence component of the exercises was crafted over an extended period by representatives from the various agencies participating in the exercise. Using this type of exercise design group requires a lead agency be designated to ensure participating planners stay on track.

The FBI, and state and local law enforcement, were provided a stream of false information about several possible terrorist attacks for the four weeks preceding the full-scale exercises. The purpose of the information was to provide an opportunity to piece together the puzzle and stop (at least one of) the attacks before they occurred. Both New Jersey and Connecticut each had one planned prevention event.

Information was disseminated to intelligence analysts via normal message traffic and intelligence reports. The FBI shared information via their Joint Terrorism Task Forces and via phone or secured fax. To be realistic, existing channels were used to share information and care was taken to not commingle notional intelligence with real intelligence.[193] The information was delivered in small pieces along with the actual daily information processed by agencies.[194]

---

[191] U.S. Department of Homeland Security - Press Release, "Transcript of Press Conference with Secretary of Homeland Security Michael Chertoff on the TOPOFF 3 Exercise" (Washington, D.C., April 4, 2005), 2.

[192] DHS, "A Review of the T3 Exercise," 44.

[193] Ibid., 18.

[194] Al Pessin, "US Terrorism Exercise Test Prevention and Response," *Voice of America News*, April 8, 2005, http://www.voanews.come/english/archive/2005-04/2005-04-08-voa81.cfm?CFID=402571448&CFTOKEN=67519485. Accessed March 29, 2006.

The intelligence analysis led to "notionally successful search warrants and arrests being made prior to TOPOFF 3 deterring some of the possible attacks."[195] Some attacks were scripted to occur regardless to ensure a realistic foundation for the response portions of the full-scale exercises.

Most TOPOFF 3 after-action reports have not yet been published. The Department of Homeland Security's Inspector General, while not granted enough access to the intelligence part of play to make official recommendations, did note that the secured messaging system and information collection and reporting structure was not sufficient to process and track the large volumes of information.[196]

Several additional lessons learned were identified during TOPOFF 3. Due to the complexity of intelligence and information sharing system, all intelligence players should be clearly identified in advance (see previous section on the Information Sharing Environment Analysis). Designers should agree on a limited number of over-arching objectives that will apply to all agencies involved. In addition, team members must be flexible during the exercise design phase, understanding that prevention exercises are still a relatively new concept. Finally, planners found that it is important to have a strong personality as the lead exercise designer.

4. TOPOFF 4

TOPOFF 4 (T4), the next exercise in the TOPOFF series, is planned for October 2007. Few details have been released about T4, however, six states and territories applied to host the exercises and three locations have been selected to participate: Oregon, Arizona, and the U.S. Territory of Guam.[197] The exercises will last ten days and involve

---

[195] College of Continuing Studies, "TOPOFF 3 AAR Summary," 8.

[196] U.S. Department of Homeland Security, Office of Inspections and Special Reviews, "A Review of the Top Officials 3 Exercise – Management Response to Draft Report" (Washington, D.C., November 2005), 53.

[197] Andy Giegerich, "Portland Picked as Site for Terror Exercise," *The Business Journal of Portland*, March 7, 2005.

simultaneous attacks in each venue. Up to 20,000 emergency workers are anticipated to be involved and observers are expected from many countries including Russia and Denmark.[198]

As of June 2006, the planning for TOPOFF 4 has included a three-day Command Post Exercise hosted in Northern Virginia. This continuity of government-oriented exercise was held in conjunction with exercises by FEMA and the FBI and involved 4,000 participants.[199]

While prevention was an underlying theme for TOPOFF 3, it will become more of a primary focus in TOPOFF 4. The exercise will involve at least two significant prevention components, one each in Oregon and Guam. Intelligence play will begin 60 days before the exercise, twice as long as was played during T3. The Arizona portion of the exercise will be a response-oriented command post exercise (CPX).

From these examples, it is apparent that the difficult task of prevention, whether in training, exercising, or in the real world, is becoming increasingly important. Agencies facing this task should know that, while difficult, it is possible to conduct prevention exercises, or at least, to incorporate realistic prevention activities and scenarios into existing homeland security exercises.

