Risk Analysis, Vol. 27, No. 5, 2007 DOI: 10.1111/j.1539-6924.2007.00955.x

Risk Analysis for Critical Asset Protection

William L. McGill,[1] Bilal M. Ayyub,[1]* and Mark Kaminskiy[1]

This article proposes a quantitative risk assessment and management framework that supports strategic asset-level resource allocation decision making for critical infrastructure and key resource protection. The proposed framework consists of five phases: *scenario identification*, *consequence and criticality assessment*, *security vulnerability assessment*, *threat likelihood assessment*, and *benefit-cost analysis*. Key innovations in this methodology include its initial focus on fundamental asset characteristics to generate an exhaustive set of plausible threat scenarios based on a target susceptibility matrix (which we refer to as *asset-driven* analysis) and an approach to threat likelihood assessment that captures adversary tendencies to shift their preferences in response to security investments based on the expected utilities of alternative attack profiles assessed from the adversary perspective. A notional example is provided to demonstrate an application of the proposed framework. Extensions of this model to support strategic portfolio-level analysis and tactical risk analysis are suggested.

KEY WORDS: Consequence; critical asset protection; decision; homeland security; risk analysis; security; terrorism; threat assessment; vulnerability

1. INTRODUCTION

Providing a defensible basis for allocating resources for critical infrastructure and key resource protection is an important and challenging problem. Investments can be made in countermeasures that increase security and hardness of an asset exposed to a threat, deterrence measures to decrease the likelihood of a threat scenario, and capabilities to mitigate human and economic losses following an incident. Multiple threats must be considered, spanning everything from natural hazards, industrial accidents, and human-caused security threats. In addition, investment decisions can be made at multiple levels of abstraction and leadership, from tactical decisions for real-time asset-level protection to strategic decisions affecting portfolios of assets. To accommodate the complexity of the decision variables, the multitude and uncertain nature of possible threats, and the need for defensible risk results to better inform resource investment decision making at all levels, a mathematically sound methodology that quantifies uncertainty, accounts for all major risk contributors, and facilitates aggregation for higher-level risk studies and comparison with other quantified risks is required.[1] This article takes on this challenge for human-caused security threats.

In the security context, risk assessment focuses on assessing the likelihood of attack, likelihood of adversary success given attack, and consequences given success for a variety of threat scenarios.[2] A common expression for security risk is often stated as:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}, \quad (1)$$

where the "$\times$" denotes the Cartesian product. Equation (1) provides the philosophical basis for many security risk assessment methodologies.[3,4] Unlike most other types of hazards, *security threats* are

[1] Center for Technology and Systems Management, University of Maryland, College Park, MD 20742.
* Address correspondence to Bilal M. Ayyub, Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, MD 20742; tel: (301)405-1956; fax: (301)405-2585; ba@umd.edu.

initiated by deliberate, innovative, and arguably unpredictable human adversaries that choose from among many possible targets and potentially innovative attack modes based on their perceptions of risk, reward, and opportunity.[5] Security threats are in this sense asymmetric: whenever possible, potential adversaries will leverage the force-multiplying effect of surprise to achieve success against defenders that are either unaware of the threat or unprepared to defend themselves against unknown tactics.[6]

The security threat landscape is constantly changing, and as such it is extremely difficult to forecast future threats; adversaries will continue to improve their tactics, enhance their capabilities, and seek opportunities to catch their opponents off guard.[7] Consequently, the threat component of Equation (1) is arguably the most uncertain aspect of the security risk problem. However, by assuming rational adversaries,[8] several game theoretic analyses have shown[9,10] that they shift their attention toward softer targets and threat types in reaction to the security investments made by defenders. Thus given a specified threat type, one can assume that potential adversaries assign greater weight to assets with higher expected utilities with respect to their intentions and capabilities. Furthermore, one must also consider the visibility of the asset; for example, it is reasonable to assume that an asset (or scenario) with significant coverage in open sources is more visible to potential adversaries than one with little or no coverage,[11] and that more visible assets are more likely to be chosen as targets for attack. A suitable risk analysis methodology for the critical asset protection must capture the changing preferences of an observant and creative adversary, and should accommodate the fact that not all assets are visible.

A number of quantitative approaches that touch on aspects of Equation (1) have been proposed. Martz and Johnson[12] developed a model that focuses on theft of munitions by armed aggressors, and employs event tree modeling to assess the probability of adversary success based on the effectiveness of available countermeasures to protect these assets. Dessent[13] developed a similar model for prison security system design that focused on preventing prisoner escape. Both of these models break the "vulnerability" portion of Equation (1) into measurable parameters such as probability of detection and defender response time; however, since the consequences of security system failure are implied for these problems (i.e., theft, prisoner escape), neither model explicitly assesses loss from adversary success. In addition, since the threats are well defined, neither model accommodates adversary innovation.

Pate-Cornell and Guikema[14] proposed an overarching model for assessing terrorism risks where threat is taken as the product of relative scenario attractiveness and probability of intent, vulnerability is taken as the probability of adversary success, and consequences are described by expected disutility associated with a threat scenario from the U.S. perspective. According to this model, the attractiveness of a scenario might decrease in response to security investments, thus giving rise to an increase in the relative attractiveness of alternative scenarios. This model seems to capture the behavior of rational adversaries; however, since relative attractiveness is assessed with respect to a strict set of scenarios derived from threat intelligence, the model may not capture plausible scenarios for which no supporting intelligence is available.

In the absence of reliable threat information, a complete set of plausible threat scenarios can be identified based solely on their inherent susceptibilities to a wide spectrum of plausible threat types and without the need for intelligence supporting adversary intent. We refer to this style of analysis as an *asset-driven* approach. Asset-driven analysis assesses the consequences and probability of adversary success for an exhaustive set of plausible threat scenarios without regard to their probability of occurrence, and then overlays threat likelihood based on the relative attractiveness of alternative threat scenarios to obtain an estimate of total risk. In contrast, a *threat-driven* approach employed in typical risk assessment methodologies begins with a predefined set of threat scenarios based on assumed adversary capabilities justified by intelligence, and proceeds through the analysis of vulnerability and consequence constrained by the definition and scope of these threats. Threat-driven approaches are appropriate for studying hazards that are well understood and whose rate of occurrence can be reasonably predicted from historical data; however, they may fail to consider emerging or unrecognized hazards devised by an innovative adversary. An asset-driven approach brings all plausible threat scenarios to the forefront in an attempt to defeat the potential for surprise attack without regard to adversary intent.

In order to provide defensible risk results that facilitate benefit-cost analysis, a quantitative framework for risk assessment and management is required. Whereas other work in this area has produced a general quantitative framework for all-hazards risk analysis,[15] this article provides an in-depth

development of an asset-driven risk analysis focused on security threats. Moreover, the proposed methodology was designed to accommodate the dynamic and highly uncertain nature of security threats, to be transparent by breaking the problem down into clearly defined parameters that reflect all important risk contributors, and to produce quantitative results that capture all relevant uncertainties. The following sections describe the details of the proposed framework, followed by a simple notional example demonstrating its implementation. Note that the proposed framework does not presume specific techniques to capture and propagate uncertainty, nor does it insist on specific approaches for assessing model parameters. Rather, what is presented is a framework that captures all relevant aspects of the security risk problem, and makes suggestions as appropriate on how to go about obtaining values for the model parameters.

2. ASSET-LEVEL RISK ANALYSIS

The proposed framework for asset-level risk analysis consists of five phases as shown in Fig. 1, namely, scenario identification, consequence and criticality

