Quantitative Risk-Based Analysis for Military Counterterrorism Systems

Kujawski, Edouard

2007

http://hdl.handle.net/10945/44442

Quantitative Risk-Based Analysis for Military Counterterrorism Systems*

Edouard Kujawski† and Gregory A. Miller

Systems Engineering Department, Naval Postgraduate School, Monterey, CA 93943

Received 11 October 2006; Revised 25 January 2007; Accepted 9 April 2007, after one or more revisions
Published online in Wiley InterScience (www.interscience.wiley.com).
DOI 10.1002/sys.20075

ABSTRACT

This paper presents a realistic and practical approach to quantitatively assess the risk-reduction capabilities of military counterterrorism systems in terms of damage cost and casualty figures. The comparison of alternatives is thereby based on absolute quantities rather than an aggregated utility or value provided by multicriteria decision analysis methods. The key elements of the approach are (1) the use of decision-attack event trees for modeling and analyzing scenarios, (2) a portfolio model approach for analyzing multiple threats, and (3) the quantitative probabilistic risk assessment matrix for communicating the results. Decision-attack event trees are especially appropriate for modeling and analyzing terrorist attacks where the sequence of events and outcomes are time-sensitive. The actions of the attackers and the defenders are modeled as decisions and the outcomes are modeled as probabilistic events. The quantitative probabilistic risk assessment matrix provides information about the range of the possible outcomes while retaining the simplicity of the classic safety risk assessment matrix based on Mil-Std-882D. It therefore provides a simple and reliable tool for comparing alternatives on the basis of risk including confidence levels rather than single point estimates. This additional valuable information requires minimal additional effort. The proposed approach is illustrated using a simplified but realistic model of a destroyer operating in inland restricted waters. The complex problem of choosing a robust counterterrorism protection system against multiple terrorist threats is analyzed by introducing a surrogate multi-threat portfolio. The associated risk profile provides a practical approach for assessing the robustness of different counterterrorism systems against plausible terrorist threats. The paper

*This is a US Government work, and, as such, is in the public domain in the United States of America.

†Author to whom all correspondence should be addressed (e-mail: ekujawsk@nps.edu).

Key words: terrorism; counterterrorism; threats; needs analysis; quantitative probabilistic risk assessment; risk assessment matrix; decision-attack event tree; Monte Carlo simulation

1. INTRODUCTION

The “primitive need” or “want” [Sage and Armstrong, 2000: 100] for a weapon system may typically be expressed by the customer as follows: We need a weapon system that deters or else counters terrorist threats by having superior capabilities for (1) putting ordnance on target and/or (2) preventing opposing forces from putting their ordnance on target. As systems engineers, we want to translate that primitive want into more specific, quantifiable system-level requirements. It is not sufficient for systems engineers and designers to specify and evaluate a system’s performance or capabilities only in terms of engineering metrics such as response time, accuracy, or reliability. The deployment of a weapon system is best justified in terms of its threat reduction capabilities or in the military jargon its “operational effectiveness.” Information such as the probability of defeating potential threats and the ratios of inflicted to sustained damage and casualties maps technical performance to force-level combat outcomes thus providing immediate insight into the value of a military system [Bailey, 2000].

The focus of this paper is on the protection of military systems from asymmetric attacks characteristic of today’s fourth generation warfare [Hammes, 2004]. The quantification of the risk reduction capability of protective countermeasures requires a vulnerability-threat analysis in several activities and phases of any system engineering design process. In the needs analysis and requirements analysis activities, the vulnerability-threat analysis provides the basis for translating the primitive need into terms of required operational effectiveness for countering terrorist threats. In the analysis of alternatives activities, the vulnerability-threat analysis is used to quantitatively assess the risk reduction capabilities of different protective counterterrorism options. Terrorism risk and risk reduction can then be expressed in absolute quantities such as the number of fatalities, the number and category of injuries, and the monetary value of material damage. Decision-makers are then able to compare different options on the basis of the absolute as-is vs. residual risks. This is in contrast with multicriteria decision analysis variants such as Mission Oriented Risk and Design Analysis [Buckshaw et al., 2005] that assesses and compares alternatives on the basis of an aggregated utility or value obtained as a weighted sum of the system and attacker criteria quantified in terms of utility or value.

