All Hazards Risk Assessment of Critical Transportation Infrastructure in the State of Tennessee

A.B. Rollins
Department of Civil and Chemical Engineering
School of Engineering and Computer Science
The University of Tennessee at Chattanooga

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
RES2013-27		

4. Title and Subtitle	5. Report Date
All Hazards Risk Assessment of Critical Transportation Infrastructure in the State of Tennesse: Part 1 Identification of the Top Ten Critical Transportation Assets	January 2015
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Rollins, A. Brent (UTC)	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
The University of Tennessee at Chattanooga Department of Civil and Chemical Engineering 615 McCallie Ave EMCS Building, Dept. 2502 Chattanooga, TN 37403	11. Contract or Grant No. EG1438330 (Contract No.)

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Tennessee Department of Transportation James K. Polk Building 505 Deaderick Street, Suite 900 Nashville, TN 37243	Final Report August 2013 to December 2014
	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Threats, both natural and man-made, exist to critical infrastructure of all types throughout the nation. Currently operating terrorist groups have indicated their intention to attack critical transportation infrastructure in the future. The possibility of terrorism against our nation's bridges is an ever-increasing threat today. Globally, between 1980 and 2006, 53 terrorist attacks specifically targeted bridges. Approximately 60% of these attacks were bombings [1]. There is general agreement that the threat of terrorist attack to the transportation sector is growing; "…there is a growing concern that within this sea of moving parts lay critical security gaps and a lack of operational resiliency that could cause tremendous damage from any significant disruptive event, whether man-made or natural." [2] Perhaps most disturbing is the recent report that an anonymous caller informed the FBI of a plot by ISIS to blow up a Memphis bridge [3].

A significant amount of work has been done since 9/11 to prepare critical transportation infrastructure for the eventuality of a terrorist attack. The overriding government publication from the Federal level is the National Infrastructure Protection Plan (NIPP), with the Transportation Sector-Specific Plan annex. Among the suggested methods to approach risk assessment is the RAMCAP process that involves using the worst-case scenario of a potential threat. The terrorist threat meets that criteria and has the distinction of being the threat vector that can be mitigated against most easily by adjustments in Department policies and designs.

The analysis relied on a survey to identify the top ten critical transportation assets in Tennessee that were then subjected to the RAMCAP risk management process. Site visits were made to assess vulnerability, and extensive research was conducted to evaluate potential threats and consequences of the losses. In general, the vulnerabilities found present in many of the assets primarily were concerned with unrestricted or lightly restricted access to the under-deck columns and abutments. Many threats were considered, with natural and man-made accidental being set aside due to their consideration in design of the bridges. The man-made intentional, or terrorist threat, was then decided to be the primary threat package.

17. Key Words	18. Distribution Statement
Risk Assessment **Critical Transportation Infrastructure** **Man-Made Hazards** **Terrorist Threat**	Report intended for the Tennessee Department of Transportation or their designees. No distribution without the written consent of the Tennessee Department of Transportation.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	70	$67,944.47

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

DISCLAIMER

This research was funded through the State Planning and Research (SPR) Program by the Tennessee Department of Transportation and the Federal Highway Administration under RES2013-27 *All Hazards Risk Assessment of Critical Transportation Infrastructure in the State of Tennessee*.

Contents

Executive Summary

Transportation infrastructure is critical for the continued operation and economic well-being of the State of Tennessee. Threats, both natural and man-made, exist to critical infrastructure of all types throughout the nation. Historically, transportation infrastructure has been a target of terrorist attacks. Currently operating terrorist groups have indicated their intention to attack critical transportation infrastructure in the future. The possibility of terrorism against our nation's bridges is an ever-increasing threat in today's society. Globally, between 1980 and 2006, 53 terrorist attacks specifically targeted bridges. Approximately 60% of these attacks were bombings [1]. There is general agreement that the threat of terrorist attack to the transportation sector is growing; "…there is a growing concern that within this sea of moving parts lay critical security gaps and a lack of operational resiliency that could cause tremendous damage from any significant disruptive event, whether man-made or natural." [2] Perhaps most disturbing is the recent report that an anonymous caller informed the FBI of a plot by ISIS to blow up a Memphis bridge [3].

There are 19,519 bridges in Tennessee, of which 8,113 are maintained by the Tennessee Department of Transportation (TDOT) [9]. These bridges represent various designs, sizes, level of historical significance, Average Daily Traffic (ADT), and vulnerability. Bridges are attractive targets of terrorists, offering a "concentrated point of attack" in which a disruption could offer a spectacular impact to freedom of movement and the economy.

A significant amount of work has been done since 9/11 to prepare critical transportation infrastructure for the eventuality of a terrorist attack. The overriding government publication from the Federal level is the National Infrastructure Protection Plan (NIPP), with the Transportation Sector-Specific Plan annex. Among the suggested methods to approach risk assessment is the RAMCAP process. The RAMCAP process is a systematic, probabilistic approach to inform levels of threat, vulnerability, and consequence, ultimately leading to a calculation of overall risk. Risk Assessment can be generalized with the following equation:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequences}$$

The analysis relied on a survey to identify the top ten critical transportation assets in Tennessee that were then subjected to the RAMCAP risk management process. Site visits were made to assess the assets' vulnerability, and extensive research was conducted to evaluate potential threats and consequences of the loss of the assets.

In general, the vulnerabilities found present in many of the assets primarily were concerned with unrestricted or lightly restricted access to the under-deck columns and abutments. Many threats

were considered, with natural and man-made accidental being set aside due to their consideration in design of the bridges. The man-made intentional, or terrorist threat was then decided to be the primary threat package that affected the assets' risk equation. The RAMCAP process involves using the worst case scenario of a likely threat; the terrorist threat meets that criteria as well as the distinction of being the threat vector that can be mitigated against most easily by adjustments in Department policies and designs.

Of the sources of terrorist attack considered, it was determined that an active shooter or explosive attack by home-grown al-Qaeda/ISIS sympathizers is the most likely Potential Threat Element (PTE). Domestic-issue groups were also considered, but found not to be as likely a threat.

A wealth of information on blast resistant bridge design has been published, but increasing standoff distance from bridge columns and abutments to vehicle access remains the most effective means of defending against a terrorist attack on bridges. Some consideration to limiting access to small-arms fire was also discussed. Recent well-publicized terrorist threats to bridges in the State have called attention to the need to be prepared for the unfortunate eventuality of a terrorist attack. This risk assessment project is not the end of that process. Rather, it is the beginning of the work to be done to ensure that the critical transportation infrastructure in the State of Tennessee and those people that watch over its well-being are prepared.

Introduction

Transportation infrastructure is critical for the continued operation and economic well-being of the State of Tennessee. Threats, both natural and man-made, exist to critical infrastructure of all types throughout the nation. Historically, transportation infrastructure has been a target of terrorist attacks. Currently operating terrorist groups have indicated their intention to attack critical transportation infrastructure in the future. The possibility of terrorism against our nation's bridges is an ever-increasing threat in today's society. Globally, between 1980 and 2006, 53 terrorist attacks specifically targeted bridges. Approximately 60% of these attacks were bombings [1]. There is general agreement that the threat of terrorist attack to the transportation sector is growing; "…there is a growing concern that within this sea of moving parts lay critical security gaps and a lack of operational resiliency that could cause tremendous damage from any significant disruptive event, whether man-made or natural." [2] Perhaps most disturbing is the recent report that an anonymous caller informed the FBI of a plot by ISIS to blow up a Memphis bridge [3]. The need to identify the transportation assets that are most critical to the State, to evaluate the threats to those assets, and to identify the consequences of their disruption has never been more pressing. Ritter, et. al. describe this pressing need succinctly:

> Although portions of the global transportation network have been heavily scrutinized since the terrorist attacks of 9/11 and a host of government and regulatory measures have been enacted, the fact remains that nearly all experts and analysts agree that the global transportation system remains vulnerable to a significant terrorist event, with many fearing that such an event is likely to have a devastating and lasting effect upon the entire system of global trade.

As a starting point, the Tennessee Department of Transportation decided to perform All Hazards Risk Assessments on the top ten critical transportation assets in the State. The All Hazards approach to risk assessment takes all potential hazards into account when assessing an asset's risk, and is a well-documented approach detailed in the National Infrastructure Protection Plan (NIPP) as well as in U.S. Department of Homeland Security risk assessment procedures. This represents a first step in securing Tennessee's portion of the global transportation network. Because design, inspection, and maintenance of bridges procedures are typically mandated by code for interactions with natural hazards (earthquake, flood, etc.), this study focuses primarily on man-made accidental and man-made intentional (terrorist) threats.

The National Infrastructure Protection Plan (NIPP)

The NIPP was established and refined by Presidential directives to serve as the overarching guidance for infrastructure protection efforts in the United States. The NIPP represents a collaborative effort across government and private sector partners to "identify national priorities; articulate clear goals; mitigate risk; measure progress; and adapt based on feedback and the changing environment." [4] Below are the Vision, Mission, and Goals of the NIPP:

Vision

A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.

Mission

Strengthen the security and resilience of the Nation's critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community.

Goals

- Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services;
- Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
- Promote learning and adaptation during and after exercises and incidents.

As part of the latest revision specified by Presidential Policy Directive (PPD) 21, a federal agency, known as a Sector-Specific Agency (SSA), was established to lead a collaborative process for critical infrastructure security within each of the 16 critical infrastructure sectors. Each Sector-Specific Agency is responsible for developing and implementing a sector-specific plan (SSP), which details the application of the NIPP concepts to the unique characteristics and conditions of their sector. As one of the 16 critical infrastructure sectors, an annex to the NIPP was produced, *The Transportation Sector-Specific Plan*, in 2010. This document is currently being reviewed for updating to the NIPP 2013. However, it is useful to consider the 2010 Transportation SSP to inform the process of all-hazards risk assessment for critical transportation infrastructure in Tennessee. The vision and mission statements for the Transportation SSP 2010 are below [5]:

Vision Statement for the Transportation Systems Sector

Our vision is a secure and resilient transportation network, enabling legitimate travelers and goods to move without undue fear of harm or significant disruption of commerce and civil liberties.

Mission Statement for the Transportation Systems Sector

Continuously improve the risk posture of the Nation's transportation system.

All Hazards Risk Assessment of Critical Transportation Assets in Tennessee represents an effort to accomplish the goals of the NIPP at the State level for the Transportation Systems SSP. It is important to realize that this risk assessment process is not a terminal goal; rather, the risk assessment process is a closed-loop system that requires continual analysis and updating. The process serves as a tool to prioritize asset risk exposure based on analysis of threats, vulnerabilities, and consequences. This project represents a portion of a much broader process to improve our risk footing in the nation across all sectors. Figure 1 below is a graphical representation of the broader process of the integrated top-down and bottom-up risk assessment cycle.

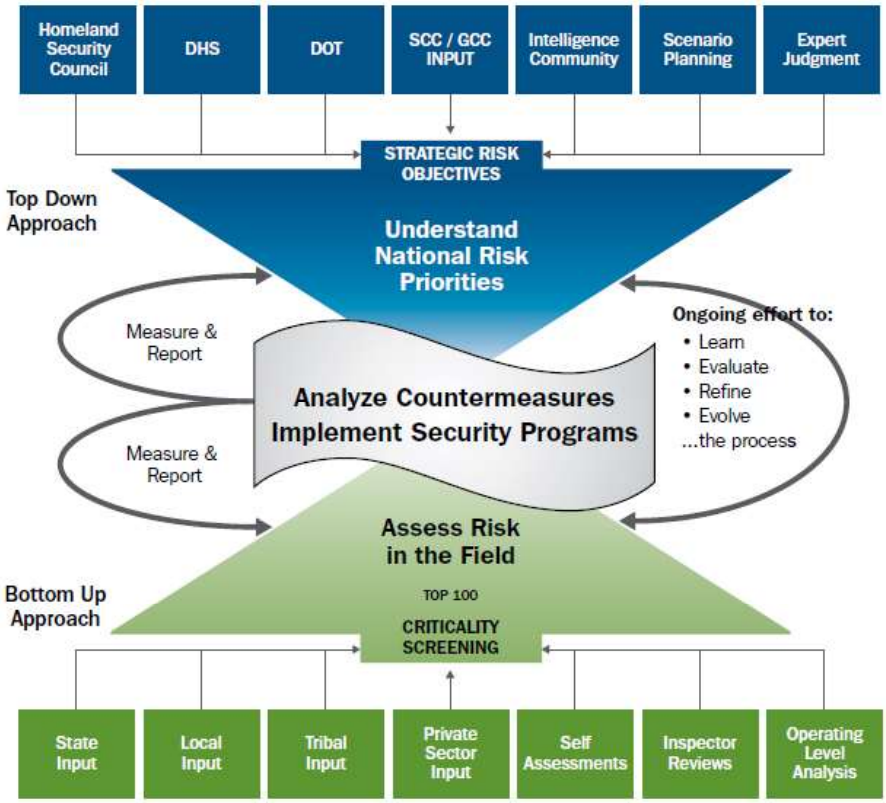


Figure 1: Integrated Top-Down, Bottom-Up Risk Assessment Cycle [6]

General Overview of Risk Environment in the Transportation Sector

A transportation network can be considered from the viewpoint of a system or individual assets. The system approach involves a collection of transportation assets, the relationships among them, the policies, rules, and regulations that support them, and the processes involved [6]. Risk assessments of transportation assets must, by nature, consider at least some level of system-wide interaction , especially in the criticality determination phase early in the process and the consequence phase later. Although the risk assessment process must focus on individual assets, it is important to recognize that the Nation's transportation network has at its core and interconnectedness across transportation modes (aviation, maritime, mass transit, highway, freight rail, pipeline) as well as across sectors. Virtually every sector defined by the NIPP has key dependencies on the transportation sector; most rely on transportation networks to deliver raw materials, products, and employees to their destinations in a reliable, consistent manner. When disruptions to the transportation sector occur, potentially every business, critical infrastructure sector and key resource can be impacted negatively.

According to the University of Tennessee's Center for Business and Economic Research [7], half of the transportation demand within the State occupies only about 11 percent of the land area. This represents a concentration of transportation demands in metro areas that is a challenge exacerbated by the existence of transportation network junction points. These junction points, if

affected by an event, will affect the movement of not only state-originating travelers and freight, but also travelers and freight that do not originate or terminate in the State. Tennessee's roadways are an important cog in the national transportation network.

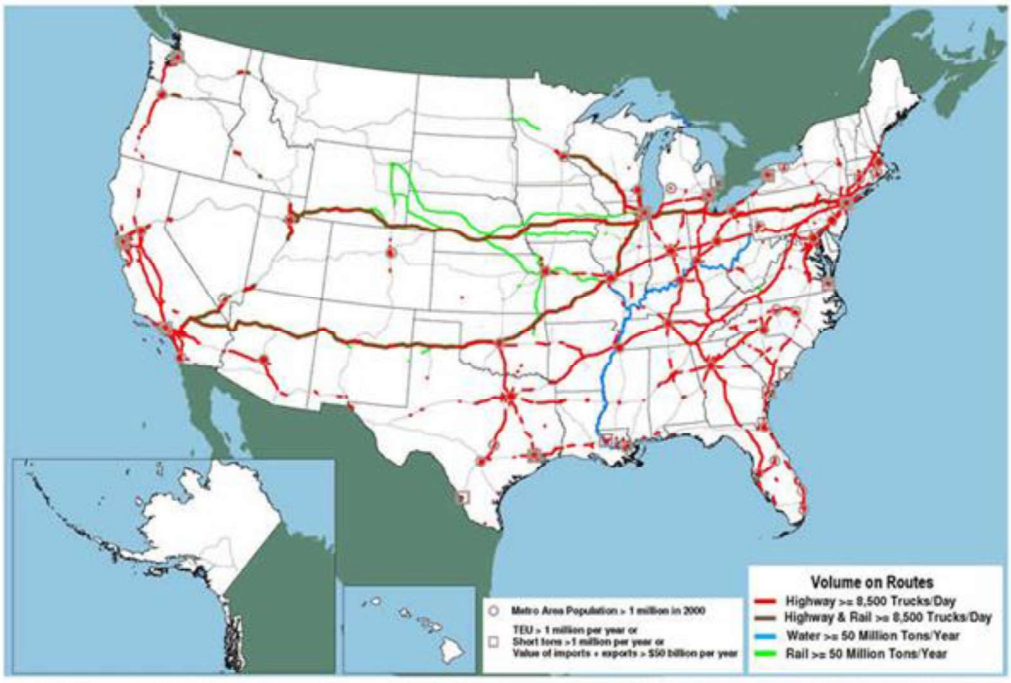


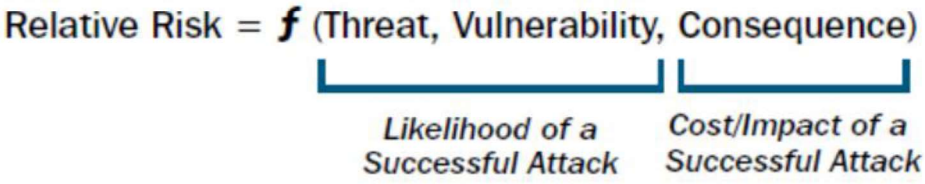
Figure 2: Tennessee's position in the national transportation network [8]

There are 19,519 bridges in Tennessee, of which 8,113 are maintained by the Tennessee Department of Transportation (TDOT) [9]. These bridges represent various designs, sizes, level of historical significance, Average Daily Traffic (ADT), and vulnerability. Bridges are attractive targets of terrorists, offering a "concentrated point of attack" in which a disruption could offer a spectacular impact to freedom of movement and the economy. Al-Qaeda operatives are instructed to destroy bridges leading into and out of cities as one of their military missions [1]. The risk environment of the Transportation Systems Sector is a "dynamic landscape of potential natural disasters, accidents, and terrorist attacks." [6] Natural disasters and accidents can be relatively easily planned for, as transportation systems designers can rely confidently on historical data to inform their decision making processes. However, terrorism presents the unique challenge of a hazard that changes tactics depending on previous responses. Add to that the fact that the transportation system continually grows and changes, and it can be seen that the task of ensuring the safety and security of the transportation system must also be adaptable. Ultimately, the risk analysis process will produce countermeasures options to improve the transportation systems sector's risk footing. The process used for decision making should therefore be sound, drawing on the experience of experts and creative thinking of analysts.

Overview of the Risk Management Process (the RAMCAP process)

The process chosen for the All Hazards Risk Assessment of Critical Transportation Infrastructure in the State of Tennessee is the Risk Analysis and Management for Critical Asset Protection

(RAMCAP). RAMCAP was developed "to facilitate the analysis and management of risk and resilience of critical facilities and infrastructures." [10] RAMCAP is based on the definition that risk is the anticipated consequence value of specific terrorist attacks and natural events weighted by the likelihood that the event could happen. The likelihood variable is modified both by the vulnerability of the asset and threat. This is the definition of risk used by the U.S. Department of Homeland Security.



A quantitative method that estimates numeric values of risk, RAMCAP fundamentally relies on Bayesian probability driven by expert analysis of threats, vulnerabilities, and consequences to calculate relative risk. The method uses terminology consistent across Federal homeland security and counterterrorism platforms (including the NIPP and DHS), and can therefore be used to compare assets nationally. RAMCAP was developed by the American Society of Mechanical Engineers (ASME) at the request of President George W. Bush after the attacks of 9/11. ASME has many years' experience with risk assessment analysis, and assembled a team of around one hundred experts to tackle the issue.

The RAMCAP process is divided into seven (7) analytical steps:

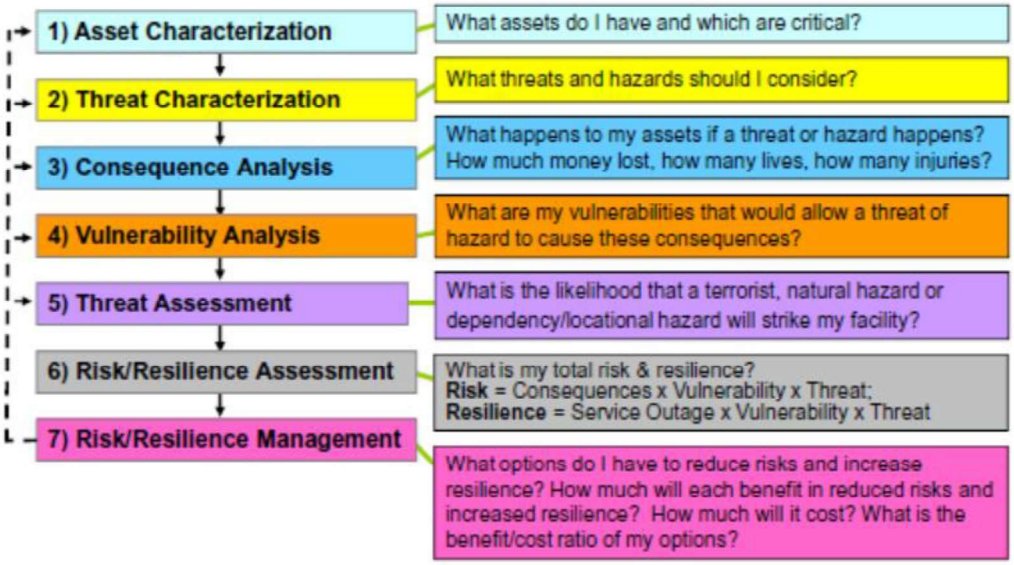


Figure 3: The seven analytical steps of the RAMCAP process [10]

1. Asset Characterization – defining which facilities and assets are critical to the

performance of the mission or function of the organization. In the case of this project, the asset characterization phase also involved determinations of which assets to study. In other words, before the project could begin, *where* to begin had to be figured out.