---

[198] Mathew Benson, "Phoenix Balks on Terror Drill," *The Arizona Republic*, April 14, 2006.

[199] U.S. Department of Homeland Security - Office of the Press Secretary, "U.S. Department of Homeland Security Announces Completion of TOPOFF 4 Command Post Exercise To Address Counterterrorism Preparedness And Response Capabilities," U.S. Department of Homeland Security, June 22, 2006, http://www.dhs.gov/dhspublic/display?content=5701/. Accessed August 12, 2006.

IV. CONCLUSION

A good plan, well-rehearsed, is better than a perfect plan unrehearsed.[200]

General George S. Patton

The purpose of exercises are to test and validate relevant policies, plans, procedures, training, equipment, and interagency agreements. Additionally, exercises help clarify and train personal in their individual and agency roles and responsibilities, which contributes to improved interagency coordination and communication. This can also improve professional relationships on the individual level. An exercise can be a form a gap-analysis, identifying resources and equipment needs. Exercises can improve individual performance and identify areas for improvement. This allows jurisdictions to focus their planning efforts on the areas of greatest need. The value of using the HSEEP methodology, in addition to being a requirement for some types of funding, ensures nationwide consistency and useful after-action reports and improvement plans.

While recognizing the benefits of prevention-oriented activities, they do not come without cost. As mentioned earlier, the June 2005 New York State Pilot Prevention Exercise lasted for twenty-three days.[201] The dedication of this much time to an exercise is significant and the level of commitment required for a realistic prevention exercise may not be within the reach of every agency. Nevertheless, this fact does not reduce the importance of realistic exercising.

The most effective method in assessing the ability to accomplish an objective is to allow tasks to be performed in a realistic environment as though they would in the real world. The evolution of a threat picture in any given scenario might take place over days, weeks, or months. In order to exercise these types of tasks and capabilities, it is best to put them in an environment where intelligence collection and analysis run their natural

[200] Col Timothy G. Malone, Schaupp, Maj Reagan E, "The Red Team: Forging a Well-Conceived Contingency Plan," *Aerospace Power Journal* XVI, no. two (Summer 2002). 12. Note that Malone and Schaupp slightly modified the original quote.

[201] Al Pessin, "US Terrorism Exercise Tests Prevention and Response," *Voice of America News*, April 8, 2005, http://www.voanews.com/english/archive/2005-04/2005-04-08-voa81.cfm//. Accessed March 25, 2006.

life cycle. This allows the human aspect to play its role of deciding what is important, who to send information to, and when. Where a one day full-scale exercise might quantitatively exercise a capability to conduct mass decontamination, for example, there may now be a need to conduct a one month exercise to test whether a systematic approach to recognizing threat indicators (not always from law enforcement) are observed, reported and integrated into the continuous flow of information by many different systems.

While this may all make sense, the question arises about why it appears to be so difficult. The reasons are many. As stated earlier, response exercises are easier to plan and conduct than prevention exercises because we are good (for the most part), at response. It is done every day by every local and state response organization in existence. Response exercises are relatively easy to budget and can be 'seen' by those in positions to approve them. Response exercises typically look the same from agency to agency. Fire trucks, police cars, medic units and others show up at a predestinated location and do what they do nearly every day. Prevention activities have no such consistency. Agencies cannot simply look to their fellow agencies and do what they have done, as, often times, they also are looking for guidance. Prevention as a science and a practice is still in its infancy. Maturity will come, but only with research, analysis, and more practice.

This thesis strives to document and demonstrate that prevention can be exercised. It makes no claim that the task is easy, but the rewards are self-evident. Understanding that prevention can be practiced and exercised through the use of certain tools is one significant step in having the guidance necessary to begin a prevention exercise, or even better, a prevention exercise program. The tools cited, 'all-crimes', information sharing environment analysis, red teaming, attack trees, behavioral analysis, and inclusion of private sector security, can be used either individually or as a group to conduct exercises. These tools, however, are not the end-state, as other tools undoubtedly exist.