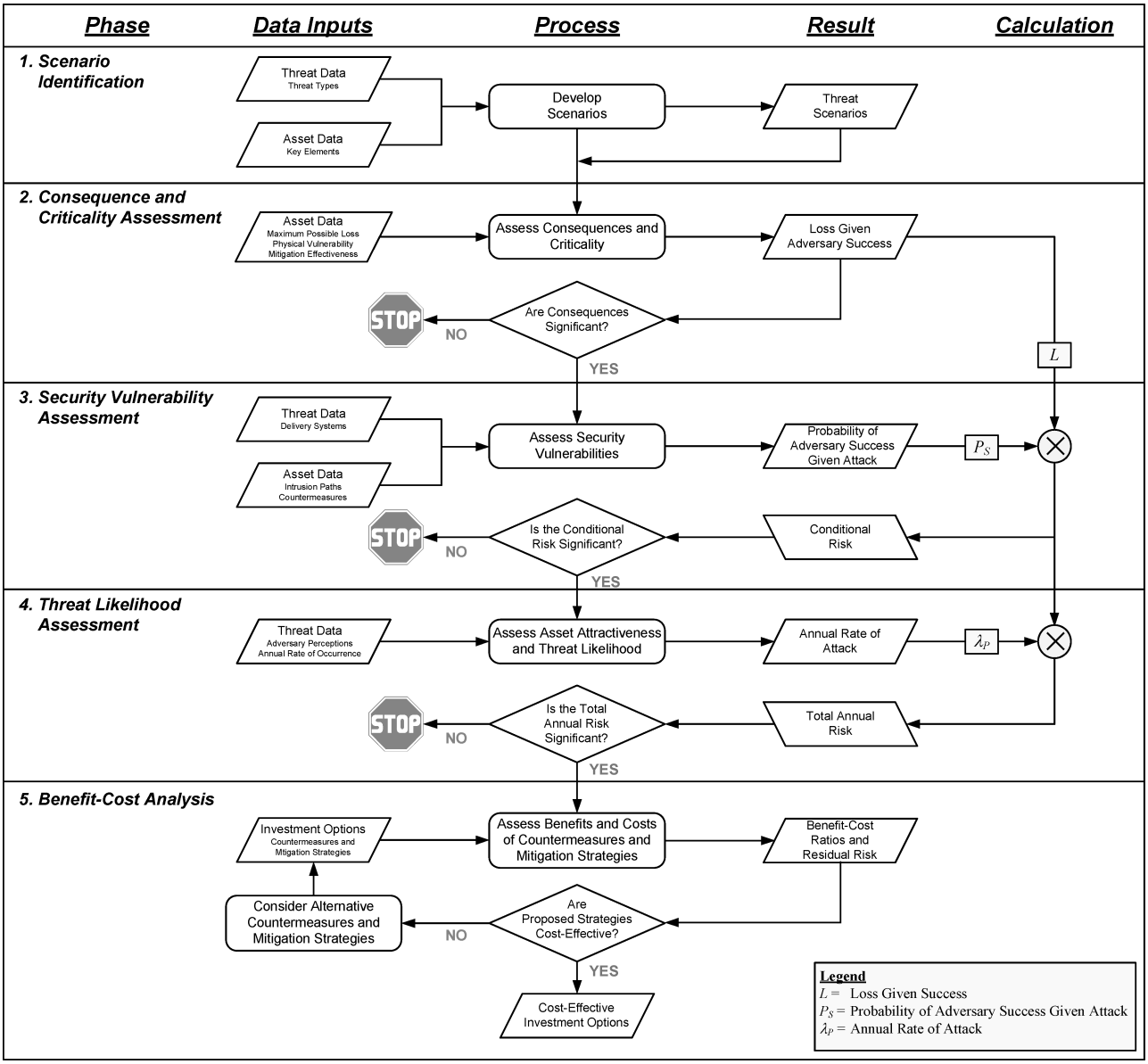

Fig. 1. Process for asset-level risk analysis.

assessment, security vulnerability assessment, threat likelihood assessment, and benefit-cost analysis. As required for any meaningful risk analysis,[16] the stated objective of this methodology is to support strategic resource allocation decisions at the asset level by providing meaningful measures of security risk that lend themselves to quantitative benefit-cost analysis. The first four phases are used to assess risk, whereas the final phase provides tools for evaluating alternative strategies for managing risk. Data for the parameters in each of these phases can be obtained via a combination of systems modeling and expert elicitation, and can be specified in terms of point estimates, mean and standard deviation, intervals, probability distributions, or imprecise probabilities. For example, Karimi and Hüllermeier[17] suggest the use of possibility-probability distributions when data for risk analysis is limited. Given finite available resources to conduct analysis, at the conclusion of each stage, results may be screened to determine which threat scenarios warrant further analytical treatment. Furthermore, in lieu of a complete analysis in each stage, conservative estimates may be used for selected parameters to facilitate rapid completion of the analysis process. These conservatisms can be revisited later if they are determined to have a significant effect on the final results. This technique also facilitates rapid screening: if conservative estimates yield acceptable risks, there is no need for additional analysis.

2.1. Scenario Identification

The scenario identification phase constructs an exhaustive set of plausible threat scenarios for an asset based on the inherent susceptibilities of its key elements to a wide range of security threats. This process begins with a complete characterization of an asset, including its mission and key elements. In this article, we define an *asset* as a physical component of a broader critical infrastructure system or key resource category that provides some sort of service to society, and may include such things as a communications tower, state monument, or product manufacturing facility (see Reference 18 for a complete list of asset types as defined by the U.S. Department of Homeland Security). Nominal performance of an asset can be described by a success scenario such as that discussed in Reference 1. We define a *key element* as one that directly contributes to the success scenario of the asset, and includes elements such as antenna, main building, or storage tank. Key elements can be identified from fault trees, reliability block diagrams, or other systems modeling techniques.[19] Once identified, each key element is classified according to its fundamental characteristics and functionality to facilitate mapping elements to relevant security threat types using a target susceptibility matrix such as the one shown in Table I. An exhaustive partitioning of the scenario space into nonoverlapping *security threat scenarios* is generated using this procedure, where each scenario defines a unique combination of key element and threat type. These scenarios can be qualitatively screened based on the potential effects and their severity following an attack using such tools as failure modes and effect analysis[20] to determine which scenarios warrant consideration.

2.2. Consequence and Criticality Assessment

The consequence and criticality assessment phase estimates the losses associated with a threat scenario

	Key Element					
Threat Type	HAZMAT Storage	Building	Pipeline	Rail Car	People	Computer Network
Explosive	**X**	**X**	**X**	**X**	**X**	**X**
Projectile/impact	**X**	**X**	**X**	**X**	**X**	–
Incendiary	**X**	**X**	–	–	**X**	**X**
Chemical	–	–	–	–	**X**	–
Biological	–	–	–	–	**X**	–
Radiological	–	–	–	–	**X**	**X**
Laser	–	–	–	–	**X**	–
Radio frequency	–	–	–	–	–	**X**
Cyber	–	–	–	–	–	**X**
Sabotage	**X**	–	**X**	**X**	–	**X**
Panic-inducing/harassment	–	–	–	–	**X**	–

Table I. Target Susceptibility Matrix

Table II. Asset-Level Consequence Dimensions

Dimension	Description
Fatalities	Number of equivalent fatalities resulting from a successful attack (accounts for deaths and injuries using tools such as the Accident Injury Scale[1]).
Repair costs	Costs to repair damage resulting from an attack measured in dollars.
Asset loss	Value of assets (e. g., goods, property, information) lost as a result of an attack measured in dollars.
Recuperation time	Time to recuperate mission following an attack measured in units of time.
Environmental damage	Environmental damage resulting from an attack measured in area affected.

given adversary success, with a primary focus on those losses that are of direct concern to the asset owner from the standpoint of continuity of operations and protection of personnel within the asset perimeter. As described in Table II, the proposed methodology examines five consequence dimensions considered to be of primary concern to the asset owner. Additional or fewer dimensions can be incorporated as needed to support asset-level decision making.

For each threat scenario, the loss, L, given adversary success (as a function of threat intensity) can be assessed for a threat scenario according to the equation:

$$L = L_{mpl} V_P (1 - E_R), \tag{2}$$

where L_{mpl} is the maximum possible (or credible) loss (assessed in units of loss per event), V_P measures the physical vulnerability for a given threat intensity, and E_R measures the effectiveness of response and recovery capabilities. The *maximum possible loss* (or *maximum credible loss*) is a single-valued measure of the worst possible (credible) loss under the worst possible circumstances from the asset owner's point of view.[21] The measure of *physical vulnerability* describes the fraction of maximum possible loss that accounts for both the fragility of the elements to a given threat intensity (such as the damage function described in Reference 22) and the effectiveness of strategies to mitigate the effects of damage (i.e., intrinsic resistance to loss). The *response effectiveness* describes the fractional reduction of potential loss considering the effectiveness of existing strategies to respond to and recover from an adverse event. Note that the loss in Equation (2) is assessed for each consequence dimension. A single measure of total loss can be obtained through the use of loss conversion factors that convert losses from their natural units to a dimension that facilitates comparison and aggregation (e.g., disruption measured in units of time to lost production measured in dollars).[21]

Values for the parameters in Equation (2) can be determined using systems modeling techniques such as event trees, fault trees, other simulation models, and experiment. Values can also be elicited from experts familiar with the asset and knowledgeable in such topics as weapons capabilities and effects, emergency response, and loss mitigation.

2.3. Security Vulnerability Assessment

The security vulnerability assessment phase investigates the likelihood that a determined adversary can successfully defeat security countermeasures and execute an attack against a target element. For security threats, this likelihood depends on the ability of the defender to protect its key elements by denying access to sensitive areas, detecting intrusion, engaging the intruder if detected, and neutralizing the intruder once engaged. The following approach to security vulnerability assessment focuses on a single attack profile and assumes a focused and determined adversary that will not give up until defeated by the response forces. This approach also assumes that defenders only respond within the asset perimeter. Consideration of multiple simultaneous attack profiles, failures of multiple components due to a single attack, and coordination between asset defenders and external response forces is reserved for future work.