2. Threat Characterization – defining what specific threats to consider for each asset.
3. Consequence Analysis – estimating the worst reasonable outcomes of each threat to each asset.
4. Vulnerability Analysis – estimating the probability that each attack on each asset will result in the estimated consequences, given that the event occurs and considering the effectiveness of existing security measures.
5. Threat Assessment – estimating the probability or likelihood that the initiating event will Occur.
6. Risk and Resilience Assessment – estimating the risk and resilience associated with each event on each asset.
7. Risk and Resilience Management – evaluating risk-reduction and resilience enhancement options for their value (usually benefit-cost) and selecting, implementing and managing those that are selected.

Asset Characterization

The first step in the process of evaluating critical transportation infrastructure in the State was to first identify the top ten assets. The process used to identify these assets for further study was a web-based survey.

Identification of Survey Recipients

It was decided to include Tennessee Department of Transportation (TDOT) personnel as well as non-TDOT personnel in the survey in consideration of the desire to ensure that the survey met the needs of the State instead of TDOT alone. Web-based research was performed to identify key TDOT and non-TDOT personnel. The survey was sent to forty seven (47) TDOT employees, ninety four (94) county emergency managers/directors, and twenty one (21) other state and municipal employees chosen from the ranks of the Tennessee Emergency Management Agency (TEMA), the Tennessee Department of Safety and Homeland Security, the Tennessee Department of General Services, and city and town governments. Please see Appendix A for a complete listing (by name) of survey recipients.

Pre-Qualification of Assets

National Bridge Inventory (NBI) data was collected from Uglybridges.com for the top 500 Average Daily Traffic (ADT) count bridges and tunnels in the State (see Appendix B for a complete listing). In addition, an examination of historic significance and lack of alternates was performed, utilizing information from Bridgehunter.com. In addition, several assets were mentioned by team members in the project kick-off meeting on September 16, 2013. A preliminary screening of the top eighty five (85) assets was performed, taking into account ADT,

historical significance, and lack of alternates. From that screening, twenty eight (28) assets were identified for inclusion in the survey.

Survey Construction

The web-based survey was constructed using Qualtrics, an online survey company under contract with the University of Tennessee system. The twenty eight (28) assets were listed along with aerial photos obtained from Google maps. Recipients were asked to rank the assets on a scale of 1 to 10, with 10 being the most critical. A copy of the survey is presented in Appendix C. The order of the questions was randomized to alleviate bias.

Survey Results

On-line survey responses typically average around eleven percent of those polled. This survey produced significantly higher response rates:

- TDOT: 34.0%
- County EMA Directors: 17.0%
- Other: 14.3%

Eleven responses were received that had no information entered. These surveys were not included in calculations.

The top ten assets, as determined by TDOT recipients were (with average ranking):

1. Desoto Mississippi River Bridge (8.79)
2. Memphis Airport (8.71)
3. Nashville Airport (8.32)
4. I-24 Bridge over Cumberland River (7.79)
5. I-440/I-240 Interchange (7.25)
6. I-440/I-65 Interchange (7.10)
7. Port of Memphis (7.00)
8. Olgiati Bridge (6.94)
9. I-65 Bridge over Cumberland River (6.78)
10. I-75/I-40 Bridge over Papermill (6.73)

The top ten assets, as determined by County EMA and "other" recipients were (with average ranking):

1. Port of Memphis (7.44)
2. Desoto Mississippi River Bridge (7.41)
3. Memphis Airport (7.22)
4. I-440/I-65 Interchange (7.00)
5. Nashville Airport (6.78)
6. I-24 Bridge over Cumberland River (6.50)
7. Campbell County Slope Failure (6.25)
8. I-65 Bridge over Cumberland River (6.12)
9. I-440/I-240 Interchange (6.00)
10. I-440/I-24 Interchange (6.00)

In general, the two groups showed good agreement, with only two assets differing from each list. The TDOT respondents averaged about a half a point higher than the non-TDOT respondents when rating the assets' criticality. Combined, the asset rankings were:

1. Desoto Mississippi River Bridge (8.01)
2. Memphis Airport (7.88)
3. Nashville Airport (7.48)
4. Port of Memphis (7.26)
5. I-24 Bridge over Cumberland River (7.08)
6. I-440/I-65 Interchange (7.05)
7. I-440/I-240 Interchange (6.52)
8. I-65 Bridge over Cumberland River (6.42)
9. Olgiati Bridge (6.18)
10. I-24/I-65 Bridge over W. Trinity (6.17)
11. I-440/I-24 Interchange (6.10)
12. I-75/I-40 Bridge over Papermill (5.99)
13. Campbell County Slope Failure (5.88)
14. I-40 Slide Area in Roane County (5.81)
15. I-40 Bridges over Hwy 41 and 2nd Ave (5.78)
16. Chattanooga Airport (5.74)
17. Harding Place Bridge over I-65 (5.73)
18. Oak Ridge Hwy Bridge over Clinch River (5.66)
19. I-75/I-40 over Hollywood (5.65)

20. Knoxville Airport (5.61)
21. Briley Parkway bridge over I-24 (5.60)
22. I-24/I-40 over Fairfield (5.47)
23. Thompson Lane over I-65 (5.44)
24. Hwy 11/64 Rock Slide (5.43)
25. Fesslers over I-40/I-24 (5.40)
26. TDOT HQ (5.39)
27. Henley St. Bridge (5.38)
28. Pelissippi over I-75/I-40 (5.17)

Survey Analysis:

Because three of the top ten identified assets lie outside clear TDOT jurisdiction (Memphis Airport, Nashville Airport, Port of Memphis), the decision was made by the project team to replace those assets with the number 11, 12, and 13 assets respectively. This decision was made in a meeting at TDOT Headquarters on 3-18-14.

Survey Conclusions:

After adjusting for jurisdictional responsibility, the top ten assets to be studied further in the All Hazards Risk Assessment framework are:

1. Hernando Desoto Mississippi River Bridge (Shelby Co., TN)
2. I-24 Bridge over Cumberland River (Davidson Co., TN)
3. I-440/I-65 Interchange (Davidson Co., TN)
4. I-40/I-240 Interchange (Shelby Co., TN)
5. I-65 Bridge over Cumberland River (Davidson Co., TN)
6. P.R. Olgiati Bridge (Hamilton Co., TN)
7. I-24/I-65 Bridge over W. Trinity Lane (Davidson Co., TN)
8. I-440/I-24 Interchange (Davidson Co., TN)
9. I-75/I-40 Bridge over Papermill (Knox Co., TN)
10. I-75 Slope Failure (Campbell Co., TN)

Figure 4: Locations of Assets Identified for Study

Asset Details

The assets identified for study consist of nine (9) bridges and one (1) section of interstate highway. The nine bridges are within metropolitan areas, with one (1) in Chattanooga, one (1) in Knoxville, two (2) in Memphis, and five (5) in Nashville. Although considered stand-alone assets, three of the subjects of study are actually multiple bridge structures at interstate interchanges. The section of interstate highway identified is in mostly rural Campbell County.

Asset	ADT Primary	ADT Secondary	Total ADT
1. Hernando Desoto Mississippi River Bridge (Shelby Co., TN)	54,760	---	54,760
2. I-24 Bridge over Cumberland River (Davidson Co., TN)	139,540	---	139,540
3. I-40/I-440 Interchange (Davidson Co., TN)	162,069	107,065	269,134
4. I-40/I-240 Interchange (Shelby Co., TN)	148,100	96,990	245,090
5. I-65 Bridge over Cumberland River (Davidson Co., TN)	95,822	---	95,822
6. P.R. Olgiati Bridge (Hamilton Co., TN)	78,858	---	78,858
7. I-24/I-65 Bridge over W. Trinity Lane (Davidson Co., TN)	161,637	25,710	187,347
8. I-440/I-24 Interchange (Davidson Co., TN)	166,744	101,291	268,035
9. I-75/I-40 Bridge over Papermill (Knox Co., TN)	178,238	28,753	206,991
10. I-75 Slope Failure (Campbell Co., TN)	32,157	---	32,157

Table 1: Average Daily Traffic (ADT) values of the assets studied (Tennessee Department of Transportation, n.d.)

As can be observed in table 1 above from the lack of a secondary ADT, four (4) of the bridges cross bodies of water, ant the I-75 slope failure area only concerns that route directly. Before the real all hazards risk assessment begins, TEEX suggests that a "Geo Analysis" is done, a determination of the population density, transportation modes, chemical and manufacturing plants, and emergency response units within a one-mile radius of the site.

Threat Characterization

The threat characterization step in the RAMCAP process is used to identify potential threat scenarios in enough detail to estimate vulnerability and consequences. Potential cascading consequences are typically not taken into account during this step, but proximity consequences - those occurring due to a geographic location near the asset may be. Below, in Figure 5 is a summary of the reference threat scenarios developed by DHS in conjunction with the RAMCAP developers [10]:

Attack Type	Tactic/Attack Description			
Marine	**M1** Small boat	**M2** Fast Boat	**M3** Barge	**M4** Deep draft shipping
Aircraft	**A1** Helicopter	**A2** Small Plane (Cessna)	**A3** Medium, Regional Jet	**A4** Large Plane Long-Flight Jet
Land-based vehicle	**V1** Car	**V2** Van	**V3** Mid-size Truck	**V4** Large Truck (18 Wheeler)
Assault Team	**AT1** 1 Assailant	**AT2** 2-4 Assailants	**AT3** 5-8 Assailants	**AT4** 9-16 Assailants
Sabotage	**S(PI)** Physical-Insider	**S(PU)** Physical-Outsider	**S(CI)** Cyber-Insider	**S(CU)** Cyber-Outsider
Product Contamination	**C(C)** Chemical	**C(R)** Radionuclide	**C(B)** Biotoxin	**C(P)** Pathogenic
	C(S) - Weaponization of sewer system			
Natural Hazards	**N(H)** Hurricanes	**N(E)** Earthquakes	**N(T)** Tornadoes	**N(F)** Floods
Dependency & Location Hazards	**D(U)** Loss of Utilities	**D(S)** Loss of Suppliers	**D(S)** Loss of Employees	**D(C)** Loss of Customers
	D(T) Loss of Transportation		**D(L)** Dangerous co-location with other targets	

Table 2: RAMCAP reference threat scenarios

The threats put forth in figure 5, above, are not asset-specific. Rather, they are benchmark (or reference) threats that span a range of all critical infrastructure sectors. Threat characterization involves more than the assumption that the specific threat is applied to the specific asset. Threat characterization requires that each threat scenario be considered as well as its maximum credible consequences. In other words, the threat is considered along with its worst reasonable case outcomes for each asset. A fundamental relationship that exists in this process is that, as the amount of resources needed by terrorists to perform the activity specified, the likelihood of that event goes up. The inverse also holds true; as the resources needed to accomplish a specific attack go up, the likelihood of that attack goes down. For the purposes of this study, the threats considered vary slightly from asset to asset, but in general include the threats noted in table 3 below.

	= Not considered for this assessment
	= Considered as an accidental or intentional release on/near bridge
	= Suspected to be asset-dependent (appropriate for some/not appropriate for others)
	=All assets expected to be evaluated in light of this threat

Attack Type	Tactic/Attack Description			
Marine	**M1** Small boat	**M2** Fast Boat	**M3** Barge	**M4** Deep draft shipping
Aircraft	**A1** Helicopter	**A2** Small Plane (Cessna)	**A3** Medium, Regional Jet	**A4** Large Plane Long-Flight Jet
Land-based vehicle	**V1** Car	**V2** Van	**V3** Mid-size Truck	**V4** Large Truck (18 Wheeler)
Assault Team	**AT1** 1 Assailant	**AT2** 2-4 Assailants	**AT3** 5-8 Assailants	**AT4** 9-16 Assailants
Sabotage	**S(PI)** Physical-Insider	**S(PU)** Physical-Outsider	**S(CI)** Cyber-Insider	**S(CU)** Cyber-Outsider
Product Contamination	**C(C)** Chemical	**C(R)** Radionuclide	**C(B)** Biotoxin	**C(P)** Pathogenic
	C(S) - Weaponization of sewer system			
Natural Hazards	**N(H)** Hurricanes	**N(E)** Earthquakes	**N(T)** Tornadoes	**N(F)** Floods
Dependency & Location Hazards	**D(U)** Loss of Utilities	**D(S)** Loss of Suppliers	**D(S)** Loss of Employees	**D(C)** Loss of Customers
	D(T) Loss of Transportation		**D(L)** Dangerous co-location with other targets	

Table 3: Threat matrix specific to this assessment

Hazards Considered

From the threat matrix above, the general threats below are considered in this assessment. Note that specific threat vectors are explained in more detail in the Threat Assessment section. Specifically, some hazards are considered in multiple contexts; for example, the vehicle scenarios (marine, air, and land) are considered in both man-made accidental and terrorist delivery of weapon contexts.

Acts of Nature

Acts of nature can have devastating effects on highways and bridges. The most commonly encountered highway and bridge failures related to natural disasters are from earthquakes and flood damage. Earthquakes can cause vertical and horizontal displacement, while flooding primarily affects bridges through scour at the abutments. However, bridge design, inspection, and maintenance requirements (in the form of state and federal codes) take precedence when considering the interaction between bridges and the forces of nature. This study assumes that each asset in question meets the codified standards of the specific geographic location and that the Tennessee Department of Transportation is aware of the risks and their level of risk tolerance surrounding these natural hazards.

Man-Made Accidental

Man-made accidental threats are just that; events caused by circumstances that are not intentional, but can still have tremendous consequences. Like natural disasters, past experience can often be used to prepare for and mitigate accidental events. However, there are instances that lack of proper preparations has caused the consequences of events to be greater than they might have been if countermeasures had been previously taken. Note that some of the threat descriptions detailed in the man-made intentional category that follows could also apply to accidental events as well, with the major difference being in the location of the event. In other words, a man-made accidental HAZMAT discharge would likely be above deck of a bridge, with the accompanying consequences that occur in that location. The following man-made accidental scenarios were considered:

1. Accidental vehicle impact
    a. M1 - Small boat
    b. M2 - Fast boat
    c. M3 - Barge
    d. M4 - Deep draft shipping
    e. A1 - Helicopter
    f. A2 - Small plane
    g. A3 - Mid-size jet
    h. A4 - Large jetliner
    i. V1 - Car
    j. V2 -Van
    k. V3 - Mid-Sized Truck
    l. V4 - Large Truck (18 wheeler)

2. Vehicle accident with HAZMAT discharge
    a. C(C) chemical agents
    b. C(B) biological agents
    c. C(R) radiological material
    d. explosive material
    e. flammable material

3. Accident from surroundings
    a. chemical release from adjacent business
    b. explosion from adjacent business
    c. fire from adjacent business

4. Deterioration/Inspection deficiencies
    a. failure from improperly inspected elements

Man-Made Intentional (Terrorist Act)

When terrorist threats are considered the identity of the person or groups that may initiate the attack is very important during the risk assessment process. The motivation of the Potential Threat Element (PTE), the history of the PTE regarding types of violent activity and previous targets, and whether the PTE has been demonstrated to have a presence in the general area of the asset are all important considerations. Typically, PTEs seek publicity for a cause, or monetary or political gain through their actions. Most of the time, these actions involve injuring or killing people, destroying or damaging assets, or stealing assets [11]. For this section, an attempt to characterize the threat vectors irrespective of the PTE is undertaken to inform the later vulnerability assessment process. The potential threat vectors considered are listed below:

1. Pedestrian/swimmer-placed explosives

Pedestrian/swimmer-placed explosives could be used to sever critical trusses or cables if strategically placed by someone with the required knowledge [12]. This threat is not considered as likely as a vehicle-borne explosive, but is still considered. The following threat scenarios were considered for delivery of pedestrian/swimmer-placed explosives in this study.

a. AT1 - 1 assailant
b. AT2 - 2-4 assailants
c. AT3 - 5-8 assailants
d. AT4 - 9-16 assailants

2. Vehicle-borne explosives

Vehicle-borne explosives are considered the primary threat to bridges [12]. Research by the National Cooperative Highway Research Program (NCHRP) addresses the threat of vehicle-borne explosives to bridges. The report discusses explosives in general, explaining that the detonation of a high explosive is a high-rate chemical reaction that produces a sudden release of energy that manifests itself as a shock wave. A shock wave is highly compressed air that radiates spherically away from the detonation source, creating an overpressure and a dynamic pressure. The study explains that fragment penetration from the explosive casing (the vehicle itself) is not typically a concern of vehicle-borne explosives when considered in the context of bridge structural capacity, but is still a casualty source for motorists and pedestrians.

The shock wave that radiates spherically from an explosion is known as the incident wave. The incident wave reflects off of any surfaces in its path. This reflection is known as the reflected wave. The reflected wave travels faster than the incident wave because the air in which it travels has already been heated and compressed. It is important to note that peak pressure decreases significantly with standoff distance (the distance from the blast to the bridge in question in this instance) [1]. The most common blast scaling relationship is described in the "cube-root scaling" or Hopkinson-Cranz scaling, shown below in equation 1. Figure 7, below, illustrates standoff distance.

$$Z = \frac{R}{W_{TNT}^{1/3}}$$

Eq. 1

Where Z = scaled standoff (ft./lb$^{1/3}$)
R = standoff, distance between center of blast source and target (ft.)
WTNT = charge weight of explosive (lb. equivalent TNT)

Because of the relationship between the incident wave and reflected waves, bridge columns and abutments are particularly vulnerable to an explosive device. Figure 8, below, illustrates this vulnerability. Although not insignificant, above-deck explosions are not considered to be as critical a threat as below-deck detonations. Although specific charge weights and individual assessments of bridge columns of the assets examined are beyond the scope of this project, figure 9, below, presents a good general rule-of-thumb for various sized vehicle borne improvised explosive devices and the appropriate standoff distances.