Risk profiles and risk assessment matrices [International Council on Systems Engineering, 2004] are two of the most commonly used graphical methods for reporting and communicating risk analysis results. But they have shortcomings. The risk profile provides the spectrum of possible outcomes (monetary damage or casualties) with each magnitude having its own probability of occurrence. The abscissa is the consequence and the ordinate is the probability that a consequence of magnitude x or greater will be produced [McCormick, 1981]. The latter is also referred to as exceedance probability [Paté-Cornell, 1996]. The use of risk curves for decision-making is challenging because it requires probabilistic thinking skills. The Classic Safety Risk Assessment Matrix (CSRAM) based on Mil-Std-882D [DoD, 2000a] provides only a limited view of mishaps in terms of the probability (or frequency) of occurrence and a point-estimate for the potential outcomes. Information about extreme outcomes which is of critical importance for making robust decisions for military protection systems and safety systems is lost. Another significant shortcoming of representing risk by a single point on a two-dimensional consequence-probability graph is that risk is often incorrectly equated to the product of these two values. There is overwhelming evidence that many rational people act on the basis that risk depends more on the potential magnitude than the probability of the undesirable outcomes [Kahneman and Tversky, 1979; Tversky and Kahneman, 1992]. Based on our experience, we think that the present situation for critical decision-making under uncertainty may be characterized as follows. When presented with risk curves, the average layman is challenged by their complexity and amount of information. In contrast, the classic risk assessment matrix provides insufficient information to support the selection of a robust solution.

This paper presents a realistic as well as practical approach to quantitatively assess terrorism risk and the risk-reduction capabilities of protective counterterrorism options in terms of physical measures such as damage cost and casualty figures. The key elements of the approach are (1) Decision-Attack Event Trees (DAET) for modeling and analyzing scenarios and (2)
a Quantitative Probabilistic Risk Assessment Matrix (QPRAM) for communicating the results. Section 2 provides a critical review of risk concepts and graphical representations. Section 3 introduces the QPRAM as an extension of the CSRAM to represent the possible consequences of any mishap in terms of a two-sided confidence interval. Section 4 reviews terrorist threats and their unique risk aspects. Section 5 develops the modeling and analysis of terrorist attacks using DAETs. The approach is illustrated using a simplified but realistic model of a destroyer operating in inland restricted waters. Section 6 addresses the problem of choosing a robust counterterrorism protection system against multiple terrorist threats. It is conveniently analyzed by introducing a surrogate multithreat portfolio against which different design options can be compared. Concluding remarks including areas for future research are presented in Section 7.

2. STANDARD GRAPHICAL RISK CHARACTERIZATIONS

2.1. The Concept of Risk

Humans are intuitively familiar with the notion of risk. It entails the probability of occurrence of a mishap and the magnitude or severity of the potential outcomes. A rigorous quantitative assessment of risk should answer the following three questions [Kaplan and Garrick, 1981]: (1) What are the possible mishaps? (2) How likely is each mishap to happen? (3) If a mishap does happen, what are the possible consequences? This demands the ability to think in probabilistic terms about hazards and vulnerabilities. Risk is a complex subject laden with traps that include judgmental biases, mental misperceptions, and psychological elements [Slovic, Fischhoff, and Lichtenstein, 1982].

The occurrence and outcome of events such as terrorist attacks, acts of nature (earthquake, flood, hurricane, lightning storm, etc.), industrial and personal accidents depend on multiple complex factors (detection time, protective measures, etc.) characterized by uncertainty and probability. Depending on the circumstances, the outcome may range from negligible to catastrophic. Risk is then associated with a spectrum of possible outcomes with each having its own corresponding probability of occurrence. It can be properly characterized by plotting the exceedance probability vs. the magnitude of the consequence expressed in absolute measures (monetary value and casualties). History has taught us that focusing on “typical” mishaps can be extremely misleading and short-sighted. Severity is a strong psychological effector. Low-probability/high-consequence events have therefore assumed a special importance in risk analysis and decision-making.