The security vulnerability assessment phase begins by identifying a complete set of plausible intrusion paths leading to each key asset element. Intrusion paths begin at the outside perimeter of a facility since it is the first line that must be crossed by an intruder to gain access to a protected element.[23] Each intrusion path consists of a sequence of discrete *security zones*; a security zone is defined as a region within the asset perimeter containing a distinct set of countermeasures and features. Security zones are generally separated by detection measures. The *cross-section* of an intrusion path shows the sequence of security zones connecting the asset perimeter to the target element, such as is shown in Fig. 2.[13] For a given threat scenario, compatible threat delivery systems (e.g., ground vehicles for explosive threats) are identified for each intrusion path. The combination of delivery system and intrusion path defines an *attack profile*. Thus, the set of attack profiles partitions a given threat scenario

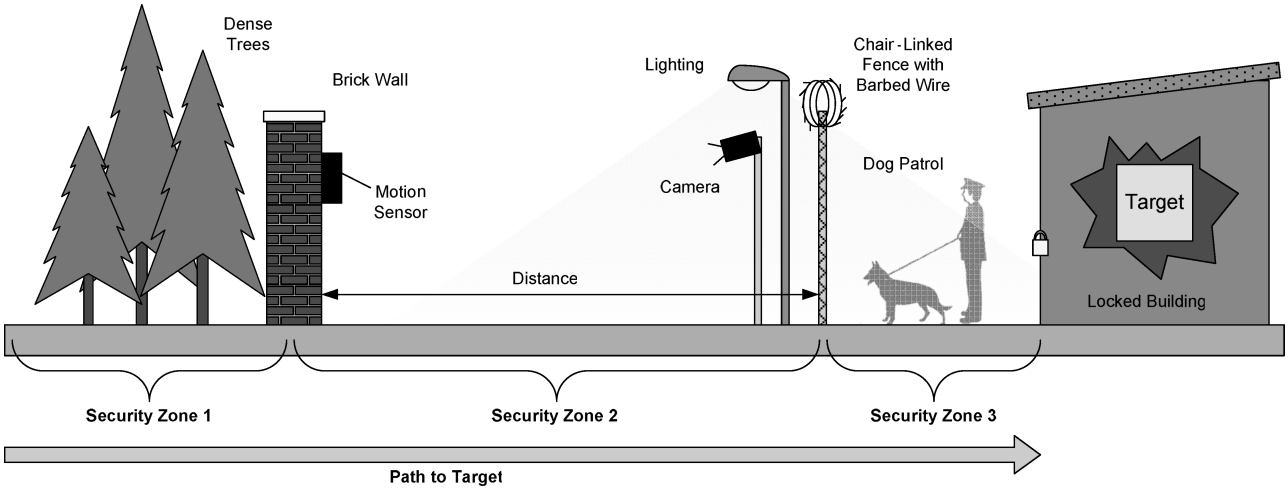

Fig. 2. Cross-section of an intrusion path.[17]

into an exhaustive set of nonoverlapping combinations of delivery system and intrusion path.

Each threat delivery system has a range of possible threat intensities it can impart on its target. For example, a vehicle-borne explosive device imparts explosive energy on a target that, for a fixed position relative to the target, is proportional to the amount of explosives it carries,[24] which can range from zero to the maximum capacity of the vehicle in either size or weight. The threat intensity of a given threat delivery system can be characterized by a probability distribution such as the one shown in Fig. 3. To simplify matters, a discrete distribution for threat intensity can be developed for a finite number of threat intensity levels (such as low, medium, and high) spanning this distribution. In discrete form, the total losses, $\hat{L}$, resulting from an attack with a particular delivery system can be determined as:

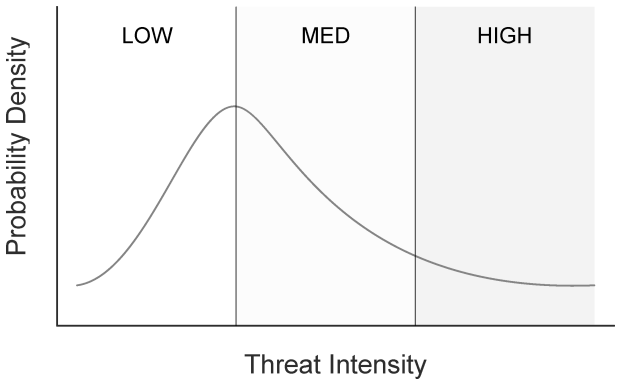

Fig. 3. Threat intensity distribution for a given delivery system.

$$\hat{L} = \sum_j p_j L_j, \tag{3}$$

where p_j is the probability of imparting threat intensity level j for the delivery system, L_j is the total loss given adversary success determined from Equation (2) conditioned on this threat intensity level, and the summation is taken over all threat intensity levels. The probabilities in Equation (3) can be obtained from experts familiar with the capabilities of alternative threat delivery systems.

In order for a security system to defeat an adversary, the adversary must be detected, engaged by response forces, and neutralized; failure to succeed at any one of these steps results in an overall failure to defeat a determined adversary.[25] Fig. 4 illustrates an event tree for this sequence of events for an intrusion path consisting of three security zones. Defining *interruption* as the combination of adversary detection and engagement by response forces, a simple equation giving the probability of interruption, P_I, for an intrusion path consisting of n security zones can be expressed as:[13]

$$P_I = P_{D_1} P_{E|D_1} + \sum_{q=2}^{n} P_{D_q} P_{E|D_q} \prod_{m=1}^{m=q-1} \{1 - P_{D_m}\}, \tag{4}$$

where P_{D_q} is the probability that the adversary is detected in security zone q, and $P_{E|D_q}$ is the probability that the guard/response force engages the adversary given detection. In general, the probabilities in Equation (4) have a time component, and their assessment can be obtained from measures of delay time associated with each barrier along an intrusion path, the

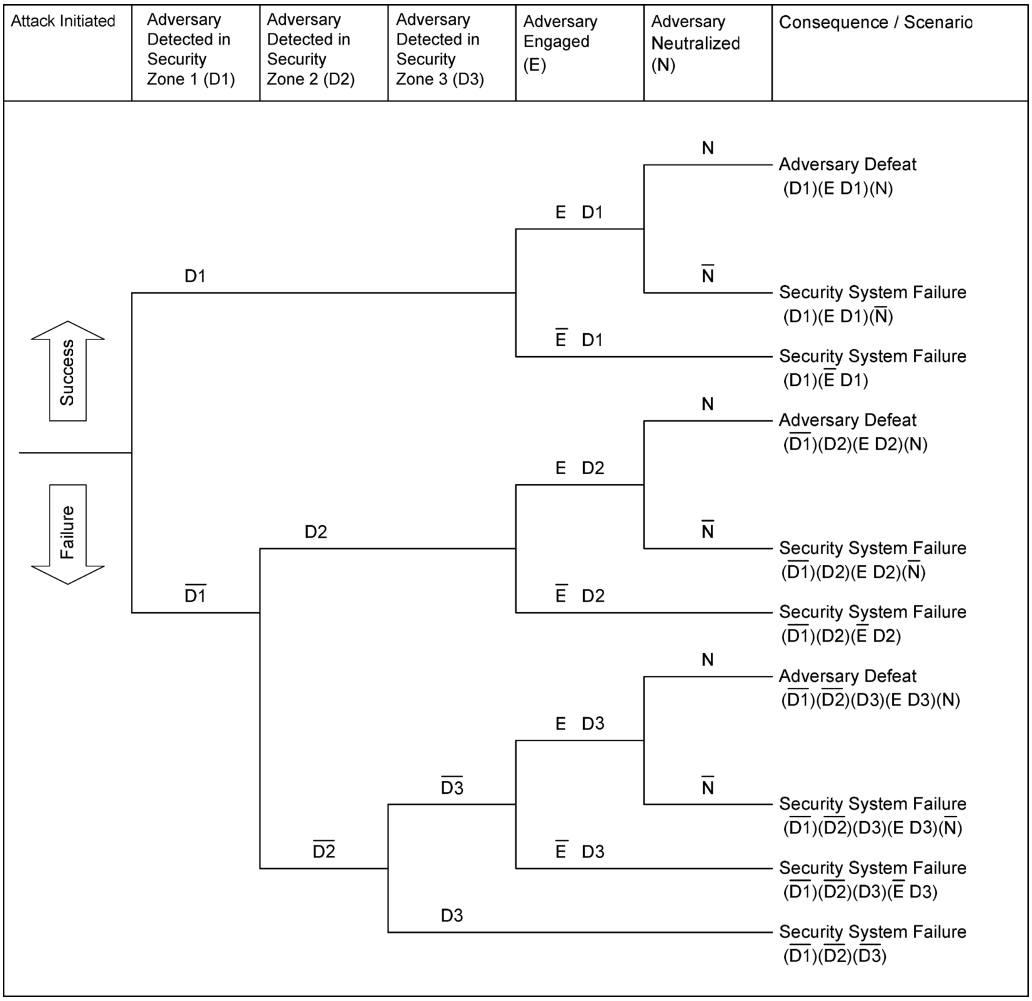

Fig. 4. Event tree for assessing security system effectiveness ("failure" indicates failure of the security system; "success" corresponds to security system success).

mean time to detect and probability of detection for static (demand-based) and active (time dependent) detection measures, respectively, and response times of the defender forces.