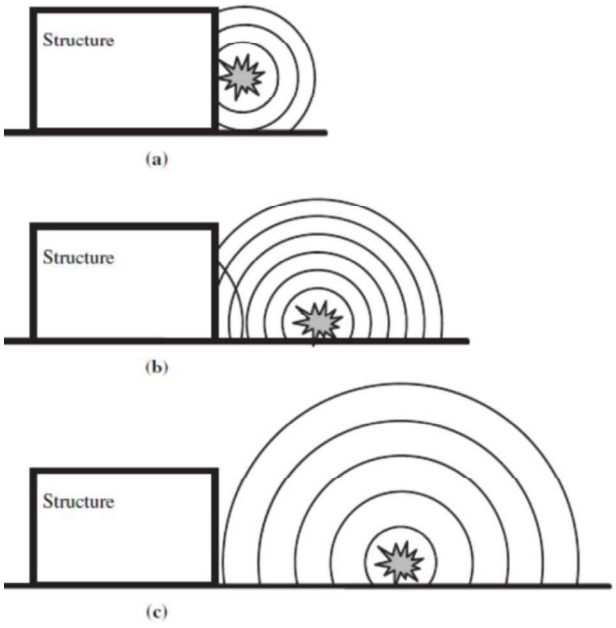


Figure 5: An illustration of the effects of standoff distance: (a) shows a near-contact detonation, (b) shows an increased standoff distance with reduced incident wave, (c) shows an increased standoff distance sufficient to dissipate the incident wave. [1]

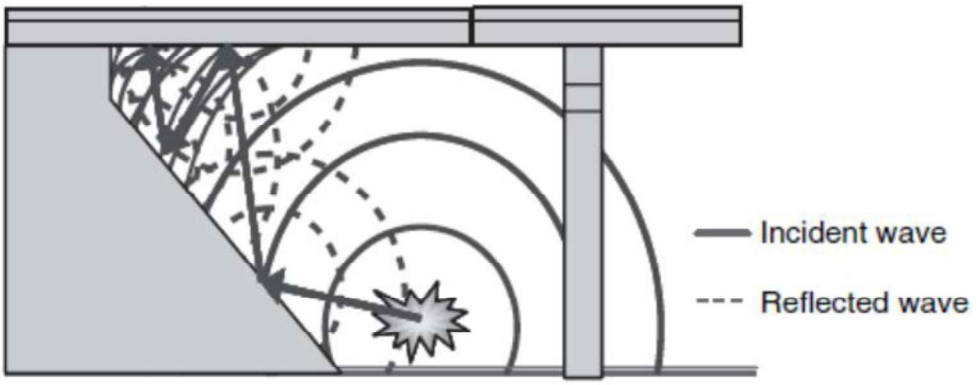


Figure 6: Illustration of the interactions between incident and reflected waves at an abutment [1]

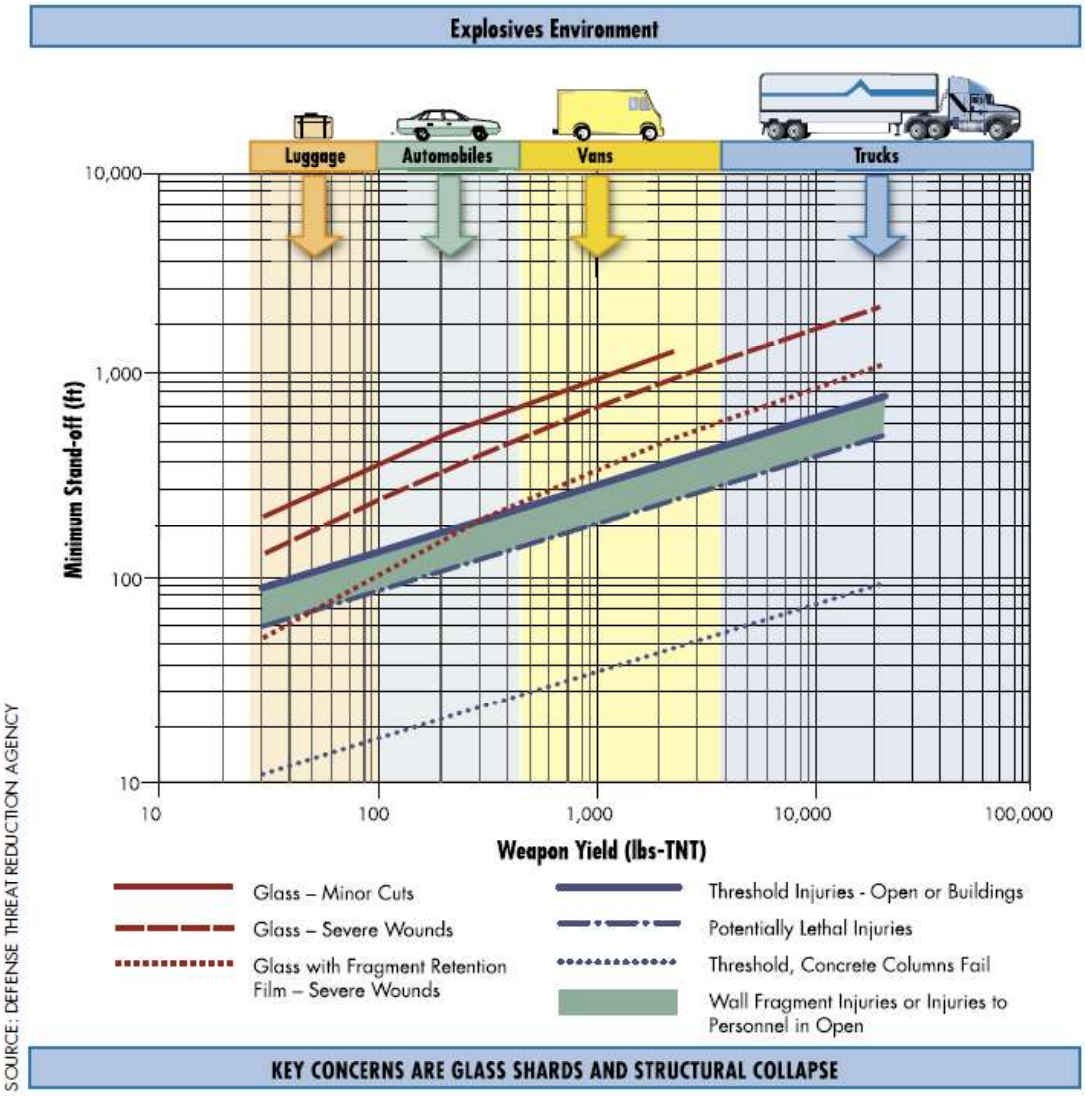


Figure 7: Comparison of explosives yield to standoff distances and effects [14]

The following vehicles were considered for this assessment as the delivery vectors for explosives:

a. M1 - Small boat
b. M2 - Fast boat
c. M3 - Barge
d. V1 - Car
e. V2 -Van
f. V3 - Mid-Sized Truck
g. V4 - Large Truck (18 wheeler)

3. Vehicle-borne other HAZMAT

The vast majority of hazardous material shipping in the U.S. involves gasoline. Annually, there are approximately 19 million gasoline shipments by truck nation-wide. Propane is the most commonly transported flammable gas, transported as liquefied compressed gas in tank trucks or cylinders. Toxic Inhalation Hazard (TIH) chemicals make up another large category of HAZMAT shipments in the U.S. Of those, the most common are anhydrous ammonia and chlorine. Anhydrous ammonia makes up more than 80% of TIH shipments [15].

The primary danger with gasoline and other flammable materials is fire. The ability of flammable materials to damage infrastructure has been made well-known in a few events across the nation. For example, in 1997 a gasoline tanker truck was going under an overpass of the New York State Thruway when it was struck by a sedan. The car hit the right side of the cargo tank in the area of the tank's external loading/unloading lines, releasing the gasoline they contained. The ensuing fire destroyed both vehicles and the overpass; the thruway remained closed for approximately 6 months [16]. Prolonged flammable liquid-fueled fires have the ability to damage infrastructure by melting the reinforcing steel in concrete. Temperatures above 800 degrees Fahrenheit cause the steel to begin to lose its strength and it begins to melt at around 2,700 degrees [15]. Concrete will also exhibit explosive spalling from fire, a phenomenon caused by a combination of water turning to steam and incompatible thermal expansion properties of aggregates and cement paste.

TIH chemicals might be enticing for terrorists to use because they bring with them the connotation of chemical warfare. Their effects, however, would be as inhalation hazards to people. The threat assessment phase of this project will examine the threat potential in more detail, but in general the effects are demonstrated below in figure 10 and 11, both from Jenkins and Butterworth, 2010:

Chemical	Hazard Zone	LC50 (ppm)	ERPG-2 (ppm)	ERPG-3 (ppm)	Boiling Point (°F)	ERG Protective Action Distance (in miles, large spill,[a] at night)
Ammonia, anhydrous	D	4000	150	750	-28.03	1.4
Bromine	A	113	0.5	5	137.80	4.6
Chlorine	B	293	3	20	-30.23	4.6
Ethylene oxide	D	4350	50	500	51.26	1.5
Hydrogen chloride	C	2810	20	150	-118.66	6.5
Hydrogen cyanide	B	40	10	25	78.80	2.3
Hydrogen fluoride, anhydrous	C	1300	20	50	66.92	2.7
Phosgene	A	5	0.2	1	46.94	7.0+
Sulfur dioxide	C	2520	3	15	14	3.9
Sulfuric acid, fuming	B	347	10 mg/ m^3	30 mg/ m^3	625	4

Table 4: TIH hazards with details

Term	Definition
TIH	Toxic inhalation hazard, a term used to describe gases and volatile liquids that are toxic when inhaled. The term is used synonymously with poison inhalation hazard (PIH).
Hazard Zone	One of four levels of hazard (A thought D) assigned by hazardous materials transportation regulations to gases and one of two levels of hazard (Aand B) assigned to liquids that are toxic when inhaled.
Hazard Zone A	Gases: LC50 less than or equal to 200 ppm. Liquids: V equal to or greater than 500 LC50, and LC50 less than or equal to 00 ppm.
Hazard Zone B	Gases: LC50 creater than 200 ppm and less than or equal to 1000 ppm. Liquids: V equal to or greater than 10 LC50, and LC50 less than or equal to 1000 ppm; criteria for Hazard Zone A are not met.
Hazard Zone C	LC50 greater than 1000 ppm and less than or equal to 3000 ppm.
Hazard Zone D	LC50 greater than 3000 ppm and less than or equal to 5000 ppm.
ERPGs	Emergency response planning guidelines, values intended to provide estimates of concentration ranges above which one could reasonably anticipate observing adverse health effects.
ERPG-2	The maximum airborne concentration below which it is believed nearly all individuals could be exposed for up to 1 hour without experiencing or developing irreversible or other serious health effects or symptoms that could impair an individual's ability to take protective action.
ERPG-3	The maximum concentration below which it is believed nearly all individuals could be exposed for up to 1 hour without experiencing or developing live-threatening health effects.
LC50	The concentration of a material administered by inhalation that is expected to cause the death of 50 percent of an experimental animal population within a specified time.
V	Saturated vapor concentration in air of a material in mL/m^3 (volatility) at 20°C and standard atmospheric pressure.
ERG Protective Action Distance	Emergency Response Guidebook (ERG) Protective Action Distances are estimates that have been developed based on historical transportation incidents. Factors considered include quantities of materials released, rates at which the materials were released, and meteorological conditions. Guidebook distances are 90 percent values based on ERPG-2 distances (i.e., in 90% of the incidents, distances are less than the ERG value).

Table 5: TIH definitions

The following threat scenarios were considered in the threat assessment section of this project:

a. C(C) chemical agents
b. C(B) biological agents
c. C(R) radiological material
d. flammable material
e. radiological material

4. Active shooter

The definition of active shooter according to the U.S. Federal Bureau of Investigation is "an individual actively engaged in killing or attempting to kill people in a confined and populated area." The number of active shooter incidents has been trending upwards in recent years. From 2000 to 2013, there were 160 incidents totaling 1,043 casualties including 557 wounded and 486 killed. All but two incidents involved a single shooter.

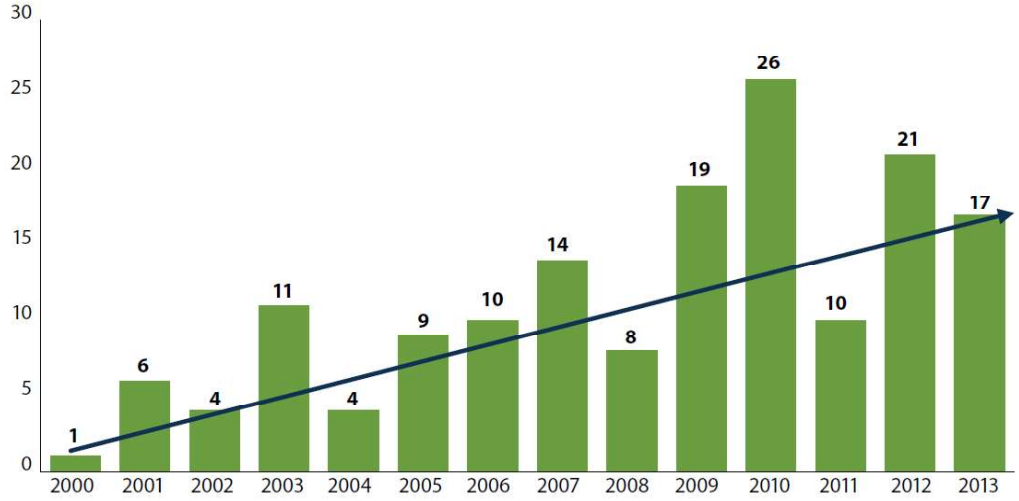


Figure 8: Upward trend of active shooter events in the U.S. [17]

Of the incidents studied, fifteen (15) occurred in "open spaces". In those incidents, 11 of the shooters fired their weapons from vehicles. None of those incidents specifically happened at a definable transportation asset (i.e. a bridge), but several happened on roads and highways [17]. The motivation for active shooters is often difficult to determine, but some of the larger categories have been found to be workplace retaliation (21%), domestic disputes (14%), and retaliation by a current or former student (7%) [18].

5. Combination

A tactic employed by terrorists in the past has been to detonate a primary device followed by a secondary device or active shooters that target emergency responders. Although not common yet in the United States, there have been some instances where this has occurred. Another concerning tactic is the use of a hoax device to elicit the response of emergency personnel followed by the detonation of an actual device [19].

Vulnerability Assessment

According to ASME, "[Vulnerability assessment/ analysis] estimates the likelihood of each specific threat or hazard to overcome the defenses of the asset to the level identified in the consequence estimate for that threat/asset combination." For terrorist attack, this measures the likelihood of the success of the terrorists to accomplish their goal, resulting in the consequences proposed. For non-terrorist events, this step seeks to identify vulnerabilities to those threat scenarios considered (man-made accidental and natural hazards). Fundamentally, vulnerability assessment involves the use of logic in the form of vulnerability logic diagrams and event trees, or hybrids of these. Both are simplified game theory exercises, with the likelihood of threat success being measured against conditions observed at the asset location. The likelihood of the success of a specific threat is assigned a number of 0 to 1, with corresponding percentages of the likelihood of success.

Bin		Decimal Description	Percentage Range (%)	Successes per Attempts
5	A	0.90 – 1.00	90 – 100	$9/10 \leq L \leq 1$
	B	0.75 – 0.89	75 – 89	$3/4 \leq L < 9/10$
	C	0.50 – 0.74	50 – 74	$1/2 \leq L < 3/4$
4		0.25 – 0.49	25 – 49	$1/4 \leq L < 1/2$
3		0.125 – 0.249	12.5 – 24.9	$1/8 \leq L < 1/4$
2		0.0625 – 0.124	6.25 – 12.4	$1/16 \leq L < 1/8$
1		0.0312 – 0.0624	3.12 – 6.24	$1/32 \leq L < 1/16$
0		< 0.0311	<3.11	$L < 1/32$

Table 6: RAMCAP vulnerability matrix [10]

It is assumed that, for a terrorist attack, the terrorist(s) will seek to do the most damage for a given asset with a given threat vector. The following is an example of the process used for all threat vectors for the assets under consideration:

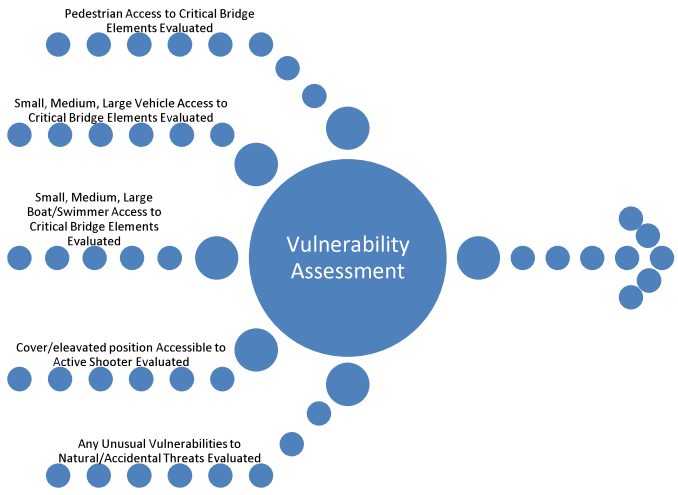


Figure 9: Vulnerability assessment process

Vulnerability Factors Considered Across the Board for All Assets Studied

From the Enhanced Threat and Risk Assessment tools [20], the following factors are also calculated during the vulnerability assessment:

1.	**Level of Visibility:** Assess the awareness of the existence and visibility of the target to the general public.		
	0=Invisible: Existence secret/Classified location	**3=Medium Visibility:** Existence known locally	
	1=Very Low Visibility: Existence not publicized	**4=High Visibility:** Existence known regionally	
	2=Low Visibility: Existence public but not well known	**5=Very High Visibility:** Existence known nationally	
2.	**Criticality of Target Site to Jurisdiction:** Assess usefulness of assets to local population, economy, government, etc. Potential targets deemed essential to the continuity of the		
	0 = No Usefulness	**2** =Moderate Usefulness	**4** = Highly Useful
	1 = Minor Usefulness	**3** = Significant Usefulness	**5** = Critical
3.	**Impact Outside the Jurisdiction:** Assess the affect loss will have outside of the jurisdiction.		
	0 = None	**2** = Low	**4** = High
	1 = Very Low	**3** = Medium	**5** = Very High
4.	**PTE Access to Target:** Assess the availability of the target for ingress and egress by a PTE.		
0=	**Restricted:** Security patrol 24/7, fenced, alarmed, CCTV, controlled access requiring prior clearance, designated parking, no unauthorized vehicle parking within 300 feet of facility, protected		
1=	**Controlled:** Security patrol 24/7, fenced, alarmed, controlled access of vehicles and personnel, designated parking, no unauthorized vehicle parking within 300 feet of facility, protected		
2=	visitors, designated parking, no unauthorized vehicles parking within 300 feet of facility, protected air/consumable entry.		
3=	Moderate: Controlled access of visitors, alarmed after business hours, protected air/consumable entry, designated parking, no unauthorized vehicle parking within 50 feet.		
4=	**Open:** Open access during business hours, locked during non-business hours, unprotected		
5=	**Unlimited:** Open access, unprotected air/consumable entry.		
5.	**Potential Target Threat of Hazard:** Assess the presence of legal WMD material (CBRNE) in quantities that could be the target of a terrorist attack or would complicate the response to an incident at that facility.		
0=	**None:** No WMD materials present.		
1=	**Minimal:** WMD materials present in moderate quantities, under positive control, and in secured		
2=	**Low:** WMD materials present in moderate quantities and controlled.		
3=	**Moderate:** Major concentrations of WMD materials that have established control features and are		
4=	**High:** Major concentrations of WMD materials that have moderate control features.		
5=	**Very High:** Major concentrations of WMD materials that are accessible to non-staff personnel.		
6.	**Potential Target Site Population Capacity:** Assess the maximum number of individuals at a site at any given time.		
	0 = 0	**2** = 251-5000	**4** = 15,001-50,000
	1 = 1-250	**3** = 5,001-15,000	**5** = >50,001
7.	**Potential for Collateral Mass Casualties**: Assess potential collateral mass casualties within a one-mile radius of the target.		
	0 = 0-100	**2** = 251-5000	**4** = 15,001-50,000
	1 = 101-250	**3** = 5,001-15,000	**5** = >50,001

Vulnerability Assessment Results Summarized

The most common vulnerabilities noted were, in order of importance:

1. Under-deck vehicular access to abutments
2. Under-deck vehicular access to bridge columns
3. Co-location with explosive/dangerous materials
4. Potential access to piers/columns to boats and swimmers
5. Pedestrian access to under-deck elements
6. Vegetative concealment and/or elevated position for active shooters

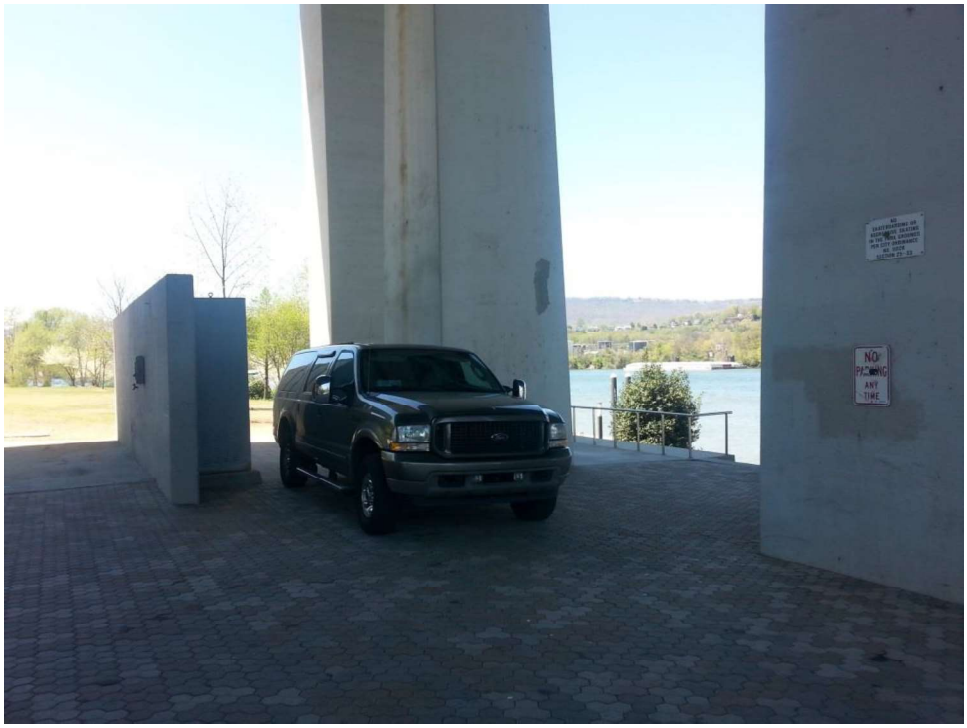


Figure 10: Example of open abutment vehicular access. Note the location of the concrete wall and the implications of reflected waves.