2.2. Risk Profile

As background material, we first consider the risk of a single-family house catching fire. Many fires are usually promptly extinguished and cause little damage. However, depending on the conditions (occupants being asleep, no or inoperative fire and smoke detectors, no or inoperative fire extinguishers, wood shingle roofs, etc.) the outcome could be catastrophic, resulting in the loss of life or spreading to other buildings [Roux, 1982]. Figures 1a and 1b depict a hypothetical but realistic Probability Distribution Function (PDF) and the associated Complementary Cumulative Distribution Function (CCDF) for the potential losses associated with an “average” single-family house catching fire. The PDF has a long tail extending into the heavy-loss regime, which is characteristic of natural hazards, industrial and personal accidents, and terrorist acts. Since Figure 1b does not incorporate the frequency of the mishap, it depicts the risk conditional on the occurrence of mishap which is also referred to as severity (Mil-Std-1629A [DoD, 1980: 9]). Statistical parameters are of critical importance to the insurance industry. But to the impacted parties, the financial damage of a house catching fire has a specific monetary value and it is not given by any statistical parameter such as the median ($30K), most likely value (~$9K), or the mean ($38K).

We note that the above data are conditional given the occurrence of a fire. To determine premiums, insurers also require the frequency per year of a house catching fire. There is an important conceptual distinction be-

![Figure 1a. Probability distribution for the possible monetary losses resulting from an “average” house catching fire. This is hypothetical data modeled using a Weibull distribution fitted to the following parameters: Location: 0, 50th percentile: $30K, 90th percentile: $80K. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.](Image not provided)
tween “probability” and “frequency” [Crellin and Smith, 1982: 2–20]: “…statistics, as a subject, is the study of frequency-type information. That is the science of handling data. On the other hand, probability as a subject is the science of handling the lack of data.” Statistical data of an average of 1 in 200 houses catching fire per year equates to a frequency of a house catching fire per year of 0.005 [Center for Educational Technologies, 2006]. There are additional regional, house condition, and resident specific factors that play important roles in the probability of a house catching fire and the severity of the consequences; but these are beyond the scope of this paper. The risk profile in Figure 1c is obtained by multiplying the probabilities of the severity profile in Figure 1b by the frequency per year of a house catching fire. Note that the range of the magnitude of the potential losses has not changed. This is consistent with the notion that risk involves both the probability of occurrence of a mishap and the spectrum of potential outcomes. If the probability of a mishap is negligible, the associated risk is negligible; the severity, however, remains unchanged. In the above illustrative example, the expected loss per year of a house that catches fire is $190 while the expected severity is $38K. Most homeowners willingly pay a premium based on the expected loss per year of $190 to be insured and thereby transfer the risk of a fire to an insurance company. Given the validity of the insurer’s risk analysis and sound business practices, the latter is economically capable of accepting the risk based on actuarial data, premiums, and its client database.

An important property of the CCDF is that its integral from minimum to maximum equals the expected value of the associated random variable [McCormick, 1981]. The area under the curve in Figure 1b equals the expected monetary loss given that the house catching fire. The area under the risk curve in Figure 1c equals the expected monetary loss times the frequency per year of the house catching fire.

A customary definition of risk $R_i$ of a mishap $E_i$ with probability of occurrence $P_i$ and mean consequence $C_i$ is [McCormick, 1981: 231]

\[ R_i = P_i \times C_i \]  

Although Eq. (1) is extensively used to quantify risk, it provides only limited insight into risk and its applicability for decision-making is subject to sound criticism [Haimes, 2004].

2.3. The Classic Safety Risk Assessment Matrix (CSRAM)

Risk assessment matrices are widely used to characterize program risks [Defense Acquisition University, 2002] and safety risk [Mil-Std-882D, 2000]. Given that terrorism results in property damage and casualties similar to safety risk, we consider the CSRAM shown in Figure 2. The columns indicate the mishap severity either qualitatively (Catastrophic, Critical, Marginal, Negligible) or quantitatively (damage in monetary value, numbers, and types of casualties). The rows indicate the mishap frequency either qualitatively (Frequent, Probable, Occasional, Remote, Improbable) or quantitatively. We note that the label of “frequency” is consistent with the Mil-Std-882D description of “mishap probability” as “potential occurrences per unit of time, events, population, items or activity” (Mil-Std-882D [DoD, 2000: 18]). Figure 2 also depicts the DoD-
suggested quantitative guidelines for classifying risks as High, Serious, Medium, and Low. It is important to note that individual organizations should substitute their own definitions and/or use other measures of damage and frequency appropriate to the domain of interest.