This thesis also endeavors to provide a road map for agencies desiring to understand and exercise prevention activities. It has attempted to do so by identifying obstacles to prevention exercising, providing prevention tools, and finally, by providing specific exercise examples. Agencies using the described, and perhaps other, tools,

working with the Homeland Exercise and Evaluation Program (HSEEP) Guidelines, using the technical expertise available from local, national, and federal subject-matter experts, and reviewing other research, should have that road map. Most importantly, on-going, realistic prevention-oriented exercises may result in actual improvements in society's ability to prevent terrorism. There is no loftier goal, or more compelling reason to test and exercise our best prevention efforts.

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Amenaza Technologies Limited. "Creating Secure Systems through Attack Tree Modeling." www.amenaza.com/downloads/docs/5StepAttackTree_WP.pdf. Accessed September 20, 2006.

Andrew, Ellison, Robert J. Moore, Richard C. Linger. "Attack Modeling for Information Security Survivability." Pittsburgh, PA: Carnegie Mellon University. March 2001.

ASIS Foundation. "Security Report: Scope and Emerging Trends." Arlington, VA: ASIS International. 2005.

ASIS International. "Private Security Officer Selection and Training." 2004.

Bach, Robert. "Transforming Border Security: Prevention First." *Homeland Security Affairs* 1, no. 1, Summer 2005.

Baird, Zoe, James Barksdale. "Mobilizing Information to Prevent Terrorism." New York City: Markle Foundation, 2006.

Bitzer, Edward. "Strategies for Cutting Turnover." *Security Management*, May 2006.

Brennan, Richard. *Protecting the Homeland*. Arlington, VA: RAND, 2002.

Bureau of Labor Statistics. "Security Guards and Gaming Surveillance Officers." *Occupational Outlook Handbook, 2004-2005 Edition*. 2004.

Center for Democracy and Technology. "Domestic Intelligence Agencies: The Mixed Record of the UK's MI-5." http://www.cdt.org/security/usapatriot/030127mi5.pdf. Accessed September 20, 2006.

Center for International Security & Cooperation, Institute for International Studies, Stanford University. "Final Report: Top Officials 2 Full Scale Exercise, May 11-15, 2003." 2003.

Colorado Department of Regulatory Agencies. "Private Security Companies and Private Security Guards." 2006.

Congressional Budget Office. "Homeland Security and the Private Sector." 2004.

Congressional Research Service. "Border and Transportation Security: Possible New Directions and Policy Options." Washington, D.C., March 2005.

Cooper, Jeffrey R. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis.* Washington, D.C.: Center for the Study of Intelligence, December 2005.

Council of State Governments. *The Impact of Terrorism on State Law Enforcement*. Washington, D.C.: Eastern Kentucky University, 2005.

Culpepper, Anna M. “Effectiveness of Using Red Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack.” Master's Thesis, Naval Postgraduate School, Monterey, CA, 2004.

Dailey, Thomas J. “Implementation of Office for Domestic Preparedness Guidelines for Homeland Security June 2003 Prevention and Deterrence.” Master's Thesis, Naval Postgraduate School, Monterey, CA, 2005.

Defense Science Board. “The Role and Status of DoD Red Teaming Activities.” Washington, D.C.: U.S. Department of Defense, September 2003.

Department of Justice, Federal Emergency Management Agency. “Top Officials (TOPOFF) 2000 Exercise Observation Report.” April 30, 2002.

Docobo, Jose M. “Community Policing as the Primary Prevention Strategy for Homeland Security at the Local Law Enforcement Level.” Master's Thesis, Naval Postgraduate School, Monterey, CA, 2005.

Ellison, Robert J. “Attack Trees.” Carnegie Mellon University. September 2005.

Federal Bureau of Investigation. “Integrated Automated Fingerprint Identification System Or IAFIS.” http://www.fbi.gov/hq/cjisd/iafis.htm. Accessed July 11, 2006.

Federal Bureau of Investigation: Counterterrorism Division. “Intelligence Bulletin: Drug Trafficking and International Terrorism.” November 16, 2005.