Figure 11: Example of partially controlled abutment vehicular access

Figure 12: Example of partially open abutment vehicular access with simultaneous bridge column access to another bridge

Figure 13: Example of co-location with dangerous substances. This photo is of liquid propane rail cars as seen from under the bridge deck

Vulnerabilities for specific assets with photos are available for discussion with appropriate personnel. Listing actual vulnerabilities for individual assets is beyond the scope of this report, but are considered in-depth in risk assessment calculations.

Threat Assessment

Threat assessment estimates the likelihood of terrorist attack, accidental event, or natural hazard. In terms of terrorism, this involves identifying not only the threat vector, but also examining people or groups that may want to carry out an attack. Because the assets in question have been assumed to be near the risk tolerance for TDOT for natural hazards and most accidental events, only threats that may manifest themselves through a particular asset's vulnerabilities are considered. For example, all assets are assumed to have gasoline tanker trucks moving across them with a frequency that is generally the same throughout the state as a percentage of total freight, so that threat is not considered in great detail. However, some assets are co-located near large quantities of dangerous substances while others are not. Those assets that do have co-location with dangerous substances have that threat taken into account when calculating risk. Also, because each asset has differences in vulnerabilities to terrorist attack, this threat vector is the major contributor to this threat assessment.

Threat assessment takes into account the threats discussed in the threat characterization sector as well as who may carry out the threat.

How Do Terrorists Think About Targets?

Jenkins and Butterworth [15] explain how terrorists think about targets. From the history of terrorist attacks on U.S. interests, it is useful to group targeting by likelihood:

1. Prominent government, political and financial figures
2. Government buildings, particularly iconic structures
3. Commercial property, especially financial institutions
4. Critical infrastructure, such as telecommunication, **transportation**, energy, and power
5. National icons such as the Statue of Liberty, Washington Monument, etc.
6. Outdoor public gatherings with large numbers of people
7. Large numbers of civilians inside public venues such as stadiums and shopping malls
8. Large numbers of civilians inside multi-unit residential housing

The list above is general as it applies to terrorist targets. Further specific targeting information is discussed below in each group's Potential Threat Element (PTE) profile.

Potential Threat Elements Considered

Terrorist threats are measured by intent and capabilities. Although it is considered to be less severe than the massive scale of the 9/11 attacks, the threat today is more complex and more diverse than at any time since then [21]. Recent attacks in Paris on the offices of the Charles Hebdo newspaper have demonstrated a significant development in terrorism circles. In the past, Islamist groups like Al-Qaeda and its affiliates have gone after very high visibility "big splash" targets such as the U.S.S. Cole, the first World Trade Center bombing, and the spectacular attacks of 9/11. The Charles Hebdo attacks have shown that the tremendous amount of effort exerted in the previous large-scale attacks is not necessarily required for the world to take notice. If this tactic catches on with terrorist groups, it could mean greater difficulty in detecting the threat before it occurs. For purposes of this analysis, it is useful to group the PTEs into two groups, Non-Jihadist Related Groups, and Jihadist-Related groups due to the similarities that can be observed among respective members of each group.

Non-Jihadist Related Groups

Non-Jihadist related groups include any identified groups that are not primarily concerned with the Islamist promotion of jihad against American targets. This includes mostly U.S.-based domestic terror and domestic hate groups.

Domestic "Hate Groups" in Tennessee

The Southern Poverty Law Center [22] defines the groups listed in the table below as "hate groups". Hate groups have no formal designation in the U.S. government, but it is prudent here to consider domestic

political unrest as a catalyst for terrorist acts. However, since 2009, the FBI has been given the legislative authority to investigate hate crimes, which they say may be prosecutable as domestic terrorism [23]. Many of the groups listed below have not engaged in widespread violence, but their extremist viewpoints are certainly an early indicator of potential threat.

Name	Type	City
American Third Position	White Nationalist	Gatlinburg
Citizen Warrior	Anti-Muslim	Nashville
Confederate Hammerskins	Racist Skinhead	Nashville
Council of Conservative Citizens	White Nationalist	Cleveland
Council of Conservative Citizens	White Nationalist	Franklin
Council of Conservative Citizens	White Nationalist	Knoxville/Chattanooga
Council of Conservative Citizens	White Nationalist	Memphis
Creativity Alliance,The	Neo-Nazi	Mountain City
Crew 38	Racist Skinhead	
Fraternal White Knights of the Ku Klux Klan	Ku Klux Klan	Woodbury
Knights of the Ku Klux Klan	Ku Klux Klan	Newport
Ku Klos Knights of the Ku Klux Klan	Ku Klux Klan	Church Hill
League of the South	Neo-Confederate	Lobelville
Loyal White Knights of the Ku Klux Klan	Ku Klux Klan	
Mary Noel Kershaw Foundation	Neo-Confederate	Lobelville
Nation of Islam	Black Separatist	Memphis
Nation of Islam	Black Separatist	Nashville
National Black Foot Soldier Network	Black Separatist	Knoxville
National Socialist Movement	Neo-Nazi	Central Tennessee
National Socialist Movement	Neo-Nazi	
Political Cesspool,The	White Nationalist	Bartlett
Political Islam	Anti-Muslim	Nashville
Revolutionary Order of the Aryan Republic	Neo-Nazi	Chattanooga
Shepherd's Call Ministries,The	Christian Identity	New Tazewell
South Africa Project	White Nationalist	

Tea Party Nation	General Hate	Franklin
Tennessee Freedom Coalition	Anti-Muslim	Nashville
True Invisible Empire Traditionalist American Knights of the Ku Klux Klan	Ku Klux Klan	La Vergne
United Klans of America	Ku Klux Klan	Dyersburg
United Klans of America	Ku Klux Klan	Nashville
United Klans of America	Ku Klux Klan	Shelbyville
United Northern and Southern Knights of the Ku Klux Klan	Ku Klux Klan	Kingsport
Volksfront	Racist Skinhead	Knoxville
National Socialist Movement	Neo-Nazi	
Political Cesspool,The	White Nationalist	Bartlett
Political Islam	Anti-Muslim	Nashville
Revolutionary Order of the Aryan Republic	Neo-Nazi	Chattanooga
Shepherd's Call Ministries,The	Christian Identity	New Tazewell
South Africa Project	White Nationalist	
Tea Party Nation	General Hate	Franklin
Tennessee Freedom Coalition	Anti-Muslim	Nashville
True Invisible Empire Traditionalist American Knights of the Ku Klux Klan	Ku Klux Klan	La Vergne
United Klans of America	Ku Klux Klan	Dyersburg
United Klans of America	Ku Klux Klan	Nashville
United Klans of America	Ku Klux Klan	Shelbyville
United Northern and Southern Knights of the Ku Klux Klan	Ku Klux Klan	Kingsport
Volksfront	Racist Skinhead	Knoxville

Table 7 SPLC hate groups listing for Tennessee (Southern Poverty Law Center, n.d.)

Sovereign Citizen Movement

In a recent study by the National Consortium for the Study of Terrorism and Response to Terrorism (START), the Sovereign Citizen Movement was identified by researchers as the top threat to domestic security in the United States. The study polled 364 officers representing 175 local, state, and tribal law enforcement agencies, with 86% responding that it was the number one threat [24]. In March, 2012, DHS had identified the Sovereign Citizen Movement as a major threat previously, acknowledging that most people identifying as Sovereign Citizens were non-violent, but instances of the group's violence and thwarted violence is seeing a swift rise [25].

Sovereign Citizens are very loosely organized, with little or no formal structure. Instead, much of the doctrine is shared via the internet. In general, most Sovereign Citizens believe that the United States government is illegal, having departed from the true Constitution. The points in time where this is said to

have happen vary, but many believe that it occurred when the U.S. left the gold standard as its currency. Because they believe that the current government is illegal, Sovereign Citizens believe that they are not subject to its rules of taxation, property laws, drivers licenses, etc. Much more widespread than violence, "paper terrorism" of flooding the courts with bogus lawsuits, appeals, and motions have been a favored tactic.

Analysis of Non-Jihadist Groups

The analysis by Jenkins and Butterworth [15] and others [80,81] conclude that 1) domestic hate groups do not equal terrorist activity, and that hate crimes typically follow, rather than precede terrorist events and that 2) non-jihadist groups are very unlikely to attack transportation infrastructure, with domestic group targets being distributed between 1995 and 2010 as seen in figure x below:

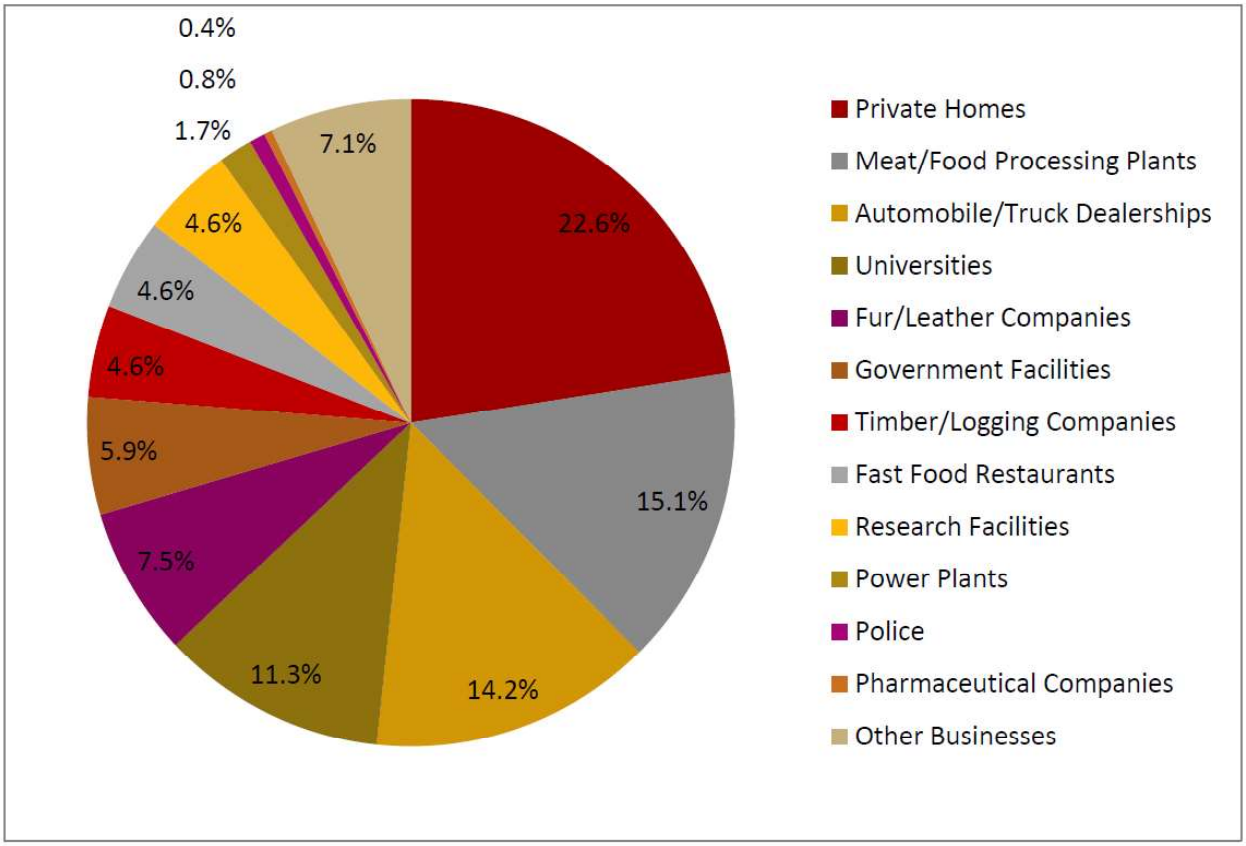


Figure 14: Target selection of U.S.-based terror groups, 1995-2010 [80]

This analysis indicates that only a very low likelihood of threats against critical transportation infrastructure in Tennessee exists from domestic groups based on their activities in the past. However, the threat environment is continually changing, and U.S. analysts and authorities are concerned that, especially with respect to Sovereign Citizens, some future catalyst may change the targeting dynamic.

The Lone-Wolf Domestic Threat

The so-called lone wolf terrorist operates without organizational support, but may well draw inspiration from internet- and paper- published materials. There are some useful common characteristics observed for lone wolf actors, including [64]:

1. The presence of a personal or political grievance or unfair treatment by an individual or a group.
2. Status and risk seeking behavior - a desire for attention or fame as a result of the attack.
3. A change in circumstances (referred to as "unfreezing") of the attacker that leaves the lone wolf in a state of distress.

Although it is feasible that a lone-wolf domestic actor could target critical transportation assets, it is not likely, based on historical information. Historically, the domestic lone wolf generally targets individuals directly related to the source of a grievance. Some potential threat elements in this category that might require further scrutiny would be those directly related to TDOT or a TDOT asset in some way. For example:

1. A disgruntled employee or former employee.
2. A person who has been displaced by construction activity associated with a TDOT asset.

Lone-wolf terrorists will typically follow the path of least resistance, i.e. easy-to-obtain materials, and easily accessible targets. For example, small arms and ammunition acquisition and targeting of individuals at an office building or a construction site is much more likely than going to the trouble of purchasing or otherwise obtaining sufficient bomb-making materials and executing an explosives attack on the asset itself. The lone-wolf terrorist is much more difficult to detect than terrorism associated with a group; the lone-wolf terrorist will typically operate in a vacuum, telling few (if anyone) people about their planned attack. The effort of obtaining bomb-making materials increases the likelihood of the lone-wolf's plans being detected ahead of time.

Jihad-Based Groups

By far, the most well-known Jihad-based groups to Americans is Al-Qaeda. Since 9/11, U.S. efforts to destabilize and remove the leadership of Al-Qaeda have seen some measures of success, forcing the group to re-invent itself. No longer is Al-Qaeda central seen as the generator of intricate, complex, and well-thought out operations. However, the metamorphosis undertaken by Al-Qaeda has made tracking the activities of all of the associated groups a difficult task. It is therefore useful to describe the activities of Al-Qaeda inspired and connected groups as part of the global Salafi Jihad.

The Global Salafi Jihad

Salafi Jihad has at its roots the Egyptian Salafist Qutb and Faraj, who believed that the state of Islam was in as bad shape as it was before the prophet Muhammed came because modern Muslim rulers refused to administer Sharia Law. Qutb and Faraj called for death of the "secular" apostate leaders. Out of that has grown the Global Salafi Jihad, a term coined by Marc Sageman in his testimony before National Commission on Terrorist Attacks upon the United States in 2003. Now the priority is fighting the "far enemy," the West and specifically the U.S. and Israel, before turning against the "near enemy," which

survive only because of Western support. This strategy has evolved from ending the U.S.'s "occupation" of the Holy Land to engaging it anywhere, as best articulated by Ayman al Zawahiri . The goal is to establish a Muslim state, reinstate the fallen Caliphate and regain its lost glory. As the United States would never allow this to happen, the global jihad must defeat this country. It needs to "inflict the maximum casualties against the opponent, for this is the language understood by the West" and "concentrate on the method of martyrdom operations" as the most efficient in terms of damages and least costly to the jihad. These victories will inspire and mobilize the Muslim masses to achieve its goal. The Global Salafi Jihad includes all the terrorist organizations implementing this strategy [26]. This broad brush includes al-Qaeda and its offshoots, and the Islamic State in Iraq and Syria, or ISIS (also known as the Islamic State in the Levant, or ISIL).

Former CIA Director R. James Woolsey has been often quoted for his astute observations during his confirmation hearings in 1993 referring to the collapse of the Soviet Union and the challenges that he foresaw in the years ahead. "Yes, we have slain a large dragon…But now we live in a jungle filled with a bewildering variety of poisonous snakes. And in many ways, the dragon was easier to keep track of." [27] This commentary was referring to the shift from conventional warfare to asymmetrical war; we had just eight years from Director Woolsey's comments to the events of 9/11 that alerted the U.S. that we were at war. In 2015, does director Woolsey's metaphor continue to hold true today?

In 2015, after several years of intense counterterrorism efforts, our enemies behave much less like disconnected poisonous snakes in a jungle and much more like a Herculean hydra that regrows two heads every time one is removed. Some heads are more connected to the body of Wahabist Islamism than others. Some arise from seemingly out of nowhere, with no warnings given as to their existence previously; these are the self-radicalized or locally radicalized. Former Secretary of Homeland Security, Janet Napolitano, has said that authorities are “just beginning to confront the reality that we have this issue ... and that we really don’t have a very good handle on how you prevent someone from becoming a violent extremist.” [28] Marc Sageman, a forensic psychiatrist and former Central Intelligence Agency (CIA) operations officer who writes about terrorism, has noted a global shift in terrorism toward decentralized, autonomously radicalized, violent jihadist individuals or groups who strike in their home countries. “This is the reality of asymmetrical warfare. When the enemy is willing to behead children, crucify entire villages, and with box cutters put commercial aircraft into buildings, there’s nothing this evil won’t do in pursuit of goal,” he said. “I think we’re at risk.” [29]

Global Salafi Jihad Asset Targeting

The threat from al Qaeda and associated groups is easier to analyze than other groups because of their history and stated intentions. Al Qaeda's history and statements indicate a preference for the "big splash" attacks; those that have high body counts and/or symbolic or emotional meanings associated with the targets. Almost all of the jihadist attacks since 9/11 have been directed against unprotected or lightly protected assets such as hotels, restaurants, nightclubs, public surface transportation (trains & buses), embassies, consulates, and commercial buildings. According to Jenkins and Butterworth, this strongly suggests a low tolerance for risk of failure [15]. It must be recognized, however, that this risk avoidance is not an avoidance of personal risk, as many of the above attacks were undertaken by suicide bombers.

The risk avoidance was strictly in the realm of operational risk, i.e. they wanted the mission to succeed, so attacked soft targets. Jenkins and Butterworth explain the situation further, "Bridges were cited as targets in a few plots, but these plots were uncovered at the “thinking about” or reconnaissance stage, before any operational planning. There is no evidence that terrorists had or could easily have acquired the means to successfully carry out attacks against inherently robust targets in the transportation sector."

The targeting activities of ISIS must be considered separately, however, due to a different set of motivations. ISIS owes its development and generation to Al-Qaeda, specifically Al-Qaeda in Iraq. However, since its inception, ISIS has notably split from central Al-Qaeda leadership, chasing their shared goal of an Islamic caliphate in a much different manner. As stated previously, Al-Qaeda has favored the "big splash" attacks aimed at the "far enemy" to influence the political landscape. However, ISIS has concentrated on a much more traditional advancement of the caliphate; actually acquiring physical land. This physical land acquisition has manifested itself in the Middle East, specifically Western Iraq and Southern Syria.

Another very important distinction to draw between ISIS and Al-Qaeda central is that ISIS has alienated much of the Islamic religious establishment through 1) the perceived illegitimate declaration of ISIS's leader, Abu Bakr al-Baghdadi, as the Caliph, and 2) their excessively brutal tactics, including rape, torture, and murder of even fellow Muslims. In spite of, and perhaps even because of, their brutal tactics, ISIS attracts a different set of followers than traditional Islamist terror groups.

Analysis of Jihad-Based Groups

Although Al-Qaeda central has certainly been destabilized, the six deadliest groups examined in 2012 were all related to Al-Qaeda, or Al-Qaeda inspired, responsible for a total of around 5,000 fatalities globally in that year. Specifically, those top six groups were: 1) The Taliban, 2) Boko Haram, 3) al Qaeda in Iraq, 4) Tehrik-e-Taliban Pakistan, 5) al Qaeda in the Arabian Peninsula, and 6) al-Shabab [68]. This is concerning because Al Qaeda, much more than ISIS, has shown a concern in attacking the "far enemy" for political gain. ISIS has not demonstrated serious attention to the "far enemy", i.e. U.S.-based assets, instead concentrating their efforts on people and assets within their physical sphere of influence. Because of this important difference, organized group-associated attacks within the United States are still more likely to come from an Al-Qaeda affiliated source rather than ISIS. The dynamic changes, however, when the activity is examined in the light of domestic Jihad-inspired cells or lone wolf terrorists.

Domestic Al Qaeda-and ISIS- Inspired Cells

Typical characteristics of people that may be inspired by Jihadist groups include immigrants that may be first or second generation converts to Islam, possibly radicalized by jihadist or Salafi websites. Their training and funding may be very limited. Rather than "taking orders" from a central command authority like Al Qaeda or ISIS, these cells generally consist of several like-minded individuals that may have a inconsistent demographic, intensity, and planning.