It is common practice to represent any mishap $E_i$ as a point on the CSRAM:

$$E_i \equiv (\text{Severity}, \text{Frequency}). \quad (2)$$

When quantitative data are available for severity and frequency, the risk of mishap $E_i$ is then typically quantified as the product of the frequency and severity in accordance with Eq. (1). The frequency of a mishap depends on its probability of occurrence, the time interval, and the number of units. It represents the mean number of mishaps per the specified time interval and it may be greater than 1. For accidents caused by system failures or external events the frequency can be computed using available reliability databases [O’Connor, 2002]. The severity that appears in Eq. (2) is ambiguous and conflicting recommendations have been made for the “best point-estimate” to assign to the spectrum of possible outcomes represented by the severity profile. These include:

1. “Measure of the most reasonable credible mishap...”  [Mil-Std-882D (DoD, 2000: 18)]
3. “…Worst credible” is a reasonable worst case, not the worst conceivable case” [Kaiser Permanente, 2002: 8].

The first three definitions are vague and at best subjective making comparisons difficult and, given the state of confusion, possibly invalid. Unfortunately, they are still extensively used, which is indicative of a serious problem with the practice of risk analysis. Only the “expected value” provides a mathematically rigorous and practical definition for a point-estimate. Consider the example in Section 2.2. The risk of a house catching fire assuming a 40-year life and no casualties or injuries is represented by the point ($38K, 0.2$). The expected monetary value of the damage over the life of the house is $7.6K$. This is consistent with the fact that the expected risk for a period of 40 years corresponds to 40 annual premiums based the $190 figure (today’s dollars). Using the CSRAM in Figure 2, the example house catching fire is a Category 3A risk (severity: marginal, probability: frequent). Consistent with the need for tailoring the CSRAM as indicated above, another classification or set of scales seems more appropriate for categorizing the risks of individual home fires.
2.4. Risk Profile vs. Classic Safety Risk Assessment Matrix

For any mishap, the CRSM depicts the probability or frequency of occurrence and the expected value of the possible outcomes. By specifying only the expected value, critical information about extreme events is lost and the CRSM fails to provide a detailed view of risk. Additional information is lost in Eq. (1) since it characterizes risk in terms of a single number given as the product of the probability and the severity values of the corresponding CRSM point. This further equates low-probability/high-severity and high-probability/low-severity events, which is a fallacy since, as discussed in the Introduction, many rational people prefer to act on the basis that risk depends more on the magnitude than the probability of the potential undesirable outcomes [Tversky and Kahneman, 1992]. This is especially relevant when discussing terrorism risks. Given their experience, many rational people have developed a commonsense recognition that asserted probabilities are often wildly unreliable and become understandably suspicious whenever they hear “Oh, don’t worry; they would NEVER do that….”

For robust decisions, one needs to consider a more general interpretation of risk than given by the CRSM and Eq. (1). Furthermore, the expected risk values of low-probability/high-consequence events obtained from experts using ad-hoc methods are highly prone to error and have been shown in numerous cases to differ from each other by orders of magnitude. Risk profiles can be used to mitigate this problem because they require the experts to focus on the spectrum of possible outcomes, including extreme events. When hard data is lacking, risk profiles can be systematically assessed using the Direct Fractile Assessment (DFA) method which elicits three percentiles (typically the 90th, 50th, and 10th percentiles) from experts [Dillon, John, and von Winterfield, 2002]. This avoids (1) the fallacy that it is easier to provide a single point estimate than a range for an uncertain quantity and (2) being trapped by a false sense of confidence. We note, however, that, even with major efforts, it is often not possible to identify all of the possible mishaps or to have a sound basis for estimating where the 10% and 90% limits lie. Nonetheless, experience indicates that it is well worth trying.