Fontenot, Colonel Gregory, U.S. Army, Retired. “Seeing Red: Creating a Red-Team Capability for the Blue Force.” *Military Review* (September-October 2005).

Ginsburg, Susan. *Countering Terrorist Mobility*. Washington, D.C.: Migration Policy Institute, February 2006.

Gotbaum, Betsy. “Undertrained, Underpaid, and Unprepared: Security Officers Report Deficient Safety Standards in Manhattan Office Buildings.” Public Advocate for the City of New York, 2005.

Hart, Peter D., Associates. “A Post-September 11 Report on Surveys of Security Officers in California, Texas, and Florida.” www.seiu.org/document.cfm?documentID=296. Accessed September 20, 2006.

Hetherington, Christopher John. “Private Security as an Essential Component of Homeland Security.” Master's Thesis, Naval Postgraduate School, Monterey, CA, 2004.

Holden, Gwen A. “Building a Homeland Security Strategy: State and Local Law Enforcement on the Line.” Washington, D.C.: University of Pennsylvania, 2003.

National Response Team. “Exercise TOPOFF 2000 and National Capital Region After-Action Report: Final Report.” August 2001.

New Jersey Domestic Security Preparedness Task Force. “2004/2005 Progress Report.” January 2006.

Horowitz, Craig. “The NYPD's War on Terror.” *New York Magazine*, February 3, 2003.

Indiana Data and Communications System. “IDACS 2000 Full Operator's Lesson Plan.” https://test.secure.in.gov/isp/idacs/training/. Accessed September 20, 2006.

Information Sharing Environment. “Program Manager Information Sharing Environment.” http://www.ise.gov/. Accessed August 7, 2006.

International Association of Chief of Police. “Private Security/Public Policing, Vital Issues and Policy Recommendations.” Washington, D.C.: IACP. 2005.

International Bureau for Narcotics, and Law Enforcement Affairs. International Narcotics Control Strategy Report. *Money Laundering and Financial Crimes*. Washington, D.C.: United States Department of State, 2006.

Kane, John and April Wall. *Identifying the Links between White-Collar Crime and Terrorism*. National White Collar Crime Center, 2004.

Kaplan, David E. “Homegrown Terrorists: How a Hezbollah Cell Made Millions in Sleepy Charlotte, N.C.” *U.S. News and World Report*, March 10, 2003.

Kind, LTG Peter A. Ret., J. Katherine Burton. “Information Sharing and Collaboration Business Plan.” Institute for Defense Analysis, 2005.

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

Krouse, William J. “Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6.” Congressional Research Service, 2004.

Lessons Learned Information Sharing. “Local Anti-Terrorism Information and Intelligence Sharing: Overview.” https://www.llis.dhs.gov/. Accessed September 20, 2006.

---. “Public-Private Partnerships for Emergency Preparedness: Education, Training, and Technical Assistance.” https://www.llis.dhs.gov/. Accessed September 20, 2006.

---. “Public-Private Partnerships for Emergency Preparedness: Information Sharing.” https://www.llis.dhs.gov/. Accessed September 20, 2006.

---. “Public-private Partnerships for Emergency Preparedness: Overview.” https://www.llis.dhs.gov/. Accessed September 20, 2006.

Leveson, Nancy. *A New Accident Model for Engineering Safer Systems*. Massachusetts Institute of Technology, April 2004.

Lewis, Ted. “Module 5 Learning Objectives.” Center for Homeland Defense and Security, Naval Postgraduate School, 2006. https://www.chds.us/courses/mod/resource/view.php?id=364/, Accessed July 16, 2006.

London Police, City of. “Project Griffin.” http://www.cityoflondon.police.uk/countering-terrorism/terrorism-griffin.html/. Accessed April 4, 2006.

Longshore, David N.M. “The Principles of Prevention and the Development of the Prevention Triangle Model for the Evaluation of Terrorism Prevention.” Master's Thesis, Naval Postgraduate School, Monterey, CA, 2005.

Los Angeles County Operational Area Exercise Program. “Operation Chimera 2005, Terrorism Early Warning Group Tabletop Exercise.” 2005.