Of particular concern is the estimated 15,000 foreigners who have gone to Syria and Iraq to assist in fighting there, including an estimated 2,000 Westerners [84]. In theater, these fighters would likely be subject to training and experience that could aid them should they wish to continue their violence once they return home.

A newly-emerging threat is the specter of "homegrown" ISIS-inspired terrorism. Although technically ISIS can be grouped in with al-Qaeda in the category of Global Salafi Jihad because they aspire to establish the global caliphate, the group's motivations differ significantly from Al-Qaeda and they attract a different sort of recruit. All terrorist groups seem to attract disaffected young men who are looking for a way to become something more important. ISIS offers the promise of power; the power to kill, loot, and rape almost at will with little of the religious concern or worry that traditionally accompanies Islamist groups. Of course, being a Muslim is required, but the opportunities for absolute wickedness with no concern for the lives or well-being of even other Muslims who oppose ISIS abound. This paradigm attracts individuals who have little power over their own lives before joining. In many ways, the psychology involved seems to mirror the mindset of youths that join U.S.-based urban gangs. Brian Michael Jenkins, a world-renowned expert on terrorism sums up the threat [84]: "The incorporation into ISIL of a large number of bloodthirsty foreign fighters who seem to have little future in any peaceful society will have long-term consequences. It means that the Islamic State can never be stable. Either the thugs are killed off or they find new killing fields on its frontiers or beyond."

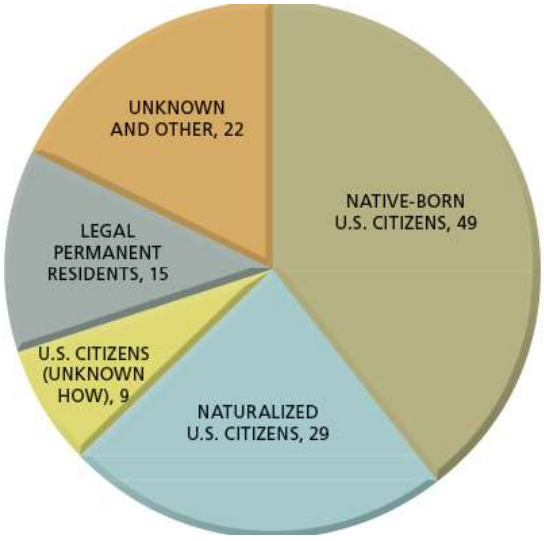


Figure 15: Nationalities of Would-Be Jihadists Returning Home [84]

Analysis of Domestic Al-Qaeda and ISIS Inspired Cells:

This PTE is perhaps the most threatening of all examined in this analysis. Because the threat is home-grown, the possibilities of detecting the threat are reduced. Although lone actors may not have the resources to pursue destruction of critical transportation assets, cells of jihadist-inspired individuals may be able to pool their resources and accomplish an attack. There is no shortage of bomb-making instructions available on the internet, and bomb making materials are not difficult to obtain, consisting of

an oxidizer, a fuel source, and an ignition source. Some restrictions and reporting requirements have been put into place to help detect nefarious activity, such as the flagging of large purchases of ammonium nitrate, a component of ANFO. However, the range of bomb-making materials is so large that it is impossible to track all potential components to the degree necessary to ensure absolute security.

Consequence Analysis

"With each piece of the global transportation network increasingly tied to every other part, the cascading impacts from adverse events can now extend further than ever before." [2] The full consequence of a disruption of service of a critical transportation asset is difficult to determine, but some fairly straightforward points of comparison can be delineated utilizing the RAMCAP method. Consequence analysis takes into account the following [10]:

1. Human Health & Safety Impacts
    a. Fatalities - on site/off site
    b. Serious injuries - on site/off site
    c. Acquisition of dangerous materials/ weapons of mass destruction
    d. Contamination to water, food, or pharmaceuticals
2. Financial & Economic Impacts
    a. Asset replacement costs
    b. Remediation costs
    c. Business interruption costs
    d. Negligence liability costs
    e. National/ regional economic losses/multiple sector impacts
    f. Loss of critical data
    g. Loss of reputation or business viability
3. National Security & Government Functionality Impacts
    a. Military mission importance and readiness
    b. Delivery of public health services
    c. Contamination of/ disruption to critical potable water or sanitation services
    d. Interruption of governance, public safety, or law enforcement
4. Environmental Impacts
    a. Permanent or long-term damage to the ecosystem
    b. Pollution of air, water, or soil
5. Psychological Impacts
    a. Impact to iconic/symbolic assets
    b. High profile and/or symbolic casualties
    c. Loss of consumer confidence
    d. Loss of confidence in governmental institutions

Many of the above categories of consequence impact to the asset are the same across the board for the ten assets studied. Since the objective of this project is to prioritize assets for consideration of mitigation activities, the parameters deemed to be the same across the ten assets

are not considered as part of the comparative process. The categories that may vary between assets, and are thus considered in the analysis are:

1. Human Health & Safety Impacts
    a. Fatalities - on site/off site
    b. Serious injuries - on site/off site
    d. Contamination to water, food, or pharmaceuticals
2. Financial & Economic Impacts
    a. Asset replacement costs
    b. Remediation costs
    c. Business interruption costs
    e. National/ regional economic losses/multiple sector impacts
3. National Security & Government Functionality Impacts
    a. Military mission importance and readiness
    b. Delivery of public health services
    c. Contamination of/ disruption to critical potable water or sanitation services
    d. Interruption of governance, public safety, or law enforcement
5. Psychological Impacts
    a. Impact to iconic/symbolic assets
    b. High profile and/or symbolic casualties

Because the above may vary depending on the asset in question, these were considered as part of the process.

Risk Assessment

In the RAMCAP framework, risk and resilience assessment creates the foundation for selecting strategies and tactics to defend against disabling attacks and events by establishing priorities based on this level of risk. This risk assessment is a tool to prioritize mitigation activities across a series of assets. The risk assessment step is a systematic and comprehensive evaluation of the previously developed estimates. The risk for each threat for each asset is calculated from the risk relationship:

Risk = Consequences x Vulnerability x Threat Likelihood.

Each asset's risk profile was calculated individually (ex. Figure 16 below), and a summary of the findings is presented in table 8.

This risk assessment takes into account the highest risk (worst case scenario) of a home-grown Al-Qaeda/ISIS - inspired cell of active shooter(s)/ explosives attack upon each asset.

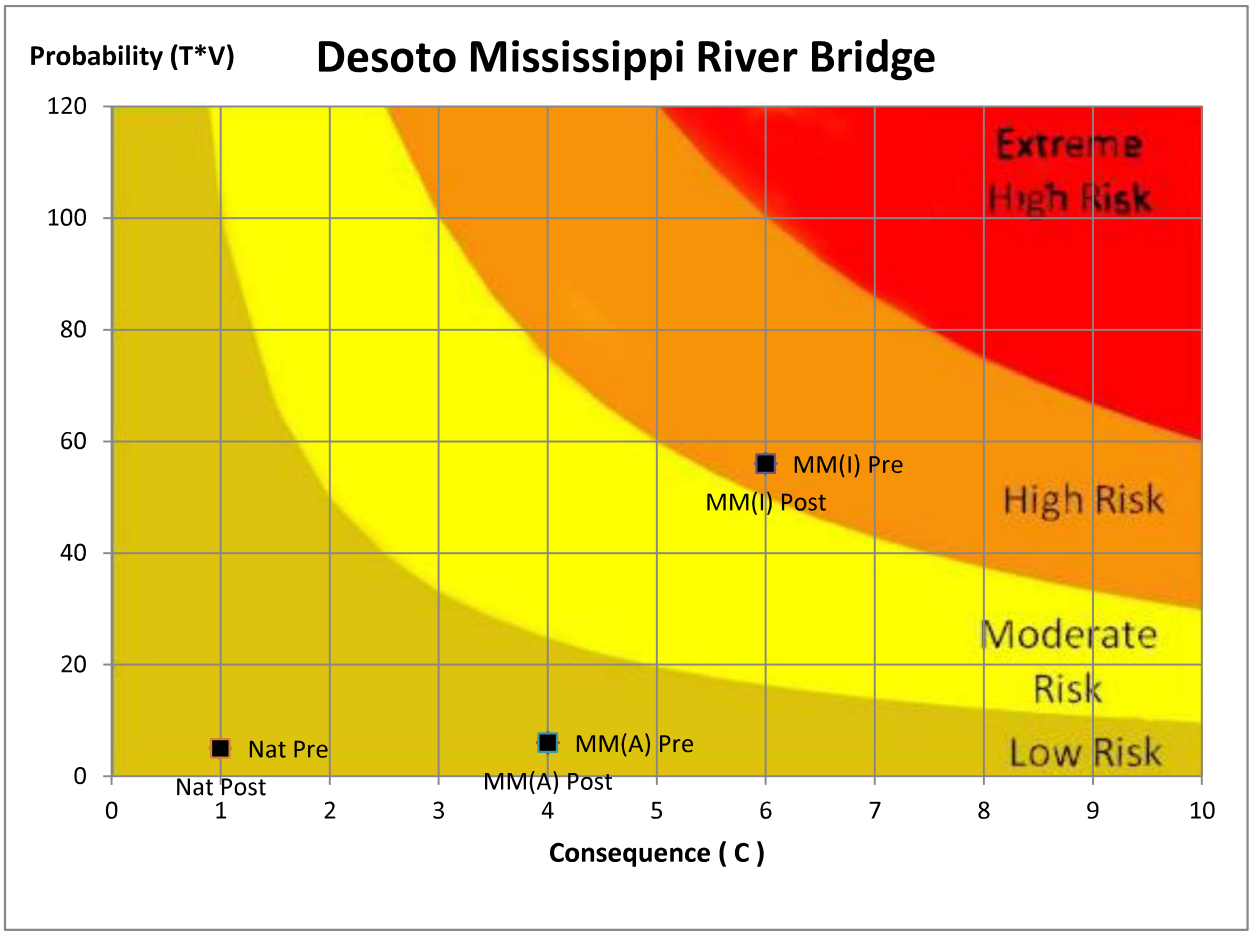


Figure 16: Example of Risk Assessment Software Results, Desoto Bridge

The risk assessment process yields the following prioritization:

	Vulnerability	Threat	Probability	Human Impact	Economic Impact	Consequence	RISK
	V	T	P= V*T	HI	EI	C= HI+EI	R= PxC
1. Hernando Desoto Mississippi River Bridge (Shelby Co., TN)	7	8	56	3	3	6	336
3. I-40/I-440 Interchange (Davidson Co., TN)	7	4	28	4	4	8	224
5. I-65 Bridge over Cumberland River (Davidson Co., TN)	7	4	28	4	4	8	224
6. P.R. Olgiati Bridge (Hamilton Co., TN)	8	4	32	3	3	6	192
2. I-24 Bridge over Cumberland River (Davidson Co., TN)	6	4	24	3	4	7	168
9. I-75/I-40 Bridge over Papermill (Knox Co., TN)	5	4	20	4	4	8	160
4. I-40/I-240 Interchange (Shelby Co., TN)	6	4	24	3	3	6	144
7. I-24/I-65 Bridge over W. Trinity Lane (Davidson Co., TN)	6	4	24	3	3	6	144
8. I-440/I-24 Interchange (Davidson Co., TN)	6	4	24	3	3	6	144
10. I-75 Slope Failure (Campbell Co., TN)	3	4	12	2	2	4	48

Table 8: Assets prioritized by calculated risk

Risk and Resilience Management

The major tasks in risk management are [10]:

1. Decide whether the risk and resilience levels for each asset/ threat pair are acceptable;
2. Define or develop countermeasures and mitigation/resilience options for each unacceptable asset/threat and estimate their investment and operating costs;
3. Evaluate the options by analyzing the facility or asset under the assumption that the option has been implemented – revisiting RAMCAP Plus process steps 2 through 6 to re-estimate the risk and resilience levels, and the estimated benefits of the option (the difference between the risk and resilience with and without the option);
4. Accumulate the benefits of all asset/threat pairs for which a single option reduces risk and/or enhances resilience, so that the option is the sum of the benefits it would bring about;
5. Estimate the benefit-cost ratio (and/or other criteria relevant in the organization's resource decision-making) to estimate the marginal value of each option;
6. Select among the options considering all the dimensions – benefit/cost ratios, fatalities, serious injuries, financial losses to the owner, economic losses to the community, and qualitative factors – and rank and allocate resources to them;
7. Implement, monitor and evaluate the performance of the selected options;
8. Conduct additional risk assessments to monitor progress and adapt to changing conditions.

The decision making used in tasks 1 through 3 relies on the recalculation of some or all the six steps in the RAMCAP Plus process, which will most likely result in an overall reduced risk of threat, vulnerability and/or the consequences of an attack. Risk reduction is recognized by comparing the current risk with the risk reduced, assuming the system changes and resilience-enhancement options have been implemented. The amount of risk reduction (lowered vulnerability, threat/hazard probability or reduced consequences) or resilience enhancement (reduction in the number of days and severity of lost service and the corresponding losses to the community) result in and define the benefits of the chosen options for the organization and the region, respectively.

Mitigation Efforts for Consideration

Throughout the literature, mitigation efforts can be summarized with the "four security Ds":

The goal of the assessment process is to achieve the level of protection sought through implementation of mitigation measures in the building design. These measures may reduce risk by deterring, detecting, denying, or devaluing the potential threat element prior to or during execution of an enemy attack. The Department of Homeland Security uses the following methodology to achieve this purpose.

Deter: The process of making the target inaccessible or difficult to defeat with the weapon or tactic selected. It is usually accomplished at the site perimeter using highly visible electronic security systems, fencing, barriers, lighting, and security personnel and in the building by securing access with locks and electronic monitoring devices.

Detect: The process of using intelligence sharing and security services response to monitor and identify the threat before it penetrates the site perimeter or building access points.

Deny: The process of minimizing or delaying the degree of site or building infrastructure damage or loss of life or protecting assets by designing or using infrastructure and equipment designed to withstand blast and chemical, biological, or radiological effects.

Devalue: The process of making the site or building of little to no value or consequence, from the terrorists' perspective, such that an attack on the facility would not yield their desired result.

Figure 17: The Four Security Ds [11]

The choices of mitigation strategies will vary by asset. In general, the costs and benefits of each mitigation strategy must be weighed to arrive at a desirable outcome that reduces the risk to the asset. Winget gave several examples of mitigation activities pertaining to bridges [12]:

- Increased law enforcement patrols
- Keyed or keyless entry systems at inspection points
- Intrusion detection systems at critical points
- CCTV monitoring
- Identification procedures for maintenance personnel
- Emergency telephones to report suspicious activities
- An advance warning system to include lights, sirens, and pop-up barriers in the event of span failure
- Physical barriers to restrict access to critical components
- Improved lighting with emergency backup
- Elimination of hiding places and clearing of overgrown vegetation
- Elimination of parking spaces beneath bridges
- Planned redundancy in future bridge construction such as building two two-lane bridges instead of one four-lane bridge
- Avoidance of architectural features that magnify blast effects such as unnecessary confined areas.

With these in mind, several example mitigation strategies are given below, grouped by their 4D category:

Threat Vector	Deterrence Measures	Detection Measures	Denial Measures	Devalue Measures
Active Shooter	Pedestrian access restricted with fencing and signage Increase Patrols by Law Enforcement/ Other	Increased CCTV Extensive Training of CCTV/Help Truck Personnel Increased Patrols by Law Enforcement/Other	Construction of Sight-line breaking walls Removal of cover/concealment surrounding asset such as billboards overlooking asset	Traffic management minimizing time spent moving slowly/ stopped on or near asset
Pedestrian-placed explosives	Pedestrian access restricted with fencing and signage	Increased CCTV Extensive Training of CCTV/ Help Truck Personnel Increased Patrols by Law Enforcement/Other Increased Lighting	Retrofit with blast mitigating materials Enclosure of abutment areas with access-controlled concrete walls	Decrease reliance on asset with alternative route construction
Vehicle Bombs	No Parking zones under bridges Signage	Increased CCTV Extensive training of CCTV/ Help Truck Personnel	Retrofit with blast mitigating materials Physically restrict vehicle access to bridge columns and abutments increasing standoff distances	Decrease reliance on asset with alternative route construction Incorporate blast mitigating designs in future bridge construction
Water-borne explosives	Signage	Increased CCTV Extensive training of CCTV/TDOT personnel Anti-Swimmer Technology	Retrofit with blast mitigating materials Physically restrict boating/swimming access to piers and columns to increase standoff distances	

Table 9: Example mitigation measures

\

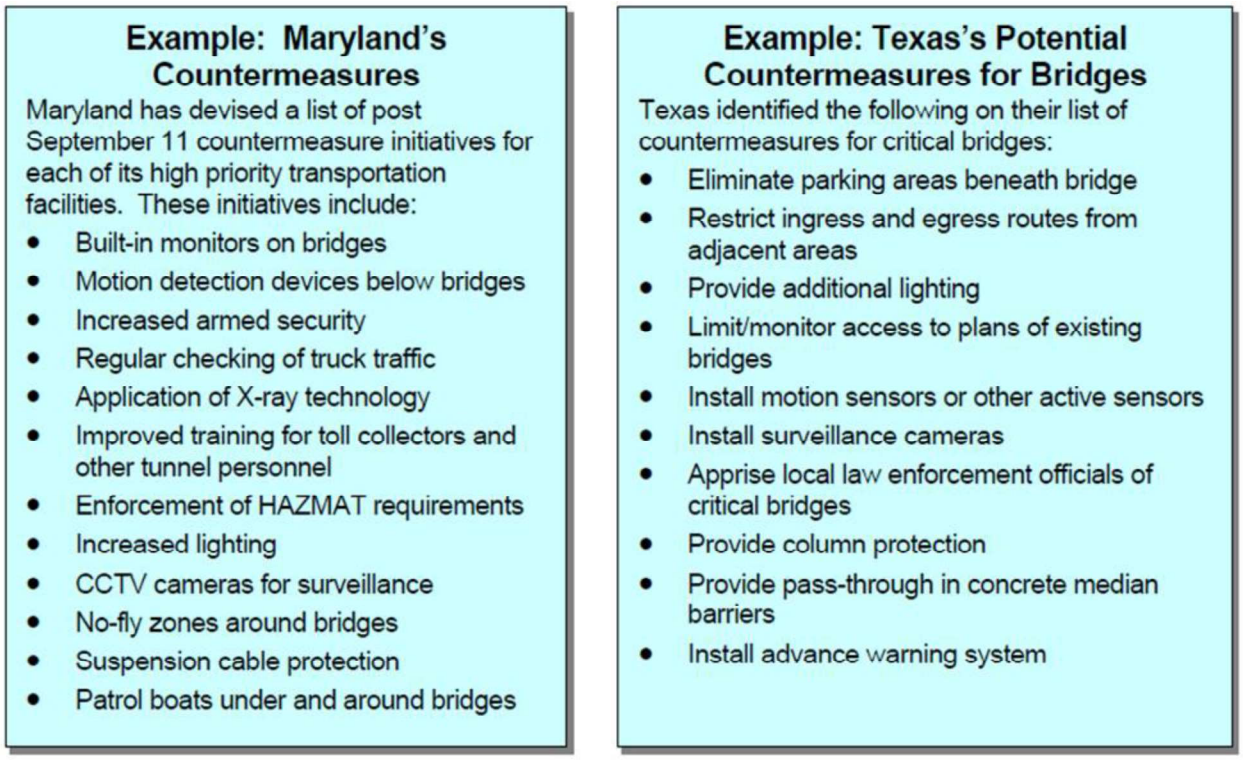


Figure 18: Example Mitigation Strategies [31]

In addition, each mitigation strategy should be weighed in reference to the following [11]:

Available Political Support - this step involves getting the necessary support from state authorities and also members of the affected community. Some mitigation efforts will be easily supported, while others may require substantial education and effort. For example, little community opposition would likely face the Department if it was decided to increase the training of CCTV and Help Truck personnel, but significant opposition to restricting under-bridge parking may be expected in some cases.

Community Acceptance - this step cannot be viewed separately from the need for political support. Both are necessary for the mitigation efforts' successful implementation. Some cases may require community-wide campaigns to explain the risks, reasons for, and expected benefits of mitigation measures.

Cost - Costs must be weighed for each mitigation measure to compare with benefits.

Benefits - The benefits of a mitigation measure may be clear-cut, as in the case of restricting vehicle access to bridge columns to outside the recommended standoff distances for the appropriate vehicles. Other mitigation measures may be less clear, such as if increased surveillance will be beneficial if the response mechanism (i.e. law enforcement) is not clearly defined for detected threats.

Available Financial Resources - After a cost/benefit analysis is performed and a Department "wish list" is developed, the financial resources available for the mitigation activity must be secured. Often, this process can involve getting/bolstering political support for the proposed activities. Some Federal and State programs may exist for financing mitigation activities.