While we strongly advocate the use of risk profiles, our experience is that laymen typically have difficulty interpreting and using them for decision-making. To address this issue, this paper proposes the QRPM as an alternative tool for comparing military counterterrorism systems and other risk reduction options. As discussed in the following section, the QRPM maintains the simplicity of the CRSM while providing some key risk profile data.

3. QUANTITATIVE PROBABILISTIC RISK ASSESSMENT MATRIX (QRPM)

The QRPM is proposed as an extension of the CRSM to effectively provide quantitative probabilistic information about a mishap’s severity and probability (or frequency). We describe the approach using the QRPM depicted in Figure 3. The key features are:

1. The consequence and probability axes are oriented so that the farther from the origin a mishap is plotted, the higher the risk.
2. The use of a logarithmic scale on each axis.
3. The mishap risk categories (High, Severe, Medium, Low) are defined by isorisk contours, \( R_c = P \times C = \text{constant} \). These are parallel straight lines when plotted using log scales for \( P \) and \( C \).
4. The expected risk of a mishap is depicted by the point (expected consequence, frequency of occurrence).
5. The magnitude of any mishap is specified in terms of the confidence interval \([L(50\%), U(90\%)]\) [Martz and Waller, 1982].

![Figure 3. Example of a quantitative probabilistic risk assessment matrix. The data points correspond to the 50th percentile, expected value, and 90th percentile risks for single-family house catching fire given the “as-is” condition presented in Section 2.2 and a hypothetical fire control approach, Option A. The scales and risk categories correspond to Mil-Std-882D. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]](image-url)
6. The frequency (or probability) of the $x$th percentile endpoint is modeled in terms of the frequency of occurrence of the mishap and the percentile of the expected value of the consequence, $x_e$, as follows:

$$\text{Freq}(x^{\text{th} \text{ percentile}}) = \left(\text{Freq. of occurrence}\right) \times \frac{(1 - x)/(1 - x_e)}.$$  \hspace{1cm} (3)

Given that for a continuous distribution the probability of any specific value is infinitesimal, Eq. (3) is offered as a pragmatic approach to plot the endpoints, $L(50\%)$ and $U(90\%)$, in the probability-consequence space of the QPRAM.

The first two modifications to the CSRAM are consistent with the Government Electronics and Information Technology Association G-48 System Safety Committee recommendations [2006]. A log scale is especially useful for monetary losses associated with accidents, acts of nature, and terrorist acts while a linear scale may be more appropriate for casualties. Property 3 provides a convenient and reasonable mathematical representation of the Mil-Std-882 risk categories. Users may need to modify (1) the probability and consequence ranges and (2) the risk categories to effectively represent their specific circumstances. That is, the location and definition of regions representing High, Severe, Medium, and Low risk categories should be determined by the organization that would suffer the loss. Property 4 provides a well-defined representation of expected risk. Properties 5 and 6 provide key risk profile data that are especially useful for mishaps with low-probability/high-consequence outcomes.

We propose the following procedure for developing the QPRAM for any mishap:

1. If possible, obtain consequence data from detailed analyses or past occurrences. Otherwise, elicit the $10^{\text{th}}$, $50^{\text{th}}$, and $90^{\text{th}}$ percentiles of the possible damage or other consequences such as casualties from experts using the DFA method. Consideration should be given to aggregating the opinions of several experts [Vose, 2006] as well as using sensitivity analysis.

2. To facilitate the subsequent analysis, characterize the severity profile using a realistic PDF. When fitting hard data, the PDF should pass an appropriate goodness of fit test [Hines and Montgomery, 1980]. For use with the DFA method, we advocate the use of the three-parameter Weibull distribution because it is flexible enough to fit three arbitrary percentiles [Kujawski et al., 2004]. The triangular distribution, because of its restrictive shape, lacks this capability.

3. The expected value of the possible outcomes (monetary damage, casualties, etc.) is obtained from the fitted PDF.

4. The frequency of occurrence is assessed using available failure-rates databases or expert judgment.

5. The frequency of occurrence of the mishap is associated with the expected value of the severity distribution.

6. The frequencies associated with $L(50\%)$ and $U(90\%)$ are obtained using Eq. (3).

The additional effort required to create a QPRAM from a credible CSRAM is minimal. Steps 1–3 are necessary to obtain credible estimates of the expected damage. Steps 4 and 5 are necessary to obtain credible estimates of the frequency of occurrence. Steps 1–5 are therefore equally necessary for the CSRAM and the QPRAM. Step 6 simply uses Eq. (3) to generate the additional risk data depicted by the QPRAM. The curve connecting the three points defined in steps 5 and 6 is a simple interpolation.