Lynch, Michael D. “Developing a Scenario-Based Training Program.” *FBI Law Enforcement Bulletin*, October 2005: 4-8.

North American Electric Reliability Council. “Risk-Assessment Methodologies for Use in the Electric Utility Industry.” September 2005.

Malone, Col Timothy G., Maj Reagan E. Schaupp. “The “Red Team”: Forging a Well-Conceived Contingency Plan.” *Aerospace Power Journal* XVI, no. 2 (Summer 2002).

Masse, Todd. “Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States.” Washington, D.C.: Congressional Research Service, May 2003.

Markle Foundation Task Force. *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*. New York: Markle Foundation, 2002.

Mauw, Sjouke, Martijn Oostdijk. “Foundations of Attack Trees.” www.win.tue.nl/~sjouke/publications/papers/attacktrees.pdf. Accessed September 20, 2006.

Metzger, Jim. “Behavior Oriented Screening System.” SEPTA Transit Police, 2005.

Moore, Judy, John Whitley, Rick Craft. *Red Gaming in Support of the War on Terrorism: Sandia Red Game Report.* Albuquerque, NM: Sandia National Laboratories, January 2004.

Murray, Williamson. *Red Teaming: Its Contributions to Past Military Effectiveness*. McClean, VA: Hicks and Associates, September 2002.

Murray, Williamson. *Thoughts on Red Teaming*. McClean, VA: Hicks and Associates, May 2003.

National Commission on Terrorist Attacks upon the United States (9-11 Commission). *Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: Norton & Co., 2004.

New Mexico Tech. "Prevention and Response to Suicide Bombing Incidents Course Manual." Socorro, N.M., 2005.

Pallos, Michael S. "Attack Trees: It's Jungle Out There." *Business Forum*, 2003.

Parfomak, Paul W. "Guarding America: Security Guards and U.S. Critical Infrastructure Protection." Congressional Research Service, 2004.

Pessin, Al. "US Terrorism Exercise Test Prevention and Response." *Voice of America News*, April 8, 2005. http://www.voanews.come/english/archive/2005-04/2005-04-08-voa81.cfm?CFID=402571448&CFTOKEN=67519485. Accessed March 29, 2006.

Police Executive Research Forum. *Protecting Your Community from Terrorism: Strategies for Local Law Enforcement. Vol. 5, Partnerships to Promote Homeland Security.* Washington, D.C., 2002.

Riley, K. Jack, Gregory F. Trevorton, Jeremy M. Wilson, Lois M. Davis. *State and Local Intelligence in the War on Terrorism.* Santa Monica: RAND, 2005.

Russack, John A. "Preliminary Report on the Creation of the Information Sharing Environment." http://www.ise.gov/. Accessed September 20, 2006.

---. "Information Sharing Environment Interim Implementation Plan." http://www.ise.gov/. Accessed September 20, 2006.

Said, Carolyn. "Security Lapse: Private Guards Get Little Training and Low Pay, Study Says." *San Francisco Chronicle*, June 11, 2002.

Schneier, Bruce. "Attack Trees." www.schneier.com/paper-attacktrees-ddj-ft.html. Accessed September 20, 2006.

Security Magazine. “Security's Top Guarding Companies.” http://www.securitymagazine.com/. Accessed September 20, 2006.

Security Management. “Training in Israel for Terrorism in the U.S.” Arlington, VA: ASIS International. November 2005.

Select Committee on Homeland Security - U.S. House of Representatives. “Statement of C. Suzanne Mencer.” July 8, 2004.

Service Employees International. “About The Industry.” January 2006. http://www.seiu.org/property/security/about_industry/index.cfm/. Accessed April 13, 2006.

Shelley, Louise, John Picarelli, Allison Irby, Douglas Hart, Patricia Craig-Hart, Phil Williams, Steven Simon, Nabi Abdullaev, Bartosz Stanislawski, Laura Covill. *Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism*. U.S. Department of Justice, 2005.

Simeone, Matthew J. “The Power of Public-Private Partnerships: P3 Networks in Policing.” *National Academy Associates*, January/February 2006.