Using the model for security effectiveness assessment described in Reference 25, the probability that the defender interrupts and defeats the adversary (i.e., probability of security system success), E_S, is obtained by:

$$E_S = P_I P_{N|I}, \tag{5}$$

where $P_{N|I}$ is the probability that the defender neutralizes the adversary given interruption. The results from Equation (6) can be interpreted as the *reliability* of the security system with respect to a given challenge defined by the attack profile (philosophically similar to the stress-strength model for structural reliability[19]) though the appropriateness of the connection between security system effectiveness and security system reliability needs to be explored further. Adversary success is achieved if the security force fails to defeat an intruder and the intruder successfully attacks the target. From this definition, the probability of adversary success, P_S, can be determined as:

$$P_S = (1 - E_S) P_K, \tag{6}$$

where $(1 - E_S)$ is the probability of security system failure, and P_K is the probability that the adversary will successfully execute the attack given security system failure. Values for the parameters in Equations (5) and (6) can be determined from discrete event simulation models such as those described in

Reference 12, or from the judgment of experts familiar with defender and adversary capabilities.

The combination of probability of adversary success, P_S, from Equation (6) and total expected loss given success, $\hat{L}$, from Equation (3) for each attack profile gives the conditional risk, R_C, as follows:

$$R_C = P_S \hat{L}. \tag{7}$$

Conditional risk is expressed in units of loss per event, and provides a measure of the static or intrinsic risk given the occurrence of a specific attack profile.

2.4. Threat Likelihood Assessment

The threat likelihood assessment phase assesses the annual rate of occurrence of plausible threat scenarios and attack profiles. Within a probabilistic framework, the likelihood of a given threat scenario is a function of its annual rate of occurrence affecting a portfolio of assets to which the asset belongs, and the probability of realizing a specific attack profile given occurrence of the threat. This latter parameter takes into account the relative attractiveness of all assets, their key elements, and potential attack profiles with respect to an adversary's perceptions of probability of success for attacking via the corresponding intrusion path and delivery system, gains from success, losses from failure, and costs to prepare for and execute an attack. Assuming a rational adversary, attack profiles perceived to have a higher expected utility are considered more attractive. Attractiveness also depends on whether the adversary is aware of a particular intrusion path to the target; less visible intrusion paths are less likely to be considered due to lack of information available to the adversary on their existence, and are therefore less attractive.

Considering the perceived probability of success, P_S^*, gain from success, G^*, loss from failure, L^*, and cost to attack, C^*, associated with a given attack profile, the expected utility of the attack profile as perceived by the adversary, U_P, can be expressed as:

$$U_P = P_S^* G^* - \left(1 - P_S^*\right) L^* - C^*. \tag{8}$$

In order to effectively apply Equation (8), it is important to first characterize the beliefs and capabilities of the notional adversary, and how these translate into values for the parameters. Such a characterization can be generic or reflective of a specific adversary. Assuming knowledge of adversary capabilities, intentions, and perceptions, values for the parameters in Equation (8) can be determined using techniques such as multicriteria decision analysis.[26] Alternatively, if one assumes that the potential adversary (1) seeks to maximize total loss, (2) has perfect knowledge (i.e., defender knowledge) of loss given success and probability of success for each attack profile, (3) has no expectations of survival after the attack, and (4) the relative cost to attack is negligible with respect to the expected gain from success, the expected utility can be expressed as:

$$U_P = R_C, \tag{9}$$

where R_C is the (aggregate) conditional risk determined from Equation (7). From the four assumptions proposed, Equation (9) suggests that the expected utility of a given attack profile from the adversary perspective is equal to the conditional risk assessed by the defender. Further assuming that probability of a specified attack profile is proportional to the relative expected utility with respect to all other attack profiles, it follows that the assumptions leading to Equation (9) yield an upper bound for risk; any deviation in adversary perceptions or preferences will apportion a greater degree of attractiveness to less consequential scenarios, and thus lower overall risk.

Similar to the attractiveness model discussed in Reference (14), the relative attractiveness of the i-th attack profile, A_{P_i}, can be defined as the ratio of the adversary perceived expected utility for a single profitable attack profile (i.e., $U_P > 0$) (discounted by visibility of the intrusion path) to the sum of all profitable attack profile utilities (also discounted by visibility of the intrusion path) for a given threat scenario:

$$A_{P_i} = \frac{U'_{P_i}}{\sum_j U'_{P_j}}, \tag{10}$$

where U'_P is the perceived expected utility of the attack profile discounted by the probability that the intrusion path is visible to the adversary, P_{VP}:

$$U'_P = P_{VP} \max(U_{P_i}, 0). \tag{11}$$

By convention, $A_{P_i} = 0$ if the denominator of Equation (10) is zero. Values for P_{VP} depend on adversary knowledge and awareness of various intrusion paths, and can be estimated based on the availability of asset information.

The relative attractiveness of the i-th threat scenario, A_{S_i}, can be defined as the ratio of the perceived expected utility for a single threat scenario (discounted by visibility of the associated key element) to the sum of all threat scenario utilities of the

corresponding threat type (also discounted by visibility of the key elements) as:

$$A_{S_i} = \frac{U'_{S_i}}{\sum_j U'_{S_i}}, \tag{12}$$

where U'_S is the perceived expected utility of the threat scenario discounted by the probability that the key element associated with the hazard scenario is visible to the adversary, P_{VE}:

$$U'_S = P_{VE} \max_i(U_{P_i}), \tag{13}$$

where the maximum is taken over all attack profiles associated with the scenario. By convention, $A_{S_i} = 0$ if the denominator of Equation (12) is zero. The value for P_{VE} depends on adversary knowledge and awareness of the various key elements comprising the asset, and can be elicited from experts familiar with the presence of the asset in open sources.

The relative attractiveness of the i-th asset, A_{A_i}, can be defined as the ratio of the perceived expected utility for attacking the asset with a given threat type (discounted by visibility of the asset) to the sum of all perceived expected utilities for all assets in a portfolio (also discounted by asset visibility):

$$A_{A_i} = \frac{U'_{A_i}}{\sum_j U'_{A_j}}, \tag{14}$$

where U'_A is the perceived expected utility associated with attacking the asset discounted by the probability that the asset is visible to the adversary, P_{VA}:

$$U'_A = P_{VA} \max_i(U'_{S_i}), \tag{15}$$

where the maximum is taken from among all threat scenarios i associated with the asset for a given threat type. The value for the asset visibility term P_{VA} depends on adversary knowledge and awareness of the asset, and can be elicited from experts familiar with the amount of publicly accessible information on the asset. By convention, $A_{A_i} = 0$ if the denominator of Equation (14) is zero.

The annual rate of occurrence, λ_P, for a given attack profile can be determined from the following equation:

$$\lambda_P = \lambda_0 A_A A_S A_P, \tag{16}$$

where λ_0 is the baseline annual rate of occurrence for a particular threat type affecting a portfolio of assets, and A_P, A_S, and A_A are the probability of adversary awareness of the respective intrusion path, key element, and asset given by Equations (10), (12), and (14), respectively. Values for the baseline annual rate of occurrence can be elicited from experts knowledgeable of trends in adversary ideology, behavior, and innovation. Following the suggestions in Reference (1), a probability of frequency approach can be used to account for the uncertainty in the annual rate of occurrence.

Alternatively, in the absence of data to produce defensible estimates of asset attractiveness and baseline annual rate of attack occurrence, Equation (16) can be replaced with an expression for relative threat probability as follows:

$$T = A_T A_S A_P, \tag{17}$$

where A_T is the relative attractiveness of alternative threat types with respect to a given asset. In a manner similar to asset, scenario, and attack profile attractiveness, the relative threat attractiveness can be obtained as:

$$A_{T_i} = \frac{U'_{T_i}}{\sum_j U'_{T_j}}, \tag{18}$$

where U'_T is the perceived expected utility associated with attacking the asset with a given threat type:

$$U'_T = \max_i(U'_{S_i}), \tag{19}$$

where the maximum is taken from among all scenarios associated with the given threat type. While Equations (17)–(19) cannot be used to estimate total annual risk for comparison with risks arising from other sources (e.g., natural hazards), these equations can be used to determine the fraction of risk (i.e., relative risk) attributable to different threat types given the occurrence of an attack at a given asset.