The data in Figure 3 labeled “As-is” corresponds to the example in Section 2.2. It captures key information of the risk profile in Figure 1c. Figure 3 also depicts the risk reduction benefits of a hypothetical fire control Option A, which might include stricter fire codes for building materials and mandatory improved fire detection and protection systems. The probability of a fire occurring and the associated severity are both reduced. Figure 3 also illustrates that a single mishap can belong to multiple risk categories and the limitations of using single point-estimates.

We consider the QPRAM to be a valuable enhancement of the CSRAM. It retains the simplicity of a two-dimensional plot while providing critical risk profile information for low-probability/high-severity events. It can readily accommodate several different mishaps and risk reduction options and thereby it provides a simple graphical tool for communicating the key results of an elaborate risk analysis. Decision-makers then have readily accessible quantitative data about the possible outcomes which they can use to support the selection of robust options.

4. CHARACTERISTICS OF TERRORIST ATTACKS

4.1. Terrorism Risk vs. Safety Risk

Terrorism risk has much in common with the notion of safety risk discussed in Sections 2 and 3. But there are
some significant conceptual differences between those that entail modifications to safety probabilistic risk analysis methods. Acts of nature and accidents behave as stochastic events; they can be evaluated using statistics and reliability databases. In contrast, terrorist threats are deliberate acts by adversaries for the purpose of causing damage and casualties. To quote Woo [2002, p. 8]: “Terrorists, on the other hand, are both subtle and malicious.” New terrorist threats are being continuously developed and will certainly be carried out if they have the potential for high-impact whether individually or cumulatively over the long term. The frequency of terrorist attacks is therefore extremely difficult, if not impossible, to assess. It requires “thinking like the enemy” [Sheffi, 2005: 55]. The use of “red” and “blue” teams is a useful approach to estimate the relative probability of potential attacks and prioritize defenses. There is much ongoing research on terrorism in psychology [Horgan, 2006], game theory [Fricker, 2006], security models [Bier, 2006], terrorist models [Goldstein, 2006], and other fields likely to provide valuable insight into future terrorist attacks.

Implementing protection systems for high-value units can have a significant impact on terrorism risk by reducing (1) the probability of an attack being carried out, (2) the probability of an attack being successful, and (3) the severity of a successful attack. Decisions dealing with terrorism risk also need to take into account the number of potential targets and years of operation similar to the Mil-Sdt-882D safety risk assessment of a fleet or inventory [DoD, 2000a]. It should, however, be noted, as pointed out by Bier and colleagues [Bier, 2006], that the net effect is likely to be less than desired since terrorists may redirect or refocus their attacks. These are some of the reasons that, as discussed in Section 2.4, rational people prefer to act on the basis of the potential magnitude of the consequences rather than asserted probabilities, especially when dealing with terrorist threats.

Given the above issues, we consider it practical and useful to characterize terrorist risk in terms of the conditional probability of the attack succeeding, given that it has been launched and the spectrum of possible outcomes. The standard risk assessment methods discussed in Sections 2 and 3 can then be applied with the following slight modifications: (1) “probability” is associated with the “conditional probability” that the attack is “successful” given that it is launched and (2) “consequence” is associated with the spectrum of possible damage inflicted upon the defending side. Since this risk is conditional on the attack having been launched, we refer to it as “conditional risk.” We note that this “conditional risk” should not be confused with the “conditional uncertainty analysis” discussed by Paté-Cornell [1999], who considers a family of risk curves conditional on a set of hypotheses.