Legal Authority - Sometimes a question may arise as to the legal authority of the Department to make mitigation improvements to an asset. For example, if restricting under-bridge vehicular access infringes on a business's employee parking, there could be some discussions needed to establish the legal authority to proceed.

Adversely Affected Population - Considerations of who the changes will affect adversely must be considered. For example, will the mitigation activities affect local boaters/ fishermen, tourists, or others?

Adverse Effects on the Already Built Environment - Some mitigation efforts may affect the already- built environment. For example:

- Effects on traffic/ vehicular mobility
- Effects on pedestrian mobility
- Effects on asset maintenance/ inspection activities
- Effects on aesthetics
- Potential interference with first responders

Impact on the Environment - Will the mitigation activity adversely affect nearby environmental assets such as protected natural resources etc.?

Technical Capacity - Will the proposed mitigation activities be handled by Department personnel, or is there the need for contractors to install or construct the mitigation measures? Will there be a need for specialized training or contractors to ensure the operation of the mitigation measure?

Funding for Maintenance and Operation - Will the mitigation activity require regular maintenance or operation? Will that maintenance and operation be handled by existing Department personnel, or will additional personnel be required?

Ease and Speed of Implementation - The relative ease and speed of implementation can also be deciding factors when choosing mitigation measures. It may be best to retrofit all of the identified assets with blast-mitigating materials, but would such a project be best when considered against the other alternatives from a speed/ease of implementation perspective?

Timeframe and Urgency - Which assets should receive quick attention? Risk assessment data can help, but a knowledge of the specific condition of the asset as well as any threats to the asset can affect the timeframe and urgency of the mitigation measures

needed. For example, the recent threat by supposed ISIS actors upon a bridge in Memphis might call for a fast timeframe, but the already-in place earthquake retrofits to bridge columns on the Desoto bridge may mitigate the risk sufficiently in the eyes of the Department to address other assets first.

Short Term Solutions/ Benefits - Are there short-term activities that can be accomplished while deciding on long-term solutions? For example, can Jersey barriers be placed to restrict vehicle under-bridge access while a more permanent, more aesthetically pleasing solution is decided?

Long Term Solutions/ Benefits - Would a long-term solution make more sense than taking costly short-term actions? In other words, if funding is not currently available for a long-term solution, will it be available soon enough to forego any short-term additional costs?

Estimating Costs - Once a pathway forward has been decided, then it is time to "sharpen the pencil" and engage in cost estimates. Sometimes this may take the form of engaging external consultants or Departmental planning of projects.

Life Cycle Cost Analysis - What will be the cost of the mitigation activity over its lifetime? Are other options available with better LCCAs? Is the asset in question up for a rebuild/ retrofit soon anyway? Would it make sense to roll a mitigation activity into the rebuild/retrofit activity?

Setting Priorities - What is the Department's order of priorities for mitigation activity? How does this mitigation activity fit in with broader Department priorities?

Discussion of Design Principles in Mitigation Activities

One of the mitigation activities that is discussed above is restriction of vehicular under-bridge access to increase standoff distances. From Ritter et. al.: [2]

> …vehicle and pedestrian access routes should be designed with security in mind, and specifically with the goal of keeping potential car and truck bombs as far away as possible from the exterior of the building [and bridge support columns, SIC]. This is paramount, because the dynamics behind the velocity of an explosion from a truck bomb dictate that the blast energy dramatically dissipates over even small distances, and even a relatively short area of separation can be the difference between a building [bridge, SIC] that is scarcely damaged and one that becomes unusable. (p. 107)

Commonly known as vehicle denial systems, these mitigation activities need not be aesthetically unpleasing. Some of the suggested more aesthetically pleasing vehicle denial systems are depicted below in figure 19:

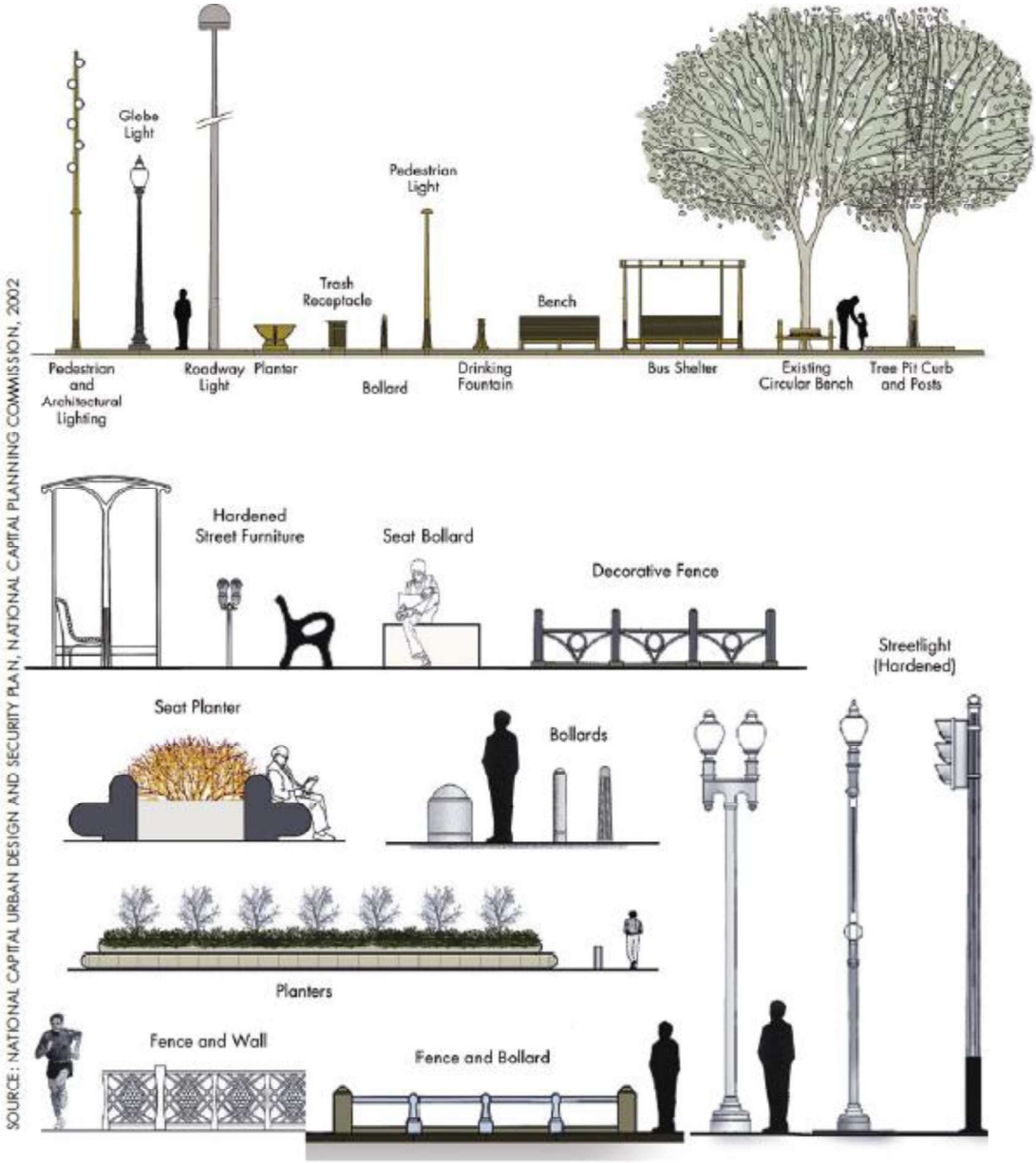


Figure 19: Some vehicle denial examples [14]

When designing vehicle denial systems, the fundamental design considerations are outlined below, in figure 20:

Barrier Design Considerations

The effectiveness of a barrier is based on the amount of energy it can absorb versus the amount of kinetic energy, *KE*, imparted by a head-on vehicle impact:

$$KE = \frac{Mv^2}{2}$$

where M is the mass of the vehicle and v is the velocity at the time of impact with the barrier. The angle of approach reduces this energy in non-head-on situations and the energy absorbed by the crushing of the bumper also reduces the energy imparted to the barriers. Because the velocity is squared in this equation, a change in velocity affects the result more than a change in vehicle weight. For this reason, it is important to review lines of approach to ensure that a vehicle does not have a long, straight road to pick up speed before impact.

The vehicle weight used for the design of barriers typically ranges from 4,000 pounds for cars up to 40,000 pounds for trucks. Impact velocities typically range from 30 mph for slanted impact areas (i.e., where the oncoming street is parallel to the curb) up to 50 mph where there is straight-on access (i.e., where the oncoming street is perpendicular to the curb).

Figure 20: Vehicle Denial Design Considerations [14]

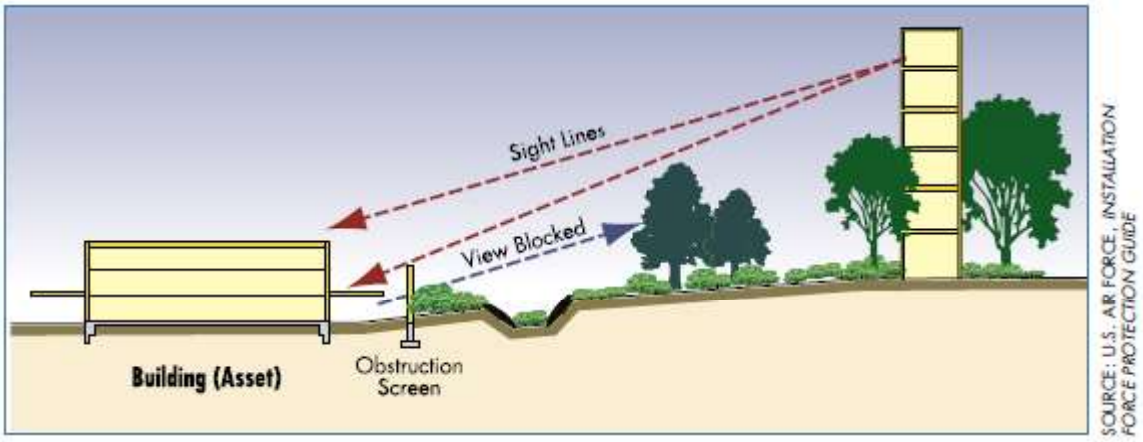


Figure 21: Example of Sight Line Denial to Deter Active Shooters

Discussion of the Role of Training and Exercises in Mitigation Activities

Terrorist attacks almost always involve pre-attack surveillance involved with them, and many include dry runs. The bad news is that intelligent terrorists can use the information gained to execute an effective attack on critical infrastructure. The good news is that each surveillance or dry run activity gives us the opportunity to detect potential terrorist activity. One relatively inexpensive way to reduce risk to the Department's assets is to train personnel (especially CCTV operations center employees and Help Truck operators) to recognize signs of terrorist surveillance.

Situational planning also plays a part. The Department should have a plan in place on how to handle suspected terrorist activity. Planning isn't the end of it, however. To fully gain the benefits of training and planning, exercises should be staged to walk Department personnel through the steps involved in responding to suspected terrorist activities. These exercises can be made up of everything from planned "table top" exercises where individuals sit around a table and play "what if" response games, to full-scale exercises that test the response of multiple agencies involved.

Conclusions

This All Hazards Risk Assessment began with the idea that all hazards would be evaluated in light of the identified assets. As it progressed, however, it became obvious that natural hazards were in effect planned for during the building of critical transportation infrastructure. In most cases, man- made accidental events were also accounted for, and it was assumed that the assets met a level of risk exposure to those accidental events during the design process. However, the terrorist threat is a changing environment, bringing with it an ever-changing matrix of players and threat vectors. This project, by necessity, has as its focus the man-made intentional events commonly called acts of terrorism. Acts of terrorism happen to also be the worst case scenario by which the RAMCAP process is performed. Because terrorist events were not actively considered in most of the assets' design, this remains the one area where TDOT can most affect the risk exposure of the State by implementing mitigation efforts.

Common vulnerabilities were found to be under-bridge access to columns and abutment areas, with some dangerous materials present at a few of the assets. The consequences of the loss of each asset were calculated to be considerable, both from a human impact and economic impact viewpoint. The worst case threat to the assets under examination was determined to be an attack by an al-Qaeda/ISIS - inspired domestic cell using active shooters or explosives. There are several mitigation activities discussed. Although not exhaustive, these mitigation activities can reduce the risk associated with each asset if deployed carefully using the recommended analytical procedures.

A wealth of information on blast resistant bridge design has been published, but increasing standoff distance from bridge columns and abutments to vehicle access remains the most effective means of defending against a terrorist attack on bridges. Some consideration to limiting access to small-arms fire was also discussed. Recent well-publicized terrorist threats to bridges in the State have called attention to the need to be prepared for the unfortunate eventuality of a terrorist attack. This risk assessment project is not the end of that process. Rather, it is the beginning of the work to be done to ensure that the critical

transportation infrastructure in the State of Tennessee and those people that watch over its well-being are prepared.

References:

[1] NCHRP. (2010). *NCHRP 645: Blast Resistant Highway Bridges: Design and Detailing Guidelines.* Washington, DC: NCHRP.

[2] Ritter, L., Barrett, J. M., & Wilson, R. (2007). *Securing Global Transportation Networks: A Total Security Management Approach.* New York: McGraw-Hill.

[3] Guerin, M. (2014, Dec 22). *FBI Bulletin Warns of Possible ISIS Terror Plot in Memphis*. Retrieved Jan 7, 2015, from MyFoxMemphis.com: http://www.myfoxmemphis.com/story/27688684/fbi-bulletin-warns-of-possible-isis-terror-plot-in-memphis

[4] United States Department of Homeland Security. (2013). *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience.* Retrieved Jan 9, 2015, from dhs.gov: http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[5] United States Department of Homeland Security. (2010). *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan.* Retrieved Jan 2, 2014, from dhs.gov: http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

[6] United States Department of Homeland Security. (2007). *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan.* Retrieved June 30, 2014, from http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

[7] UT Center for Business and Economic Research. (2011, Jan). *An Economic Report to the Governor of the State of Tennessee 2011.* Retrieved Jan 2, 2015, from utk.edu: http://www.tn.gov/ecd/pdf/Older_PDFs/Economic_Report_Governor.pdf

[8] United States Federal Highway Administration. (n.d.). *Major Freight Corridors*. Retrieved Jan 10, 2015, from fhwa.gov: http://ops.fhwa.dot.gov/freight/freight_analysis/freight_story/major.htm

[9] Tennessee Department of Transportation (n.d.). *tdot.state.tn.us*. Retrieved Jan 3, 2015, from Structures Division - Tennessee Bridge Facts: http://www.tdot.state.tn.us/chief_engineer/assistant_engineer_design/structures/facts.htm

[10] ASME Technologies Institute. (2009). *All-Hazards Risk and Resilience: Prioritizing Critical Infrastructure using the RAMCAP Plus Approach.* Washington, DC: ASME.

[11] Federal Emergency Management Association. (2005) *FEMA 452 Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings.* Retrieved Dec 12, 2014 from: https://www.fema.gov/what-mitigation/fema-452-risk-assessment-how-guide-mitigate-potential-terrorist-attacks-against

[12] Winget, D. G. (2005). Recommendations for Blast Design and Retrofit of Typical Highway Bridges. *6th International Bridge Engineering Conference: Reliability, Security, and Sustainability in Bridge Engineering, July 17-20, 2005*, 1-8.

[13] Williamson, E. B. (2005). Risk management and design of critical bridges for terrorist attack. *Journal of Bridge Engineering*, 96-106.

[14] Federal Emergency Management Association. (2003, Dec). *FEMA 426: Risk Management Series: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings.* Retrieved Dec 22, 2014, from FEMA.gov: http://www.fema.gov/media-library-data/20130726-1455-20490-7465/fema426_ch4.pdf

[15] Jenkins, B. M., & Butterworth, B. R. (2010). *Potential Terrorist Uses of Highway-Borne Hazardous Materials.* San Jose, California: Mineta Transportation Institute, College of Business, San Jose State University.

[16] National Transportation Safety Board. (1998, May 5). *Board Meeting: Collision and Fire of Tractor/Cargo Tank Semitrailer and Passenger Vehicle, Yonkers, New York, October 9, 1997*. Retrieved Dec 22, 2014, from ntsb.gov: http://www.ntsb.gov/news/events/Pages/Collision_and_Fire_of_TractorCargo_Tank_Semitrailer_and_Passenger_Vehicle_Yonkers_New_York_October_9_1997.aspx

[17] United States Department of Justice: Federal Bureau of Investigation. (2013, Sept 16). *A Study of Active Shooter Incidents in the United States between 2000 and 2013.* Retrieved Jan 2, 2013, from fbi.gov: http://www.fbi.gov/news/stories/2014/september/fbi-releases-study-on-active-shooter-incidents/pdfs/a-study-of-active-shooter-incidents-in-the-u.s.-between-2000-and-2013

[18] Department of Homeland Security, Federal Bureau of Investigation. (2013, Jan 10). *(U//FOUO): DHS-FBI Bulletin: Recent Active Shooter Incidents Highlight Need for Continued Vigilence*. Retrieved Jan 2, 2015, from publicintelligence.net: https://publicintelligence.net/dhs-fbi-bulletin-recent-active-shooters/

[19] United States National Counterterrorism Center. (2012, Aug 7). *(U//FOUO) Worldwide: IED Targeting of First Response Personnel-Tactics and Indicators*. Retrieved Jan 12, 2015, from publicintelligence.net: https://publicintelligence.net/nctc-first-responder-ieds/

[20] Texas Engineering Extension Service TEEX. (2009). *Enhanced Threat and Risk Assessment.* College Station, TX: Texas Engineering Extension Service.

[21] Bergen, P. a. (2010). *Assessing the Terrorist Threat: A Report of the Bipartisan Policy Center's National Security Preparedness Group.* Washington, DC: Bipartisan Policy Center.

[22] Southern Poverty Law Center. (n.d.). *Southern Poverty Law Center*. Retrieved 6 30, 2014, from splcenter.org: http://www.splcenter.org/

[23] Federal Bureau of Investigation. (n.d.). *Hate Crime - Overview*. Retrieved Nov 22, 2014, from fbi.gov: http://www.fbi.gov/about-us/investigate/civilrights/hate_crimes/overview

[24] Rivinius, J. (2014, July 30). *Sovereign citizen movement perceived as top terrorist threat* . Retrieved Jan 15, 2015, from start.umd.edu: http://www.start.umd.edu/news/sovereign-citizen-movement-perceived-top-terrorist-threat

[25] Shoemaker, J. (2012, Mar 27). *Significant Terrorism Events in the News: Feb. 21 - March 25, 2012*. Retrieved Apr 22, 2014, from start.umd.edu: http://www.start.umd.edu/news/significant-terrorism-events-news-feb-21-march-25-2012

[26] Sageman, M. (2003, July 9). *Statement of Marc Sageman to the National Commission on Terrorist Attacks Upon the United States*. Retrieved Jan 10, 2015, from govinfo.library.unt.edu: http://govinfo.library.unt.edu/911/hearings/hearing3/witness_sageman.htm

[27] Jehl, D. (1993, Feb 3). *CIA Nominee Wary of Budget Cuts*. Retrieved Jan 5, 2015, from nytimes.com: http://www.nytimes.com/1993/02/03/us/cia-nominee-wary-of-budget-cuts.html

[28] Bjelopera, J. a. (2010). *American Jihadist Terrorism: Combating a Complex Threat.* Washington, DC: Congressional Research Service.

[29] Schaeffer, C. (2015, Jan 9). *America's First Navy Seal Congressman Puts Obama Foreign Policy on Full Blast Over Islamic Terror*. Retrieved Jan 10, 2015, from IJReview.com: http://www.ijreview.com/2015/01/229910-navy-seal-congressman-puts-obamas-foreign-policy-blast-risk/

[30] United States Army. (2001). *FM 3-19.30 Physical Security.* Retrieved Jun 6, 2014, from wbdg.org: https://www.wbdg.org/ccb/ARMYCOE/FIELDMAN/fm31930.pdf

[31] SAIC. (2002, May). *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection.* Retrieved 1 12, 2015, from transportation.org: http://highwaytransport.transportation.org/Documents/NCHRP_B.pdf

[32] United States Federal Bureau of Investigation. (n.d.). *Indicators of Terrorist Activity: Stopping the Next Attack in the Planning Stages.* Retrieved Dec 3, 2014, from http://media.cygnus.com/files/cygnus/document/OFCR/2012/JAN/terroristindicators_10619278.pdf

[33] ArcGIS. (2012). *USA Population Density*. Retrieved 1 12, 2015, from arcgis.com: http://www.arcgis.com/home/webmap/viewer.html?webmap=a18f489521ba4a589762628893be0c13

[34] *Bridgehunter.com*. (n.d.). Retrieved 8 2013, from http://bridgehunter.com/

[35] HSPD-8. (2011, March 30). *Presidential Policy Directive 8*. Retrieved Dec 12, 2014, from dhs.gov: http://www.dhs.gov/presidential-policy-directive-8-national-preparedness

[36] Levine, M. (2015, Jan 11). *ISIS Renews Previous Calls for Attacks in West as Police Remain Vigilant*. Retrieved Jan 12, 2015, from abcnews.go.com: http://abcnews.go.com/US/isis-renews-previous-calls-attacks-west-police-remain/story?id=28151629

[37] Obama, B. (2013, Feb 12). *Presidential Policy Directive 21*. Retrieved Jan 5, 2015, from whitehouse.gov: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[38] Silber, M. a. (2007). *Radicalization in the West: The Homegrown Threat.* New York: The New York City Police Department.