The combination of conditional risk from Equation (7) and threat rate of occurrence from Equation (16) gives the following expression for total annual attack profile risk, R_P:

$$R_P = \lambda_P P_S \hat{L}. \tag{20}$$

Total annual risk is expressed in units of consequence per unit time. The total annual risk associated with an asset can be determined by summing the results from Equation (20) for all threat scenarios and attack profiles. The total annual risk can also be represented

by a loss-exceedence curve,[19] with the exceedence rate λ_e for loss value l determined as:

$$\lambda_e(l) = \sum_i \lambda_{P,i} P_{S,i} P(\hat{L}_i > l), \tag{21}$$

where $P(\hat{L} > l)$ is the probability that the loss for the attack profile exceeds l and the summation is taken over all attack profiles. If uncertainty is specified on the annual rate of threat occurrence, a family of curves can be plotted using Equation (16) and different percentile values for λ_P. Note that if the relative threat probability from Equation (17) is used in lieu of the annual rate of occurrence in Equation (20), total annual risk will be expressed as a conditional risk measured in units of loss per event.

2.5. Benefit-Cost Analysis

The benefit-cost analysis phase assesses the cost effectiveness of proposed countermeasures and consequence mitigation strategies. In the context of security threats, countermeasures aim to reduce the probability of attack or probability of adversary success, and consequence mitigation strategies aim to reduce the potential consequences following an attack. The benefit of a risk mitigation action is the difference between the values of loss, conditional risk, or total annual risk (collectively referred to as "state") before and after its implementation.[21] The benefit-to-cost ratio is given by:

$$\frac{\text{Benefit}}{\text{Cost}} = \frac{\text{Unmitigated State} - \text{Mitigated State}}{\text{Cost}}, \tag{22}$$

where higher-valued ratios indicate better risk mitigation actions from a cost-effectiveness standpoint. The probability that a favorable benefit-to-cost ratio will be realized can be represented as:

$$\Pr\left(\frac{\text{Benefit}}{\text{Cost}} \geq \alpha\right) = 1 - \Pr(\text{Benefit} - \alpha \cdot \text{Cost} \leq 0), \tag{23}$$

where α is an acceptability criterion specified according to the dimensions of benefit and cost. In addition to the results of Equation (23), selection of a suitable risk mitigation action must also consider the affordability of each alternative and whether it achieves risk reduction objectives.

3. ILLUSTRATIVE EXAMPLE

To illustrate a simple application of the proposed risk framework, consider the notional chemical storage facility with seven key elements as shown in Fig. 5. Note that all values used throughout this example are purely notional.

3.1. Scenario Identification

A complete set of threat scenarios can be developed using the target susceptibility matrix shown in Table I. For the purposes of illustration, this example focuses on the single threat scenario "explosive attack against chemical tank 2."

3.2. Consequence and Criticality Assessment

Table III shows the number of fatalities and economic loss given success as a function of intensity for this scenario determined from Equation (2) and values assumed for maximum possible (credible) loss, physical vulnerability, and response effectiveness. For simplicity, uncertainty in the physical vulnerability and mitigation effectiveness is specified in terms of coefficients of variation on the parameter values.

3.3. Security Vulnerability Assessment

Four representative intrusion paths were identified with cross-sections shown in Fig. 6. Table IV lists the four representative explosive threat delivery systems with associated threat intensity distributions, and combined with the loss given success as a function of threat intensity in Table III, the total loss given success was determined from Equation (3). Table V specifies the probability of detection and probability of engagement for each security zone to determine the probability of intervention for each intrusion path from Equation (4), which in turn is used to calculate the probability of adversary success and conditional risk from Equations (5)–(7) for each attack profile as shown in Table VI.

3.4. Threat Likelihood Assessment

Assuming perfect visibility of the asset, its key elements, and intrusion paths, and perfect adversary knowledge of security countermeasure effectiveness, the total annual risk for each attack profile is determined from Equations (8)–(16) and (20), as shown in Tables VII, VIII, and IX. Under the aforementioned assumptions, the perceived expected utility for each attack profile from the adversary perspective is equal to the conditional risk assessed by the defender. Uncertainty in the baseline annual rate of occurrence was specified in terms of a coefficient of variation.

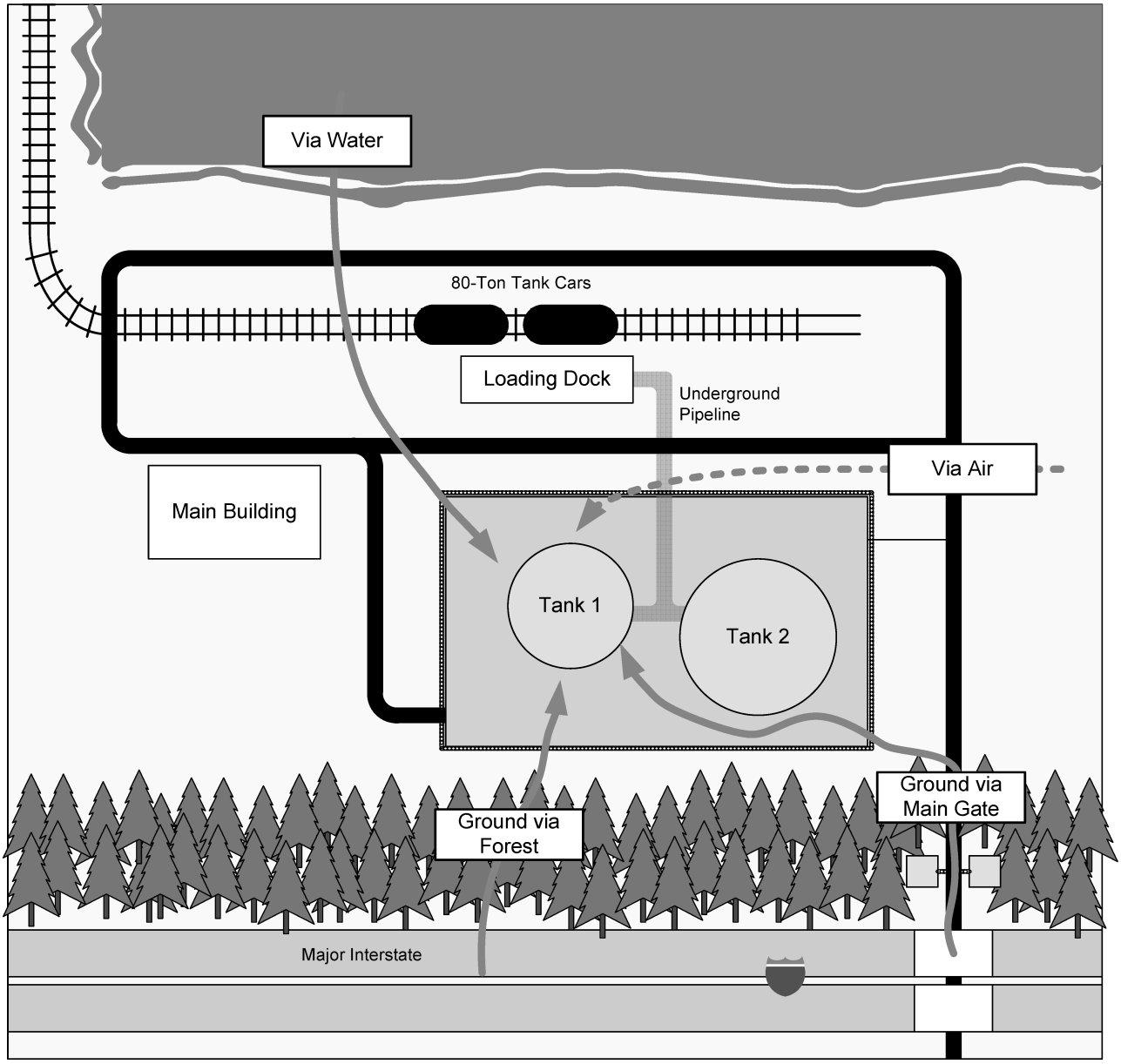

Fig. 5. Notional chemical storage facility and representative intrusion paths.

From the results in Table IX, the total risk for this threat scenario (assuming a constant $6-million statistical value of life for illustration) is $18,899 per year with a coefficient of variation of 0.61. The corresponding loss-exceedence curves for this threat scenario were determined from Equation (21) as shown in Figs. 7 and 8 for fatality and economic loss, respectively. The uncertainty in total annual risk was determined using approximate techniques for uncertainty propagation described in Reference (25) and the coefficients of variation specified for the various parameters.