Skroch, Michael J. *Red Team Assessments as a CIP Tool for First Responder Preparedness & Training.* Albuquerque, NM: Sandia National Laboratories, August 2005. PowerPoint Presentation.

Spiller, Suzel. “The FBI’s Field Intelligence Groups and Police: Joining Forces.” *FBI Law Enforcement Bulletin*. May 2006.

Stevermer, CAPT Andy. *TOPOFF 2: Lessons Learned*. Presentation, Seattle, WA, August 2003. http://depts.washington.edu/nwcphp/siphp2003/summerinst.html)/. Accessed August 12, 2006.

Sullivan, John P. “Terrorism Early Warning and Co-Production of Counterterrorism Intelligence.” Canadian Association for Security and Intelligence Studies, October 2005.

TOPOFF Exercise Planning Conference Final Report. May 21 1999. PDF, http://www.gnyha.org/eprc/general/nbc/chemical/200202_ChemGuidebook.pdf. Accessed August 12, 2006.

Tucker, Jonathon B. “Strategies for Countering Terrorism: Lessons from the Israeli Experience.” *Homeland Security Journal*, March 2003.

U.S. Army Training and Doctrine Command (TRADOC). *Terror Operations: Case Studies in Terrorism*. Fort Leavenworth, KS, August 2005.

U.S. Bureau of Labor Statistics. *Occupational Outlook Handbook (OOH), 2006-07 Edition.* Washington, D.C.: Government Printing Office, 2004.

U.S. Congress. "Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001." 2002.

U.S. Department of Homeland Security. *Guidelines for Homeland Security, Prevention and Deterrence*. Washington, D.C., 2003.

---. *Homeland Security Exercise and Evaluation Guide. Volume I: Overview and Doctrine*. Washington, D.C., 2004.

---. *Homeland Security Exercise and Evaluation Guide. Volume V: Prevention and Deterrence Exercises*. Washington, D.C., 2005.

---. *Homeland Security Exercise and Evaluation Program*. August 2005.

---. *Prevention Exercise Training Course: Participant Handbook*. Washington, D.C., March 2006.

---. *Target Capabilities List, Draft Version two*. Washington, D.C., 2005.

---, Office of Inspections and Special Reviews. *A Review of the Top Officials 3 Exercise – Management Response to Draft Report.* November 2005.

---, Prevention and Deterrence Exercise Support Team. *Pilot Exercise Internal AAR and IP*. U.S. Department of Homeland Security, 2005.

---, U.S. Department of Justice. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New World*. 2005.

U.S. Office of Homeland Security. *National Strategy for Homeland Security*. Washington, D.C., 2002.

U.S. House Committee on Homeland Security Democratic Staff. *Beyond Connecting the Dots: A VITAL Framework for Sharing Law Enforcement Intelligence Information.* 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Brady K. O'Hanlon
   U.S. Department of Homeland Security
   Washington, D.C.

4. Jonathan Cleck
   US Department of Homeland Security
   Washington, D.C.

5. Joe Autera
   Debonair Inc.
   Woodbridge, NJ

6. Robin "Butch" Colvin
   U.S. Department of Homeland Security
   Washington, D.C.

7. J. Steven Tidwell
   Federal Bureau of Investigation
   Los Angeles, CA

8. Lt. John Sullivan
   Terrorism Early Warning Group
   Monterey Park, CA

9. Col. Gregory Fontenot, U.S. Army, Retired
   University of Foreign Military and Cultural Studies
   Fort Leavenworth, KS

10. Under Secretary for Preparedness
    Department of Homeland Security
    Washington, DC

11. Director
Homeland Security Institute
Arlington, VA

12. Special Assistant
Homeland Security Institute
Arlington, VA

13. President
National Governors Association
Washington, DC

14. Senior Policy Analyst
Center for Best Practices, National Governors Association
Washington, DC

15. Research Assistant
Center for Strategic and International Studies
Washington, DC

16. Director
Homeland Security Policy Institute, George Washington University
Washington, DC

17. Director
Integrative Center for Homeland Security, Texas A&M
College Station, TX

18. Vice President
RAND
National Security Research Division
Santa Monica, CA