[39] Tennessee Department of Transportation. (n.d.). *AADT Book 2012.* Retrieved 8 2013, from http://www.tdot.state.tn.us/projectplanning/adt.asp

[40] *Ugly Bridges.com*. (n.d., n.d.). Retrieved 8 2013, from http://www.uglybridges.com/

[41] United States Department of Homeland Security. (n.d.). *Definition of Terms*. Retrieved Dec 12, 2014, from dhs.gov: http://www.dhs.gov/definition-terms#0

[42] DHS. (2010). *DHS Risk Lexicon.* Retrieved Dec 30, 2014, from dhs.gov: http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

[43] U.S. Army. (2005, Sept 6). *U.S. Army Improvised Explosive Device (IED) Safe Standoff Distance Cheat Sheet*. Retrieved Jan 12, 2015, from publicintelligence.net: https://publicintelligence.net/u-s-army-improvised-explosive-device-ied-safe-standoff-distance-cheat-sheet/

[44] United States National Counter Terrorism Center. (2014) *Bomb Threat Standoff Distances*. Retrieved Jan 2, 2015 from: http://www.nctc.gov/site/technical/bomb_threat.html

[45] United States Department of Energy (2000) *Physical Security Systems Inspectors Guide*. Retrieved April 13, 2014 from: https://www.cccure.org/Documents/Physical_Security/Physical%20Security%20Systems%20Inspectors%20Guide.htm

[46] O'Rourke, T.D. (2007) *Critical Infrastructure, Dependencies, and Resilience*. Appearing in The Bridge: Linking Engineering and Society the Jouranal of the National Academy of Engineering, retrieved Dec 12, 2014 from: https://www.nae.edu/Publications/Bridge/EngineeringfortheThreatofNaturalDisasters/CriticalInfrastructureInterdependenciesandResilience.aspx

[47] UT Center for Business and Economic Research. (2014, Jan). *An Economic Report to the Governor of the State of Tennessee 2011.* Retrieved Jan 2, 2015, from utk.edu: http://cber.utk.edu/tefslist.htm

[48] United States Department of Transportation, Federal Highway Administration (2006, Mar) Multiyear Plan for Bridge and Tunnel Security Research, Development, and Deployment. Retrieved Oct 11, 2014 from: http://www.trb.org/main/blurbs/157304.aspx

[49] United States Federal Highway Administration (2003) *Recommendations for Bridge and Tunnel Security.* Retrieved Dec 3, 2014 from: http://www.fhwa.dot.gov/bridge/security/brp.pdf

[50] United States Department of Commerce, National Institute of Standards and Technology (2007) *A Guide to Printed and Electronic Resources for Developing a Cost-Effective Risk Mitigation Plan for New and Existing Constructed Facilities.* Retrieved Feb 24, 2014 from: http://fire.nist.gov/bfrlpubs/build07/art011.html

[51] Sbati, Haysaam and Roden, David (2010) *Best Practices for the use of Micro Simulation Models*. Retrieved June 7, 2014 from: http://statewideplanning.org/wp-content/uploads/259_NCHRP-08-36-90.pdf

[52] Schrank, David; Eisele, Bill; Lomax, Tim (2012) *TTI's 2012 Urban Mobility Report*. Retrieved Jan 2, 2015 from: http://mobility.tamu.edu/ums/

[53] Nashville Metropolitan Planning Organization (n.d.) *Freight Movement*. Retrieved Jan 20, 2015 from: http://www.nashvillempo.org/regional_plan/freight/

[54] Miller, Erin et. al. (2014, Dec) *Terrorist Attacks in the U.S. Between 1970 and 2013: Data from the Global Terrorism Database (GTD)*. National Consortium for the Study of Terrorism and Response to Terrorism (START) Retrieved Jun 22, 2014 from: https://www.start.umd.edu/pubs/Overview%20of%20Terrorist%20Attacks%20in%20the%20US%201970-2013_1.pdf

[55] Ligon, Gina et. al. (2014, Nov) *The Islamic State of Iraq and the Levant: Branding, Leadership Culture, and Lethal Attraction*. National Consortium for the Study of Terrorism and Response to Terrorism (START) Retrieved Jun 22, 2014 from: https://www.start.umd.edu/pubs/START_ISIL%20Branding%20Leadership%20Culture%20and%20Lethal%20Attraction_Ligon_Nov2014.pdf

[56] Bier, Vicki; Kosanoglu, Fuat (2014, Nov) *Target-oriented utility theory for modeling the deterrent effects ofcounterterrorism.* Retrieved Jan 20, 2015 from: http://www.sciencedirect.com/science/article/pii/S0951832014002786#

[57] LaFree, Gary, and Bianca E. Bersani. (2014) *County-Level Correlates of Terrorist Attacks in the United States*. Criminology & Public Policy (November): 1-27. http://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12092/abstract

[58] Smith, Brent L., and Paxton Roberts, Jeff Gruenewald, Brent Klein. (2014) *Patterns of Lone Actor Terrorism in the United States: Research Brief*. START College Park, MD. October. http://www.start.umd.edu/pubs/START_ATS_PatternsofLoneActorTerrorismUS_ResearchBrief.pdf

[59] Kruglanski, Arie W. (2014) *Psychology Not Theology: Overcoming ISIS' Secret Appeal*. October 28. http://www.e-ir.info/2014/10/28/psychology-not-theology-overcoming-isis-secret-appeal/.

[60] Miller, Erin, and Kathleen Smarick. (2014) *Profiles of Perpetrators of Terrorism in the United States: Research Highlight*. START College Park, MD. July. http://www.start.umd.edu/pubs/START_ProfilesofPerpetratorsofTerrorismintheUS_ResearchHighlight_July2014.pdf

[61] Gruenewald, Jeff, and Joshua D. Freilich, Steven M. Chermak, William S. Parkin. (2014, June) *Research Highlight: Violence Perpetrated by Supporters of al-Qa'ida and Affiliated Movements (AQAM): Fatal Attacks and Violent Plots in the United States*. Research Brief to the Resilient Systems Division, Science and Technology Directorate, U.S. Department of Homeland Security. College Park, MD: START, 2014. http://www.start.umd.edu/pubs/START_ECDB_ViolencePerpetratedbySupportersofAQAM_ResearchHighlight_June2014.pdf

[62] Simonelli, Corina. (2014) *The Evolution of the Islamic State of Iraq and the Levant (ISIL): Relationships 2004-2014.* START Fact Sheet. College Park, Maryland. June. http://www.start.umd.edu/pubs/START_EvolutionofISILRelationships_FactSheet_June2014.pdf

[63] Brachman, Jarret. (2014) *Transcending Organization: Individuals and 'The Islamic State'*. START Analytical Brief. College Park, Maryland. June. http://www.start.umd.edu/pubs/START_TranscendingOrganizationIndividualsandtheIslamicState_AnalyticalBrief_June2014.pdf

[64] McCauley, Clark, and Sophia Moskalenko, Benjamin Van Son. (2014) *Characteristics of Violent Lone-Offenders: A Comparison of Assassins and School Attackers.* START. College Park, MD. May. http://www.start.umd.edu/pubs/START_LoneActorViolentOffenderComparisonAssassinSchoolAttacker_May2014.pdf

[65] Miller, Erin, and Gary LaFree. (2014) *Country Reports on Terrorism 2013: Annex of Statistical Information*. National Consortium for the Study of Terrorism and Responses to Terrorism (START). April. http://www.state.gov/j/ct/rls/crt/2013/224831.htm

[66] Cutter, Susan L. (2013). *Building Disaster Resilience: Steps Toward Sustainability*. Challenges in Sustainability (Jan). http://econpapers.repec.org/article/lib000cis/v_3a1_3ay_3a2013_3ai_3a2_3ap_3a72-79.htm

[67] Binder, Markus, and Gary Ackerman. (2014) *Anatomizing Chemical Biological Non-State Adversaries*. https://www.start.umd.edu/pubs/STARTResearchBrief_Anatomizing.pdf

[68] Braniff, William. (2014) *Testimony before the United States House Armed Services Committee Hearing on the State of Al Qaeda, its Affiliates, and Associated Groups: View From Outside Experts*. Washington, DC: United States House of Representatives. (February): http://www.start.umd.edu/pubs/STARTCongressionalTestimony_StateofAQandAffiliates_WilliamBraniff.pdf.

[69] Jensen, Michael, Patrick James, and Herbert Tinsley. (2015) *Profiles of Individual Radicalization in the United States: Preliminary Findings*. January. https://www.start.umd.edu/pubs/PIRUS%20Research%20Brief_Jan%202015.pdf

[70] Jensen, Michael, Patrick James, and Herbert Tinsley. (2015) *Profiles of Individual Radicalization in the United States: An Empirical Assessment of Domestic Radicalization*. January. https://www.start.umd.edu/pubs/PIRUS%20Fact%20Sheet_Jan%202015.pdf

[71] Deloughery, Kathleen. (2013) *Simultaneous Attacks by Terrorist Organizations*. Perspectives on Terrorism (December): 79-89. http://terrorismanalysts.com/pt/index.php/pot/article/view/312

[72] Liu, Brooke, and Elizabeth Petrun. (2013) *Training in Risk and Crisis Communication Modules: Fact Sheet*. http://start.umd.edu/sites/default/files/publications/local_attachments/STARTFactSheet_TRACCModules_0.pdf

[73] Smith, Brent L., and Paxton Roberts, Kelly Damphousse. (2013) *Update on Geospatial Patterns of Antecedent Behavior among Perpetrators in the American Terrorism Study (ATS)*. Report to Resilient Systems Division, DHS Science and Technology Directorate. College Park, MD: START, 2013. http://start.umd.edu/pubs/START_IUSSD_GeospatialPatternsofAntecedentBehaviorAmongPerpetrators_October2013.pdf

[74] LaFree, Gary, and Stanley Presser, Roger Tourangeau, Amy Adamcyzk. (2013) *U.S. Attitudes toward Terrorism and Counterterrorism Before and After the April 2013 Boston Marathon Bombings*. October. www.start.umd.edu/start/publications/local_attachments/START_USAttitudesTowardTerrorismandCT_BeforeAfterBoston_Nov2013.pdf

[75] Asal, Victor, and Kathleen Deloughery, Ryan King. (2013) *Research Highlight: Understanding Lone-actor Terrorism -- A Comparative Analysis with Violent Hate Crimes and Group-based Terrorism*. College Park, MD. (October) http://www.start.umd.edu/pubs/START_UnderstandingLoneActorTerrorism_ResearchHighlight_Oct2013.pdf

[76] McCauley, C. & Moskalenko, S. (2013), Two possible profiles of lone-actor terrorists. Pp.84-91 in Hriar Cabayan, Valerie Sitterle, and Matt Yandura (Eds.), Looking Back, Looking Forward: Perspectives on Terrorism and Responses to It. Strategic Multi-layer Assessment Occasional White Paper, Department of Defense.

[77] Gelfand, Michele J, and Laura Severance, Lan Bui-Wrzosinska, Sarah Lyons, Andrzej Nowak, Wojciech Borkowski, Nazar Soomro, Naureen Soomro, Anat Rafaeli, Dorit Efrat Treister, Chun-Chi Lin, Susumu Yamaguchi. (2013) *The psychological structure of aggression across cultures* Journal of Organizational Behavior (April): 835-865. http://onlinelibrary.wiley.com/doi/10.1002/job.1873/abstract

[78] Ligon, Gina, and Daniel Harris, Mackenzie Harms, JoDee Friedly. (2013) *The Organization and Leadership of Violence*. August 26. http://www.start.umd.edu//pubs/START_OrganizationandLeadershipofViolence_ResearchBrief_Aug2013.pdf

[79] Dugan, Laura. (2013) *Thinking Beyond Deterrence*. April. www.start.umd.edu/news/discussion-point-thinking-beyond-deterrence

[80] Chermak, Steven, and Joshua Freilich, Celinet Duran, William Parkin. (2013) *An Overview of Bombing and Arson Attacks by Environmental and Animal Rights Extremists in the United States*, *1995-2010*. April. http://www.start.umd.edu/sites/default/files/files/publications/START_BombingAndArsonAttacksByEnvironmentalAndAnimalRightsExtremists_May2013.pdf

[81] Deloughery, Kathleen, Ryan D. King, Victor Asal, and R. Karl Rethemeyer. (2012) *Analysis of Factors Related to Hate Crime and Terrorism.* National Consortium for the Study of Terrorism and Responses to Terrorism (December): http://www.start.umd.edu/sites/default/files/files/publications/START_AnalysisofFactorsRelatedtoHateCrimeandTerrorism.pdf

[82] Jones, Seth (2014) *A Persistant Threat: The Evolution of Al'Qaida and other Salafi Jihadists*. Rand Corporation National Defense and Research Institute: http://www.rand.org/pubs/research_reports/RR637.html

[83] Finucane, Melissa; Clancy, Noreen; Willis, Henry H.; Knopman, Debra (2014) *The Hurricane Sandy Rebuilding Task Force's Infrastructure Resilience Guidelines: An Initial Assessment of Implementation by Federal Agencies*. Rand Corporation Homeland Security and Defense Center: http://www.rand.org/pubs/research_reports/RR637.html

[84] Jenkins, Brian Michael (2014) *When Jihadis Come Marching Home: The Terrorist Threat Posed by Westerners Returning from Syria and Iraq*. Rand Corporation: http://www.rand.org/pubs/perspectives/PE130.html

[85] Jenkins, Brian Michael; Liepman, Andrew; Willis, Henry H; (2014) *Identifying Enemies Among Us: Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing.* The Rand Corporation: http://www.rand.org/pubs/conf_proceedings/CF317.html

[86] Jenkins, Brian Michael (2011) *Stray Dogs and Virtual Armies: Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11*. Rand Corporation: http://www.rand.org/pubs/occasional_papers/OP343.html

[87] Perry, Walter L.; Berrebi, Claude; Brown, Ryan Andrew; Hollywood, John; Jaycocks, Amber; Roshan, Parisha; Sullivan, Thomas; Miyashiro, Lisa (2013) *Predicting Suicide Attacks: Integrating Spatial, Temporal, and Social Features of Terrorist Attack Targets*. Rand Corporation Homeland Security and Defense Center: http://www.rand.org/pubs/monographs/MG1246.html

[88] Jenkins, Brian Michael (2015) *Eight Lessons from the Charlie Hebdo Attacks*. Slate.com: http://www.slate.com/articles/news_and_politics/foreigners/2015/01/_8_lessons_from_charlie_hebdo_attack_what_we_have_learned_about_the_terrorists.html

[89] Kingman, Arizona Historic District (n.d.) *The Disaster Story*. July 5, 1973 propane rail car explosion. http://kingmanhistoricdistrict.com/points-of-interest/firefighters-memorial-park/the-disaster-story.htm

Appendix A: Key Definitions

Absolute Risk - level of risk expressed with standard units of measurement that allows for independent interpretation without comparison to estimates of other risks. The absolute risk value of a scenario has a meaningful independent interpretation in contrast to relative risk that is meaningful only in comparison to other similarly constructed risk values. Can be measured using annualized lives lost, expected economic impact, or other metrics but it is not a ratio of risks. Can measure absolute level of risk pre-or post-risk reduction measures. (DHS, 2010)

Acceptable Risk - level of risk at which, given costs and benefits associated with risk reduction measures, no action is deemed to be warranted at a given point in time. (DHS, 2010)

Access Control - A Crime Prevention through Environment design (CPTED) design principle incorporating alternatives to traditional physical security concepts (i.e., locks, barriers, badge/ID systems) such as sidewalks, gates, lighting, and landscaping. It seeks to reduce criminal access to sensitive areas and increases natural surveillance to restrict criminal intrusion. This is especially true of areas not easily observed. (TEEX, 2009, pp. B-2)

Access controls (physical security context) - Refers to any portion of a security system that serves to limit the intruder access to, limit/prevent introduction of a WMD into a potential target. Examples include physical barriers, entrance controls, employee controls, visitor, vendor, or contractor controls, sensors, etc. Designed to protect critical assets. (TEEX, 2009, pp. B-2)

Accidental Hazard - source of harm or difficulty created by negligence, error, or unintended failure. (DHS, 2010)

Active Sensors - Sensors that both transmit and receive; examples include acoustic, radio frequency, infrared, and microwave sensors. (TEEX, 2009, pp. B-2)

Activity Support - A Crime Prevention through Environment Design (CPTED) design principle using the presence of activity planned for a given space. It involves placing activity into an area where individuals engaged in the activity will become part of the natural surveillance system. Examples include placing safe activities in areas that will discourage potential offenders. Another idea involves relocating higher risk activities to safer areas. (TEEX, 2009, pp. B-2)

Actual Occurrence - any natural, technological, national security or terrorism incident that has happened in the jurisdiction in question for which a coordinated emergency response or recovery operation was required. This includes both large-scale incidents that have resulted in a presidential declaration of emergency or major disaster and those occurrences of a lesser magnitude which require significant state and/or local response and recovery activities. (TEEX, 2009, pp. B-2)

Adaptive Risk - category of risk that includes threats intentionally caused by humans. Adaptive risks can include insider threats, civil disturbances, terrorism, or transnational crime. Those threats are caused by

people that can change their behavior or characteristics in reaction to prevention, protection, response, or recovery measures taken. (DHS, 2010)

Adversary - individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. An adversary can be hypothetical for the purposes of training, exercises, red teaming, and other activities. An adversary differs from a threat in that an adversary may have the intent, but not the capability, to conduct detrimental activities, while a threat possesses both intent and capability. (DHS, 2010)

After Action Report or After Action Review (AAR) - A structured review process that allows training participants to discover for themselves what happened, why it happened, and how it can be done better. The AAR is a summary of joint universal lessons learned and describes a real world operation or training exercise and identifies significant lessons learned. (TEEX, 2009, pp. B-2)

All-Hazards - An approach for prevention, protection, preparedness, response, and recovery that addresses a full range of threats and hazards, including domestic terrorist attacks, natural and manmade disasters, accidental disruptions, and other emergencies. (TEEX, 2009, pp. B-2)

Asset - Contracts, facilities, property, electronic and non-electronic records and documents, unobligated or unexpended balances of appropriations, and other funds or resources other than personnel. (TEEX, 2009, pp. B-3)

Attack Method - manner and means, including the weapon and delivery method, an adversary may use to cause harm on a target. Attack method and attack mode are synonymous. (DHS, 2010)

Attack Path - steps that an adversary takes or may take to plan, prepare for, and execute an attack. An attack path may include recruitment, radicalization, and training of operatives, selection and surveillance of the target, construction or procurement of weapons, funding, deployment of operatives to the target, execution of the attack, and related post-attack activities. (DHS, 2010)

Baseline Risk - current level of risk that takes into account existing risk mitigation measures. Often, the word ―risk‖ is used to imply ―baseline risk‖ with the unstated understanding that the reference is the current circumstances. It should not be confused with risk as a measurement, which can change with the substitution of different variables. (DHS, 2010)

Biological Agent - Living organisms or the materials derived from them (such as bacteria, viruses, fungi, and toxins) that cause disease in or harm to humans, animals, or plants, or cause deterioration of material. (TEEX, 2009, pp. B-4)

Biological Warfare Agent - Living organisms or their derivatives that can be used in weapons to cause incapacitation or death. Biological agents have the ability to reproduce themselves, thus they are less predictable than chemical agents. (TEEX, 2009, pp. B-4)

Blast Effects - When a high explosive detonates, the solid or liquid explosive material is converted into mostly gaseous product. These extremely hot gases expand immediately and compress the air around the charge to form a blast wave. By definition, an explosion is the rapid expansion of gases accompanied by heat, light, and a loud noise. (TEEX, 2009, pp. B-4)

Capabilities-Based Planning - Capabilities-based planning is all-hazards planning. The Goal's approach focuses efforts on identifying and developing the critical capabilities from the Department of Homeland Security's (DHS) Task Capability List (TCL) to perform the critical tasks from the Universal Task List for the National Planning Scenarios. The Scenarios provide common planning factors in terms of the potential scope, magnitude, and complexity of major events that will help to determine the target levels of capability required and apportion responsibility among all potential partners. DHS believes that developing appropriate capabilities to address this range of scenarios will best prepare the Nation for terrorist attacks, major disasters, and other emergencies. (TEEX, 2009, pp. B-4)