3.5. Benefit-Cost Analysis

To reduce the total risk associated with this threat scenario, several countermeasures were considered as described in Table X. The costs, benefits, and probability of realizing a net benefit for each option are given in Table XI as determined from Equations (22)

Table III. Total Expected Loss Given Success

Consequence Dimension	Maximum Possible Loss,[1] L_{mpl} (per Event)	Loss Conversion Factor[1]	Physical Vulnerability,[2] V_P, (by Threat Intensity Level)			Response Effectiveness Factor,[3] E_R	Loss Given Success,[4] L (by Threat Intensity Level)		
			Low	Med	High		Low	Med	High
Fatalities	50 persons	$6.0-M	0.20	0.60	0.80	0.20	8	24	32
Repair Costs	$5.0M	N/A	0.60	0.70	0.80	0.20	$2.4M	$2.8M	$3.2M
Asset Loss	$10.0M	N/A	0.70	0.75	0.80	0.20	$5.6M	$6.0M	$6.4M
Recuperation Time	60 days	$100 K/day	0.25	0.50	0.75	0.20	$1.2M	$2.4M	$3.6M
Environmental Damage	5 acres	$200 K/day	0.10	0.50	0.80	0.20	$80 K	$400 K	$640K

[1] M = Millions, K = Thousands.
[2] 0.25 coefficient of variation assumed on each physical vulnerability factor.
[3] 0.25 coefficient of variation assumed on each response effectiveness factor.
[4] 0.35 coefficient of variation calculated for each loss estimate based on the values from notes 2 and 3.

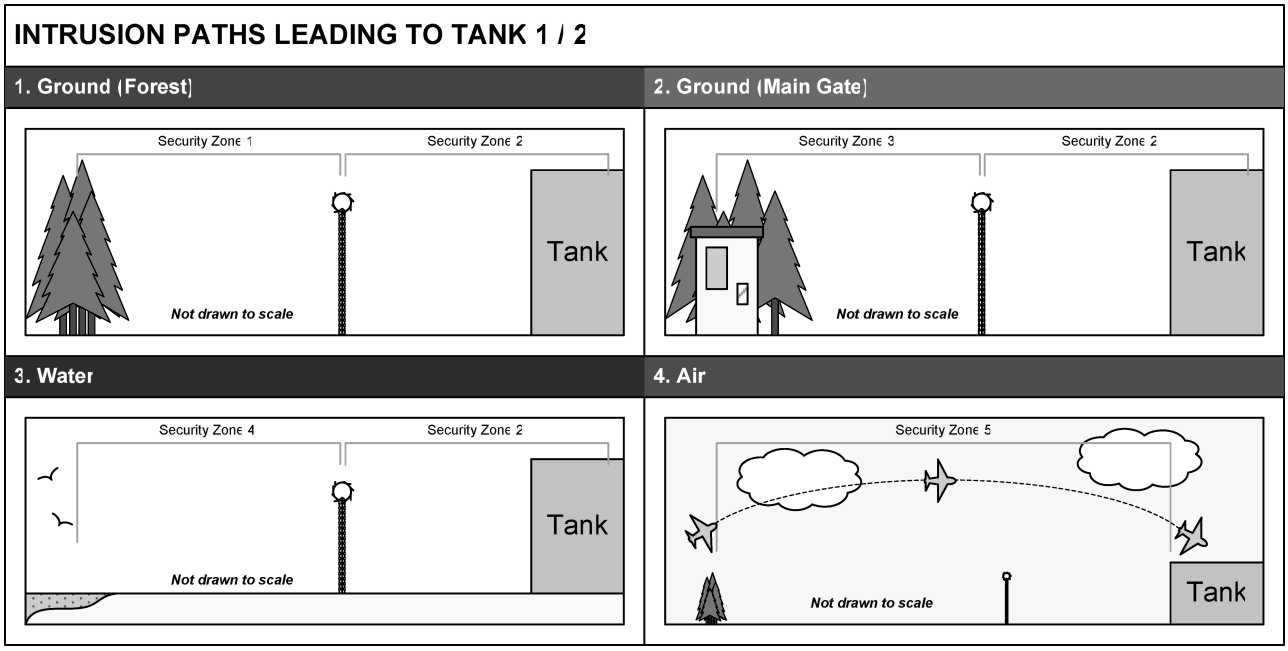

Fig. 6. Intrusion paths to a chemical tank.

Delivery System	Probability of Intensity, p			Total Fatalities Given Success per Event[1]	Total Expected Economic Loss Given Success per Event[1,2]
	Low	Med	High		
Hand Emplaced	0.9	0.1	0.0	9.6 (0.28)	$9.51M (0.21)
Ground Vehicle	0.0	0.1	0.9	31.2 (0.33)	$13.62M (0.19)
Manned Aerial Vehicle	0.8	0.2	0.0	11.2 (0.25)	$9.74M (0.19)
Unmanned Aerial Vehicle	1.0	0.0	0.0	8.0 (0.35)	$9.28M (0.24)

Table IV. Explosive Threat Delivery System and Expected Loss Given Success

[1] Coefficient of variation specified in parentheses calculated from values in Table III.
[2] Total expected economic loss is the sum of the losses due to repair costs, asset loss, recuperation time, and environmental damage.

Table V. Security Zones and Countermeasure Effectiveness

	Security Zone 1		Security Zone 2		Security Zone 3		Security Zone 4		Security Zone 5	
Delivery System	P_D	$P_{E\|D}$	P_D	$P_{E\|D}$	P_D	$P_{E\|D}$	P_D	$P_{E\|D}$	P_D	$P_{E\|D}$
Hand Emplaced	0.5	0.98	0.8	0.50	0.9	1.00	0.2	1.00	- -	- -
Ground Vehicle	- -	- -	0.7	0.00	0.7	0.05	- -	- -	- -	- -
Manned Aerial Vehicle	- -	- -	- -	- -	- -	- -	- -	- -	0.6	1.00
Unmanned Aerial Vehicle	- -	- -	- -	- -	- -	- -	- -	- -	0.3	0.96

Table VI. Probability of Adversary Success for Each Attack Profile

Attack Profile						Conditional Risk,[1] R_C	
Delivery System	Intrusion Path	P_I	$P_{N\|I}$	P_K	P_S	Fatalities	Economic
Hand Emplaced	Ground (Forest)	0.69			0.38	3.6 (0.28)	$3.59M (0.21)
	Ground (Main Gate)	0.94	0.90	1.0	0.16	1.5 (0.28)	$1.49M (0.21)
	Water	0.52			0.53	5.1 (0.28)	$5.07M (0.21)
Ground Vehicle	Ground (Main Gate)	0.03	0.05	1.0	1.00	31.1 (0.33)	$13.59M (0.19)
Manned Aerial Vehicle	Air	0.60	0.10	1.0	0.94	10.5 (0.25)	$9.16M (0.19)
Unmanned Aerial Vehicle	Air	0.29	0.05	1.0	0.99	7.9 (0.35)	$9.15M (0.24)

[1] Coefficient of variation specified in parentheses.

Table VII. Relative Attack Profile Attractiveness

Attack Profile						
Delivery System	Intrusion Path	P_{VP}	P_S^*	G^1	U_P'	A_P
Hand Emplaced	Ground (Forest)	1.0	0.38	67.1	25.3	0.06
	Ground (Main Gate)	1.0	0.16	67.1	10.5	0.03
	Water	1.0	0.53	67.1	35.7	0.09
Ground Vehicle	Ground (Main Gate)	1.0	1.00	200	200	0.50
Manned Aerial Vehicle	Air	1.0	0.94	76.9	72.3	0.18
Unmanned Aerial Vehicle	Air	1.0	0.99	57.3	56.5	0.14

[1] Gain from success in units of millions of dollars.

and (23) assuming the risk before and risk after implementation to be perfectly correlated. Observe that implementation of either Option 1 or 2 actually increases total annual risk; the cause for this increase is shifting adversary preferences toward alternate attack profiles. Overall, Option 3 alone is the best option from the standpoint of cost effectiveness and probability of achieving a net benefit. However, additional information on whether the needed resources are available to implement this option and whether this option meets risk reduction objectives is required prior to making a final decision. Furthermore, due to constant shifting of adversary preferences in response to security investments, a more complete picture of asset-level risk considering all threat scenarios is necessary to fully evaluate the benefits of proposed security investments.

Table VIII. Relative Threat Scenario Attractiveness

Threat Scenario					
Threat Type	Key Element	P_{VE}	Max(U_P')[1]	U_S'	A_S
Explosive Attack	Main Building	0.80	50.1	40.1	0.07
	Personnel	0.80	60.1	48.1	0.09
	Loading Dock	0.60	20.0	12.0	0.02
	Pipeline	0.40	20.0	8.02	0.01
	80-Ton Rail Car	0.80	60.1	48.1	0.09
	Chemical Tank 1	1.00	180	180	0.34
	Chemical Tank 2	1.00	200	200	0.37

[1] Notional maximum attack profile utilities provided for other key elements. Utility expressed in millions of dollars.