4.2. Risk-Based System Engineering Approach

The design of robust and cost-effective counterterrorism systems requires a systematic approach that includes analyzing target vulnerabilities and comparing different options against a comprehensive set of present and future threats. Systems engineering with its multidisciplinary focus is well suited to tackling this complex problem [Mackey et al., 2003; Mackey, 2006]. We propose the following nine-step process that is built upon several previous models which consist of the “secure system engineering methodology” [Salter, Saydjari, and Schneier, 1998], the “six-step ship defense analysis process” [Farris and Stuckey, 2000], and the “seven-task methodology for integrating risk management and allocation of resources in antiterrorism” [Parnell, Dillon-Merrill, and Bresnick, 2006]:

1. Identify critical assets for potential targets.
2. Analyze their vulnerabilities.
3. Characterize the adversaries:
   - Identify a comprehensive set of plausible present and near-term threats.
4. Define a set of distinct threats, referred to as the design-basis threat set, for detailed analysis.
5. Analyze the design-basis threat set:
   - Determine the conditional probabilities of successful attacks
   - Quantify the outcomes in quantitative measures such as monetary value of damage, number and types of casualties, lost time, etc.
6. Decide on the need for additional protective countermeasures
   - If none required, stop.
   - Else, proceed to step # 7.
7. Identify protective countermeasure options:
   - Develop system architecture
   - Develop concept of operations.
8. Evaluate the different options:
   - Effectiveness and robustness of threat risk reduction capability
   - Risk of collateral damage
   - Availability, flexibility, etc.
   - Cost.
9. Select the preferred option based on the above criteria.

All of the above nine steps are difficult and critical to support a sound decision. Step 3 is arguably one of the most challenging because this is where the unique
aspects of terrorism threats discussed in Section 4.1 need to be addressed. Techniques such as setting up “red” and “blue” teams and the use of facilitators encourage “thinking like the enemy” and help develop a broad spectrum of perspectives. In Step 4, it is essential to ensure that the design-basis threat set stresses the functions of detection, identification, and deter or defeat for different attack types, environmental conditions, and geographical locations. In Step 5 we advocate using the scenarios developed in Step 4 to translate the sensor and weapon performance characteristics into operational effectiveness or risk reduction capability measured in absolute terms such as casualties, kill/loss ratios, probability of mission success, etc. For Step 6, one requires criteria for decision-making. For example, it seems reasonable based on the DoD risk management guidelines [Department of the Navy, 2006] that a protection system should address all attacks with conditional probability of success greater than 10% and consequences with severity catastrophic or critical.

Robustness is a key criterion for the design and selection of a protection system as specified in Steps 7–9. The “robust decision approach” advocated by Lempert, Pepper, and Bankes [2003: 44–45] provides a useful guideline for the design of robust protective counterterrorism systems. The four key elements are:

1. “Consider ensembles of large numbers of scenarios.”
2. “Seek robust, rather than optimal strategies that perform well enough by meeting or exceeding selected criteria across a broad range of plausible futures and alternative ways of ranking the desirability of alternative scenarios.”
3. “Employ adaptive strategies to achieve robustness.”
4. “Design the analysis for interactive exploration of the multiplicity of plausible futures.”

In Section 6 we present a multi-threat portfolio approach whereby the large number of plausible terrorist threats is reduced to a single composite threat. This provides a practical and effective way to evaluate the different options (Step 8) and ensure the selection of robust options (Step 9).

The outcome of a terrorist attack depends on many parameters such as the target vulnerabilities, the attackers’ capability and strategy, the defenders’ detection and response times, all of which are characterized by variability and uncertainty. Consequently, the resulting damage is more accurately and realistically represented by probability distributions than expected values. An analysis based on a probabilistic risk assessment approach is presented in Sections 5 and 6.

5. DECISION-ATTACK EVENT TREES (DAETs)

5.1. Modeling Attack Scenarios

Decisions and event trees include the notion of time with events on the right occurring after those on the left. They therefore provide a useful tool for modeling and analyzing terrorist attacks where the sequence of events and outcomes are time-sensitive [Martz and Johnson, 1987]. The outcomes of terrorist attacks depend on (1) the actions of the attackers and the defenders which are treated as decisions, and (2) the properties of sensors, weapons, and target vulnerabilities which are treated probabilistically. We choose to use decision/event trees rather than attack trees or fault trees because (1) they can better handle temporal relationships among events [Paté-Cornell, 1984] and (2) they conveniently capture attack and defense decisions and the probabilistic aspect of outcomes. To differentiate the battle-applied decision-event trees approach from attack trees [Schneier, 1999], we refer to them as Decision-Attack Event Trees (DAETs).