Capability - means to accomplish a mission, function, or objective. Adversary capability is one of two elements, the other being adversary intent, that are commonly considered when estimating the likelihood of terrorist attacks. Adversary capability is the ability of an adversary to attack with a particular attack method. Other COIs may use capability to refer to any organization's ability to perform its mission, activities, and functions. (DHS, 2010)

Consequence - effect of an event, incident, or occurrence. Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment. (DHS, 2010)

Consequence Assessment - product or process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence. (DHS, 2010)

Countermeasure - action, measure, or device intended to reduce an identified risk. A countermeasure can reduce any component of risk -threat, vulnerability, or consequence. (DHS, 2010)

Covert Tactics - Those tactics involving stealth entry or using false identification. (TEEX, 2009, pp. B-6)

Crime Prevention Through Environment Design (CPTED) - CPTED is separate from, but complimentary to, facility hardening and security engineering. It considers design of an area so that it enhances the needs of legitimate users of the space while still providing security measures. CPTED is defined by five overlapping principles: territoriality, natural surveillance, access control, activity support, and maintenance. (TEEX, 2009, pp. B-6)

Criticality - importance to a mission or function, or continuity of operations. (DHS, 2010)

Criticality Assessment - product or process of systematically identifying, evaluating, and prioritizing based on the importance of an impact to mission(s), function(s), or continuity of operations. (DHS, 2010)

Critical Incident Stress Management (CISM) - A formal program designed to reduce the psychological impact of the incident and educate the emergency responders and the public about stress and ways to deal with it by alleviating adverse reactions to a catastrophic incident such as a WMD/terrorism mass casualty incident. The program's professional counseling services focus on the emergency responders during the response phase of the incident (defusing sessions) and the emergency responders and incident victims through support groups and outreach seminars that assist in handling grief and stress. (TEEX, 2009, pp. B-5)

Decision Analysis - techniques, body of knowledge, and professional practice used to provide analytical support for making decisions through a formalized structure. Decision analysis can be used in the context of risk analysis to evaluate complex risk management decisions. Decision analysis can be applied to strategic, operational, and tactical decisions. (DHS, 2010)

Design-Basis Threat - The specific vulnerability by which assessment and corrective actions are measured; it is the specific threat to which one is adapting physical and operational changes at a facility. (TEEX, 2009, pp. B-8)

Deterrent - measure that discourages, complicates, or delays an adversary's action or occurrence by instilling fear, doubt, or anxiety. A deterrent reduces threat by decreasing the likelihood that an attack (or illegal entry, etc.) will be attempted. One form of deterrent is a prospective punitive action intended to discourage the adversary from acting (e.g., massive nuclear retaliation, Mutual Assured Destruction during the Cold War, or prison for conventional crimes). Another form of deterrent is a measure or set of measures that affects the adversary's confidence of success (e.g., fences, border patrols, checkpoints). A deterrent may cause an adversary to abandon plans to attempt an attack (or illegal entry, etc). A deterrent may cause the adversary to react by "threat shifting" in any of several domains: shift in time (delay); shift in target; shift in resources (additional resources); and/or a shift in plan or method of attack. Resilience, in terms of both critical economic systems and infrastructure and in societal resilience (e.g., the famed British ―stiff upper lip‖ of WWII, advance preparation for effective consequence reduction response operations, etc.), also has a potential deterrent value achieved when terrorist groups perceive that the strategic impact they seek through a particular attack or type of attack will not be achieved. (DHS, 2010)

Direct Consequence - effect that is an immediate result of an event, incident, or occurrence. Direct consequences can include injuries, loss of life, on-site business interruption, immediate remediation costs, and damage to property and infrastructure as well as to the environment. The distinction between direct and indirect consequences is not always clear, but what matters in risk analysis is a) capturing the likely effects – be they designated as direct or indirect – that should be part of the analysis, b) clearly defining what is contained as part of direct consequences and what is part of indirect consequences, and c) being consistent across the entire analysis. Such consistency and clarity is important for comparability across scenarios and risk analyses. (DHS, 2010)

Domestic Terrorism - Involves groups or individuals who are based and operate widely within the United Sates and are directed at elements of our government or population without foreign direction. (TEEX, 2009, pp. B-9)

Drills - A drill is a coordinated, supervised activity usually employed to test a single, specific operation or function in a single agency or organizational entity. Drills are commonly used to provide training on new equipment, develop or test new policies or procedures, or practice and maintain current skills. Typical attributes of drills include the following:

- Narrow focus, measured against established standards
- Instant feedback
- Realistic environment
- Performance in isolation (TEEX, 2009, pp. B-9)

Economic Consequence - effect of an incident, event, or occurrence on the value of property or on the production, trade, distribution, or use of income, wealth, or commodities. When measuring economic consequence in the context of homeland security risk, consequences are usually assessed as negative and measured in monetary units. (DHS, 2010)

Emergency - Absent a Presidentially declared emergency, any incident(s), human-caused or natural, that requires responsive action to protect life or property. Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, an emergency means any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement state and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States. (TEEX, 2009, pp. B-10)

Emergency Management Agency (EMA) - Organizations that are directed to coordinate preparedness, recovery, and mitigation for CBRNE/All-hazards terrorism incidents at the jurisdiction level. (TEEX, 2009, pp. B-10)

Emergency Operations Centers (EOC) - The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., Federal, State, regional, county, city, tribal), or some combination thereof. (TEEX, 2009, pp. B-10)

Emergency Operations Plan (EOP) - A planning document that 1) assigns responsibility to organizations and individuals for implementing specific actions at projected times and places in an emergency that exceeds the capability or routine responsibility of any one agency; 2) sets forth lines of authority and organizational relationships, and shows how all actions will be coordinated; 3) identifies personnel, equipment, facilities, supplies, and other resources available for use during response and recovery operations; and 4) identifies steps to address mitigation issues during response and recovery activities. (TEEX, 2009, pp. B-10)

Emergency Responder - Local police, emergency medical services, emergency management services, fire service, hazardous material services, public works, governmental administrative personnel, public safety communication, healthcare personnel, and public health agencies who, during an incident, take action to save lives, protect property, and meet basic human needs. (TEEX, 2009, pp. B-10)

Event Tree - graphical tool used to illustrate the range and probabilities of possible outcomes that arise from an initiating event. (DHS, 2010)

Fault Tree - graphical tool used to illustrate the range, probability, and interaction of causal occurrences that lead to a final outcome. (DHS, 2010)

Frequency - number of occurrences of an event per defined period of time or number of trials. (DHS, 2010)

Frequentist Probability- interpretation or estimate of probability as the long-run frequency of the occurrence of an event as estimated by historical observation or experimental trials. (DHS, 2010)

Game Theory - branch of applied mathematics that models interactions among agents where an agent's choice and subsequent success depend on the choices of other agents that are simultaneously acting to maximize their own results or miminize their losses. (DHS, 2010)

Hazard - natural or man-made source or cause of harm or difficulty. A hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed. A hazard can be actual or potential. (DHS, 2010)

Hazardous Materials (HazMat) - Any material that is explosive, flammable, poisonous, corrosive, reactive, or radioactive, or any combination thereof, and requires special care in handling because of the hazards it poses to public health, safety, and/or the environment. Any hazardous substance under the Clean Water Act, or any element, compound, mixture, solution, or substance designated under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA); any hazardous wasted under the Resource Conservation and Recovery Act (CAR); any toxic pollutant listed under pretreatment provisions of the Clean Water Act; any hazardous pollutant under Section 112 of the Clean Air Act; or any imminent hazardous chemical substance for which the administrator has taken action under the Toxic Substances Control Act (TOSCA) Section 7. (TEEX, 2009, pp. B-13)

Human Consequence - effect of an incident, event, or occurrence that results in injury, illness, or loss of life. When measuring human consequence in the context of homeland security risk, consequence is assessed as negative and can include loss of life or limb, or other short-term or long-term bodily harm or illness. (DHS, 2010)

Incident - occurrence, caused by either human action or natural phenomena, that may cause harm and that may require action. Homeland security incidents can include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, law enforcement encounters and other occurrences requiring a mitigating response. Harm can include human casualties, destruction of property, adverse economic impact, and/or damage to natural resources. (DHS, 2010)

Indirect Consequence - effect that is not a direct consequence of an event, incident, or occurrence, but is caused by a direct consequence, subsequent cascading effects, and/or related decisions. Examples of indirect consequences can include the enactment of new laws, policies, and risk mitigation strategies or investments, contagion health effects, supply-chain economic consequences, reductions in property values, stock market effects, and long-term cleanup efforts. Accounting for indirect consequences in risk assessments is important because they may have greater and longer-lasting effects than the direct consequences. Indirect consequences are also sometimes referred to as ripple, multiplier, general equilibrium, macroeconomic, secondary, and tertiary effects. The distinction between direct and indirect consequences is not always clear but what matters in risk analysis is a) capturing the likely effects – be they designated as direct or indirect – that should be part of the analysis, b) clearly defining what is contained as part of direct consequences and what is part of indirect consequences, and c) being consistent across the entire analysis. Such consistency and clarity is important for comparability across scenarios and risk analyses. Induced consequences are occasionally estimated separately from indirect consequences but should be contained within indirect estimates. (DHS, 2010)

Infrastructure - The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (TEEX, 2009, pp. B-15)

Integrated Risk Management - structured approach that enables the distribution and employment of shared risk information and analysis and the synchronization of independent yet complementary risk management strategies to unify efforts across the enterprise. (DHS, 2010)

Intent - a state of mind or desire to achieve an objective. Adversary intent is the desire or design to conduct a type of attack or to attack a type of target. Adversary intent is one of two elements, along with adversary capability, that is commonly considered when estimating the likelihood of terrorist attacks and often refers to the likelihood that an adversary will execute a chosen course of action or attempt a particular type of attack. (DHS, 2010)

Intentional Hazard - source of harm, duress, or difficulty created by a deliberate action or a planned course of action. (DHS, 2010)

Jurisdiction - A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, tribal, State, or Federal boundary lines) or functional (e.g., law enforcement, public health). (TEEX, 2009, pp. B-16)

Key Resources - As defined in the Homeland Security Act, key resources are publicly-controlled or privately-controlled resources essential to the minimal operations of the economy and government. (TEEX, 2009, pp. B-16)

Mission Consequence - effect of an incident, event, operation, or occurrence on the ability of an organization or group to meet a strategic objective or perform a function. Valuation of mission consequence should exclude other types of consequences (e.g., human consequence, economic consequence, etc.) if they are evaluated separately in the assessment. (DHS, 2010)

Mitigation - refers to those capabilities necessary to reduce loss of life and property by lessening the impact of disasters. Mitigation capabilities include, but are not limited to, community-wide risk reduction projects; efforts to improve the resilience of critical infrastructure and key resource lifelines; risk reduction for specific vulnerabilities from natural hazards or acts of terrorism; and initiatives to reduce future risks after a disaster has occurred. (HSPD-8, 2011)

Model - approximation, representation, or idealization of selected aspects of the structure, behavior, operation, or other characteristics of a real-world process, concept, or system. (DHS, 2010)

National Preparedness - refers to the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. (HSPD-8, 2011)

Natural Hazard - source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena. (DHS, 2010)

Normalized Risk - measure of risk created by mathematically adjusting a value in order to permit comparisons. (DHS, 2010)

Non-adaptive Risk - category of risk that includes threats caused by natural and technological hazards. (DHS, 2010)

Operational Risk - risk that has the potential to impede the successful execution of operations. (DHS, 2010)

Prevention - refers to those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. Prevention capabilities include, but are not limited to, information sharing and warning; domestic counterterrorism; and preventing the acquisition or use of weapons of mass destruction (WMD). For purposes of the prevention framework called for in this directive, the term "prevention" refers to preventing imminent threats. (HSPD-8, 2011)

Probabilistic Risk Assessment - type of quantitative risk assessment that considers possible combinations of occurrences with associated consequences, each with an associated probability or probability distribution. (DHS, 2010)

Probability - numerical value between zero and one assigned to a random event (which is a subset of the sample space) in such a way that the assigned number obeys three axioms: (1) the probability of the random event ―A‖ must be equal to, or lie between, zero and one; (2) the probability that the outcome is within the sample space must equal one; and (3) the probability that the random event ―A‖ or ―B‖

occurs must equal the probability of the random event ―A‖ plus the probability of the random event ―B‖ for any two mutually exclusive events. (DHS, 2010)

Protection - refers to those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. Protection capabilities include, but are not limited to, defense against WMD threats; defense of agriculture and food; critical infrastructure protection; protection of key leadership and events; border security; maritime security; transportation security; immigration security; and cybersecurity. (HSPD-8, 2011)

Psychological Consequence - effect of an incident, event, or occurrence on the mental or emotional state of individuals or groups resulting in a change in perception and/or behavior. (DHS, 2010)

Recovery - refers to those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources. (HSPD-8, 2011)

Redundancy - additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process. (DHS, 2010)

Relative Risk - measure of risk that represents the ratio of risks when compared to each other or a control. (DHS, 2010)

Residual Risk - risk that remains after risk management measures have been implemented. (DHS, 2010)

Resilience - refers to the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies. (HSPD-8, 2011)

Response - refers to those capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. (HSPD-8, 2011)

Risk - potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. Risk is defined as the potential for an unwanted outcome. This potential is often measured and used to compare different future situations.
Risk may manifest at the strategic, operational, and tactical levels. For terrorist attacks or criminal activities, the likelihood of an incident, event, or occurrence can be estimated by considering threats and vulnerabilities. (DHS, 2010)
Risk Acceptance - explicit or implicit decision not to take an action that would affect all or part of a particular risk. (DHS, 2010)

Risk Analysis - systematic examination of the components and characteristics of risk. In practice, risk analysis is generally conducted to produce a risk assessment. Risk analysis can also involve aggregation of the results of risk assessments to produce a valuation of risks for the purpose of informing decisions. In

addition, risk analysis can be done on proposed alternative risk management strategies to determine the likely impact of the strategies on the overall risk. (DHS, 2010)

Risk Assessment - product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making. (DHS, 2010)

Risk Avoidance - strategies or measures taken that effectively remove exposure to a risk. Risk avoidance is one of a set of four commonly used risk management strategies, along with risk control, risk acceptance, and risk transfer. (DHS, 2010)

Risk Communication - Definition: exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to act appropriately in response to an identified risk. Risk communication is practiced for both non-hazardous conditions and during incidents. During an incident, risk communication is intended to provide information that fosters trust and credibility in government and empowers partners, stakeholders, and the public to make the best possible decisions under extremely difficult time constraints and circumstances. (DHS, 2010)

Risk Control - deliberate action taken to reduce the potential for harm or maintain it at an acceptable level. (DHS, 2010)

Risk Data - information on key components of risk that are outputs of or inputs to risk assessments and risk analyses. (DHS, 2010)

Risk Governance - actors, rules, practices, processes, and mechanisms concerned with how risk is analyzed, managed, and communicated. (DHS, 2010)

Risk Identification - process of finding, recognizing, and describing potential risks. (DHS, 2010)

Risk Indicator - measure that signals the potential for an unwanted outcome as determined by qualitative or quantitative analysis. (DHS, 2010)

Risk Management - process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken. Effective risk management improves the quality of decision making. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to control risk. (DHS, 2010)

Risk Management Alternatives Development - process of systematically examining risks to develop a range of options and their anticipated effects for decision makers. (DHS, 2010)

Risk Management Cycle - sequence of steps that are systematically taken and revisited to manage risk. (DHS, 2010)

Risk Management Plan - document that identifies risks and specifies the actions that have been chosen to manage those risks. (DHS, 2010)

Risk Management Strategy - course of action or actions to be taken in order to manage risks. Proactive approach to reduce the usually negative impacts of various risks by choosing within a range of options that include complete avoidance of any risk that would cause harm or injury, accepting the risk, controlling the risk by employing risk mitigation options to reduce impacts, or transferring some or all of the risk to another entity based on a set of stated priorities. (DHS, 2010)

Risk Matrix - tool for ranking and displaying components of risk in an array. (DHS, 2010)

Risk Mitigation - application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences. (DHS, 2010)

Risk Mitigation Option - measure, device, policy, or course of action taken with the intent of reducing risk. (DHS, 2010)

Risk Perception - subjective judgment about the characteristics and/or severity of risk. Risk perception may be driven by sense, emotion, or personal experience. (DHS, 2010)

Risk Profile - description and/or depiction of risks to an entity, asset, system, network, or geographic area. A risk profile can be derived from a risk assessment; it is often used as a presentation tool to show how risks vary across comparable entities. (DHS, 2010)

Risk Reduction - decrease in risk through risk avoidance, risk control, or risk transfer. Risk reduction may be estimated during both the decision and evaluation phases of the risk management cycle. Risk reduction can be accomplished by reducing vulnerability and/or consequences (damages). (DHS, 2010)

Risk Score - numerical result of a semi-quantitative risk assessment methodology. (DHS, 2010)

Risk Tolerance - degree to which an entity, asset, system, network, or geographic area is willing to accept risk. (DHS, 2010)

Risk Transfer - action taken to manage risk that shifts some or all of the risk to another entity, asset, system, network, or geographic area. 1) Risk transfer may refer to transferring the risk from asset to asset, asset to system, or some other combination, or shifting the responsibility for managing the risk from one authority to another (for example, responsibility for economic loss could be transferred from a homeowner to an insurance company). Risk transfer is one of a set of four commonly used risk management strategies, along with risk control, risk acceptance, and risk avoidance. (DHS, 2010)

Scenario - hypothetical situation comprised of a hazard, an entity impacted by that hazard, and associated conditions including consequences when appropriate. A scenario can be created and used for the purposes of training, exercise, analysis, or modeling as well as for other purposes. A scenario that has occurred or is occurring is an incident. (DHS, 2010)

Security - refers to the protection of the Nation and its people, vital interests, and way of life. (HSPD-8, 2011)

Social Amplification of Risk - distortion of the seriousness of a risk caused by public concern about the risk and/or about an activity contributing to the risk. Describes the phenomenon by which hazards interact with psychological, social, institutional, and cultural processes in ways that may amplify or attenuate the public's perceived level of risk. The social amplification of risk phenomenon is the subject of a field of study that seeks to systematically link the technical assessment of risk with sociological perspectives of risk perception and risk-related behavior. (DHS, 2010)

Subject Matter Expert - individual with in-depth knowledge in a specific area or field. (DHS, 2010)

Subjective Probability - interpretation or estimate of probability as a personal judgment or ―degree of belief‖ about how likely a particular event is to occur, based on the state of knowledge and available evidence. Like all probabilities, subjective probability is conventionally expressed on a scale from zero to one where zero indicates the event is impossible and one indicates the event has or certainly will occur. Within the subjective probability interpretation, it is possible to estimate probabilities of events (using experts or models) that have not previously occurred or that have only rarely occurred, such as acts of terrorism. However, because subjective probabilities incorporate historical or trial data when available, the subjective probability will approximate the frequentist probability as data becomes more plentiful. Subjective probability is currently one of the most common uses of probability among statisticians and the risk analysis community. Bayesian probability is colloquially used as a synonym for subjective probability. In statistical usage, Bayesian probabilistic inference is an approach to statistical inference that employs Bayes' theorem to revise prior information using evidence. (DHS, 2010)

System - any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (DHS, 2010)

Target - asset, network, system or geographic area chosen by an adversary to be impacted by an attack. (DHS, 2010)

Threat - natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Threat as defined refers to an individual, entity, action, or occurrence; however, for the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest. (DHS, 2010)

Threat Assessment - product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property. (DHS, 2010)

Threat Shifting - response of adversaries to perceived countermeasures or obstructions, in which the adversaries change some characteristic of their intent to do harm in order to avoid or overcome the countermeasure or obstacle. (DHS, 2010)

Value of Statistical Life - amount people are willing to pay to reduce risk so that on average one less person is expected to die from the risk. The VSL is not intended to value very large reductions in mortality risk or place a value on the lives of identified individuals. VSL measures the monetized value of small reductions in mortality risk for a large number of people. For example, a countermeasure that reduces the annual risk of death by one in a million for 20 million people will, on average, save 20 lives a year. If the VSL is estimated at $5 million, the value of this mortality risk reduction is $100 million (20 expected lives saved times $5 million per life). Most VSL estimates are based on studies of the wage compensation for occupational hazards or studies that elicit people's willingness to pay for mortality risk reduction directly. (DHS, 2010)

Vulnerability - physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard. Characteristic of design, location, security posture, operation, or any combination thereof, that renders an entity, asset, system, network, or geographic area susceptible to disruption, destruction, or exploitation (DHS, 2010)

Vulnerability Assessment - product or process of identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards. (DHS, 2010)