4. DISCUSSION AND FUTURE DIRECTIONS

To assess the annual rate of occurrence for an attack profile, the proposed framework relies on the

Table IX. Annual Rate of Occurrence and Total Annual Risk for Each Attack Profile

Attack Profile		P_{VA}	$U_S'^2$	$A_A^{2,3}$	Baseline Frequency,[4] λ_0 (Events per Year)	λ_4^P (Events per Year)	Total Annual Profile Risk,[1] R_P (Loss per Year)	
Delivery System	Intrusion Path						Fatalities	Economic Loss
Hand Emplaced	Ground (Forest)	1.0	200	0.01	1/25	9.455E-05	3.427E-04 (0.80)	$34 (0.78)
	Ground (Main Gate)					3.919E-05	5.886E-05 (0.80)	$6 (0.78)
	Water					1.334E-05	6.820E-04 (0.80)	$68 (0.78)
Ground Vehicle	Ground (Main Gate)					7.482E-05	2.330E-03 (0.82)	$1017 (0.77)
Manned Aerial Vehicle	Air					2.700E-05	2.843E-04 (0.79)	$247 (0.77)
Unmanned Aerial Vehicle	Air					2.107E-05	1.661E-04 (0.83)	$193 (0.79)

[1] Coefficient of variation specified in parentheses.
[2] Utilities expressed in units of millions of dollars.
[3] Portfolio assumed to contain assets with a sum total attractiveness of 20,000. This value is used for the denominator in Equation (16).
[4] 0.75 coefficient of variation assumed on annual rate of occurrence.

assumption of a constant baseline annual rate of occurrence for a given threat type to calculate total annual risk. Though the previous example demonstrated the ability of the proposed methodology to directly account for shifting adversary preferences in response to security investments for a given threat type, it has been shown[27] that determined adversaries may also shift their tactics in response to measures taken that make certain threat types more difficult, and thus the baseline annual rate of occurrence is not constant but rather as dynamic as asset attractiveness. As a result, it is very difficult to obtain defensible estimates of frequency of certain types of attack given the complexity of the security environment and the interactions between defenders and potential adversaries on the global scale. Fortunately, the proposed framework provides an alternative for assessing threat likelihood that considers the relative attractiveness of the different threat types; while this alternative will not produce estimates of total annual risk, it may yield insights into the relative contribution to total risk from each plausible threat type. Regardless of whether annual rate of occurrence or relative threat probability is used, the proposed framework supports comparative risk analysis among assets.

Moreover, given the proliferation of advanced technology combined with pace of adversary innovation, it has become more important to focus on events

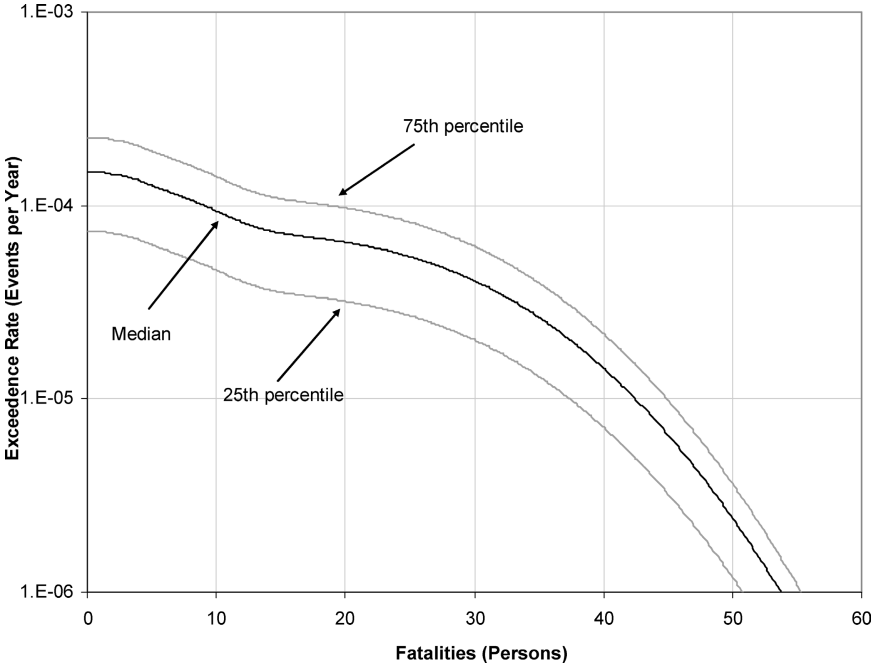

Fig. 7. Fatality loss-exceedence curve.

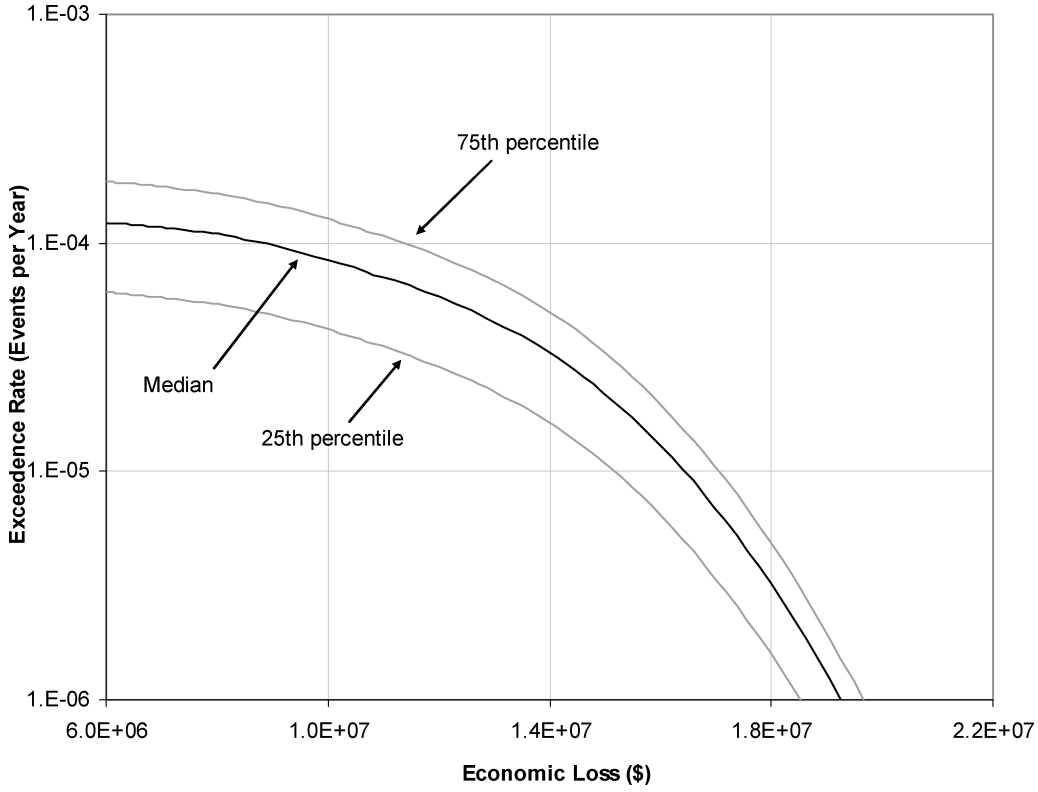

Fig. 8. Economic loss-exceedence curve.

that are possible rather than to rely on only those that are considered probable. The proposed methodology establishes bounds on the possible by focusing on the inherent susceptibilities of an asset's key elements to derive a complete set of plausible threat scenarios independent of their assessed likelihood, and thus eliminates those threats deemed irrelevant (e.g., biological attack against computer network). From here, reasonable estimates of annual threat frequency (or relative threat attractiveness) can be made as needed to facilitate higher-level aggregation and comparison with other societal risks.

Table X. Countermeasure Options

Option	Impact[1]
Option 1: Enhance access control in security zone 3	$P_D = 0.99$ for all delivery system attacks through security zone 3
Option 2: Enhance detection capability in security zone 1 and add signage	$P_D = 0.8$ for all delivery systems through security zone 1
Option 3: Add vehicle barriers in security zone 3	$P_I = 1.00$ in security zone 3 $P_{N\|I} = 0.99$ in security zone 3

[1] Combined options with redundant effects use most favorable value for risk calculations.

If guidance was available on adversary perception, the proposed methodology could, in principle, capture the effects of deterrence. Deterrence affects the psyche of the adversary; the greater the number of visible safeguards, the more nervous the adversary may become.[28] *Deterrence measures* focus on influencing adversary perceptions without necessarily having an effect on the adversary's true probability of success, and include such measures as decoys, camouflage, and fake cameras. According to Equation (14), enough deterrence could lower the attractiveness of alternative threat scenarios and attack profiles enough to remove the asset from consideration. Knowledge of how adversaries think opens up a wide range of inexpensive countermeasure options aimed at perception management. Methods to both characterize adversary beliefs and capabilities and estimate the effectiveness of deterrence measures are subjects that warrant future research consideration.

Table XI. Benefits and Costs of Proposed Countermeasures

Option	Annual Cost to Implement over 5 Years[1] ($/Year)	Annual Risk Before Implementation[1] ($/Year)	Annual Risk After Implementation[1] ($/Year)	Benefit[1] ($/Year)	Benefit-to-Cost Ratio[2]	Probability of Realizing Net Benefit[3]
Option 1	1,000 (0.25)	18,899 (0.61)	19,003 (0.61)	−104 (0.61)	−0.10	0.00
Option 2	2,500 (0.25)	18,899 (0.61)	19,248 (0.62)	−349 (1.16)	−0.14	0.00
Option 3	5,000 (0.25)	18,899 (0.61)	2,935 (0.37)	15,964 (0.65)	+3.19	0.85
Option 1 + 2	3,500 (0.19)	18,899 (0.61)	19,359 (0.62)	−450 (1.03)	−0.13	0.00
Option 1 + 3	6,000 (0.21)	18,899 (0.61)	2,793 (0.42)	16,106 (0.64)	+2.68	0.83
Option 2 + 3	7,500 (0.19)	18,899 (0.61)	2,967 (0.38)	15,932 (0.65)	+2.12	0.79
Option 1 + 2 + 3	8,500 (0.17)	18,899 (0.61)	2,828 (0.44)	16,071	+1.89	0.77

[1] Coefficient of variation specified in parentheses.
[2] Benefit-to-cost ratio calculated from Equation (16).
[3] Calculated from Equation (17) with $\alpha = 1.0$.

For a set of assets in a given portfolio, the total portfolio risk, not including effects of interdependencies, can be obtained by summing the corresponding risk results obtained from Equation (20). Because of the tendency of adversaries to respond to security investments by shifting preferences, portfolio-level analysis would yield insights into how risks shift between assets in response to security investments. In this sense, an asset-level assessment requires portfolio-level analysis to account for the shift in adversary attention toward softer alternatives. Similarly, portfolio-level analysis cannot succeed without leveraging the results from asset-level risk analyses for probability of adversary success and consequences, which would then feed into the analysis of physical, geographic, cyber, and logical interdependencies.[29] For example, knowledge of the recuperation time (and percentage disruption) required to recover from a successful attack would facilitate the assessment of cascading consequences due to loss of an asset's functionality.

On a final note, the focus of the proposed framework is on supporting *strategic* risk assessment and management rather than on *tactical* analysis. In contrast to tactical analysis that measures risk real time considering the current and near-term threat, security, and situational (loss) environment, strategic analysis focuses on the future threat and as such requires a robust methodology that supports investment decisions considering the full spectrum of possible adversary actions. To accommodate tactical analysis, the expression for total attack profile risk in Equation (20) can be modified as follows:[31]

$$R_P(t) = P_A(t) P_S(t) L(t), \tag{24}$$

where the threat component is replaced by a dynamic probability of attack, P_A, that captures the real-time intent of a potential adversary, and the probability of success and loss given success terms are now functions of time. The model in Equation (24) can be used for justifying alert levels (e.g., terrorism warnings analysis),[30] and hence allocating tactical resources among assets to reduce the real-time risk. However, in contrast to the model proposed in the previous sections, the assessment of tactical risk using Equation (24) requires intelligence information, not just for the probability of attack, but for probability of success (a function of adversary and defender capabilities at the time of attack) and consequence potential (a function of the situational environment). Efforts are currently under way to develop an evidence-based framework for leveraging intelligence to produce quantitative assessments for probability of attack.[31]

ACKNOWLEDGMENTS

The authors wish to thank the Maryland Emergency Management Agency and the Maryland Governor's Office of Homeland Security, and its representatives, including Mr. Dennis Schrader, Mr. Christopher Geldart, Mr. Mel Blizzard, Mr. Daniel Green, and Mr. Adam Trister. The funding source had the right to review and comment on the article but did not have the right to approve or disapprove the final version.

REFERENCES

1. Garrick, B. J., Hall, J. E., Kilger, M., McDonald, J. C., O'Toole, T., Probst, P. S., Parker, E. R., Rosenthal, R., Trivelpiece, A. W., Van Arsdale, L. A., & Zebroski, E. L. (2004). Confronting

the risks of terrorism: Making the right decisions. *Reliability Engineering and System Safety*, *86*(2), 129–176.
2. Broder, J. F. (1984). *Risk Analysis and the Security Survey*. Massachusetts: Butterworth Publishers.
3. Moteff, J. (2005). *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. Congressional Research Service Report to Congress, Order Code RL32561.
4. Matalucci, R. V. (2002). Risk assessment methodology for dams (RAM-D). *Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management (PSAM6), 23–28 June 2002 San Juan, Puerto Rico, USA, Vol. 1*, 169–176.
5. Hoffman, B. (1998). *Inside Terrorism*. New York: Columbia University Press.
6. Grabo, C. M. (2002). *Anticipating Surprise: Analysis for Strategic Warning*. Washington, DC: Joint Military Intelligence College.
7. Manunta, G. (2002). Risk and security: Are they compatible concepts? *Security Journal, 15*(3), 43–55.
8. Hoffman, B. (1998). *Inside Terrorism*. New York: Columbia University Press.
9. Sandler, T., & Lapan, H. E. (1988). The calculus of dissent: An analysis of terrorists' choice of targets. *Synthese*, *76*, 245–261.
10. Bier, V. M., Nagaraj, A., & Abhichandani, V. (2005). Protection of simple series and parallel systems with components of different values. *Reliability Engineering & System Safety*, *87*, 313–323.
11. Pluchinsky, D. (2002). They heard it all here, and that's the trouble. *Washington Post*, 16 June 2002 p. B03.
12. Martz, H. F., & Johnson, M. E. (1987). Risk analysis of terrorist attacks. *Risk Analysis*, *7*(1), 35–47.
13. Dessent, G. H. (1987). Prison perimeter cost effectiveness. *Journal of the Operational Research Society*, *10*, 975–980.
14. Pate-Cornell, E., & Guikema, S. (2002). Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. *Military Operations Research*, *7*(4), 5–232.
15. McGill, W. L., Ayyub, B. M., & Kaminskiy, M. (in press). Critical asset and portfolio risk analysis for homeland security: An all hazards framework. *Risk Analysis*.
16. Elms, D. G. (1992). Risk assessment. In D. I. Blockley (Ed.), (1982). *Engineering Safety*. London: McGraw-Hill.
17. Karimi, I., & Hüllermeier, E. (2007). Risk assessment system for natural hazards: A new approach based on fuzzy probability. *Fuzzy Sets & Systems*, *158*(9), 987–999.
18. Department of Homeland Security. (2006). *Infrastructure Taxonomy*. Version 2.
19. Ayyub, B. M., & McCuen, R. H. (1999). *Probability, Statistics, and Reliability for Engineers and Scientists*, 2nd ed. Boca Raton, FL: Chapman & Hall/CRC.
20. Modarres, M. M., Kaminskiy, M., & Krivstov, V. (1999). *Reliability Engineering and Risk Analysis: A Practical Guide*. New York: Marcel Deckker.
21. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*. Florida: Chapman & Hall/CRC Press.
22. Washburn, A. R. (2002). *Notes on Firing Theory*. Naval Postgraduate School. Available at http://http://diana.cs.nps.navy.mil/∼arwashbu/Files/FiringTheory.pdf.
23. Fischer, R. J., & Green, G. (2004). *Introduction to Security*, 7th ed. MA: Elsevier.
24. Conrath, E. J., Krauthammer, T., Marchand, K. A., & Mlakar, P. F. (1999). *Structural Design for Physical Security: State of the Practice*. Virginia: ASCE.
25. Hicks, M. J., Snell, M. S., Sandoval, J. S., & Potter, C. S. (1999). Physical protection systems—Cost and performance analysis: A case study. *IEEE AES Systems Magazine*, April 1999.
26. Dubois, D., Grabisch, M., Modave, F., & Prade, H. (2000). Relating decision under uncertainty and multicriteria decision making models. *International Journal of Intelligent Systems*, *15*(10), 967–979.
27. Enders, W., & Sandler T. (2005). *After 9/11: Is it All Different Now?* Working Paper. Available at http://www.cba.ua.edu/∼wenders/after_911_ms.pdf.
28. Fuqua, P., & Wilson, J. V. (1977). *Terrorism: The Executive's Guide to Survival*. Texas: Gulf Publishing Company.
29. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Complex networks: Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, December 2001.
30. McGill, W. L., & Ayyub, B. M. (2006). Quantitative techniques for terrorism warnings analysis. Presented at the 2006 Society for Risk Analysis Annual Meeting, Baltimore, Maryland, 3–6 December 2006.
31. McGill, W. L., & Ayyub, B. M. (2005). Quantitative intelligence analysis: application of the transferable belief model to the analysis of competing hypotheses. Presented at the 2005 Society for Risk Analysis Annual Meeting, Orlando, Florida, 4–7 December 2005.