Consider the attack on a destroyer operating in inland restricted waters by terrorists in a speed boat loaded with explosive charges, as depicted in Figure 4. The U.S. Navy has adopted a layered defense scheme around ships that defines three zones for the rules of engagement: assessment, warning, and threat [Department of the Navy, 2006]. The probability of the attackers entering the threat zone to cause significant damage to the destroyer depends on (1) avoiding being identified as a threat by blending with neutral commercial and recreational boats and (2) approaching undetected because poor weather and sea conditions reduce the effectiveness of the ship’s sensors [Wagner, Mylander, and Sanders, 1999] or limited operational status of the crew and sensors. Time is a critical factor in the attack scenario and its outcome. The performance of the sensors and command and control systems and the response time of the crew determine their ability to detect and identify the threat in time to defeat it and mitigate damage and casualties. The sooner the threat is detected and identified, the greater the opportunity for multiple engagements resulting in a higher probability of defeating it and minimizing the severity of the consequences.

Figure 5 depicts a simplified DAET corresponding to the Figure 4 scenario. The DAET includes decision nodes (square) and chance nodes (circle). Once the attackers have selected the target, they are faced with the decision of selecting under which visibility and sea conditions to attack. This is represented by a decision node and, for simplicity, three branches corresponding to the following options: attack under excellent visibil-
ity and sea state 0 or 1 conditions (denoted by Ex_Co); attack under average visibility and sea state 2 or 3 conditions (Av_Co); attack under poor visibility and sea state 4 or above conditions (Po_Co). We aggregate the sequence of events to simplify the modeling of detect, identify, warn, engage, and defeat the attackers. The probabilities of detect, classify, deter, and defeat for the different ranges and the damage values are hypothetical. They are provided as a means to illustrate the approach. Of special interest is the fact that the

Figure 4. Scenario of an attack on a destroyer operating in inland-restricted waters by terrorists in a speed boat loaded with explosive charges. (Destroyer: blue; terrorists: orange.) [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

Figure 5. Decision-attack event tree for the terrorist attack depicted in Figure 4 for three different weather and sea conditions. The labels are as follows:
P1_T1: Scenario identifier where P1 denotes the shipboard protection system Option P1 and T1 denotes a terrorist attack in a speed boat loaded with shaped charges
Ex_Co: Attack under excellent visibility and sea state 0 or 1 conditions
Av_Co: Attack under average visibility and sea state 2 or 3 conditions
Po_Co: Attack under poor visibility and sea state 4 or above conditions
DE_Gt_500y: Attackers detected and classified at greater than 500 yards
DE_500_300: Attackers detected and classified within 500 and 300 yards
DE_300: Attackers detected and classified within 300 yards
KE: Attackers are deterred or stopped before setting off the detonation
NKE: attackers are not stopped before setting off the detonation.
Each outcome branch is quantified by a probability (1st number) and the inflicted damage specified by a Weibull distribution with 10th, 50th, and 90th percentiles in $M$ or location (0, 50th, and 90th percentiles.)
outcome consequences are modeled using distributions rather than point estimates or abstract utility measures [Haimes, 2004; Kujawski, 2002]. The potential outcomes (outmost right branches) are modeled and quantified using Weibull distribution specified in terms of the 10th, 50th, and 90th percentiles in accordance with the DFA method; i.e. the damage of each possible outcome is given by Weib(10th, 50th, 90th percentiles). (When the minimum damage is negligible, the Weibull distribution is assumed to have location 0 and the 10th percentile is not used.) It should be noted that even in those instances where a “kill” occurs, some damage may result. The use of PDFs in DAETs provides a powerful framework for modeling and analyzing risk. The complexity of DAETs increases with the desire or need for a higher level of fidelity.

Figure 6 depicts the monetary value of the ship damage. The data is largely hypothetical with the one exception being the use of the USS Cole attack data [Perl and O’Rourke, 2001] for calibration purposes. This was a dramatic event: 17 crewmembers dead, 39 crewmembers injured, serious damage with a repair cost of about $250M in 2001 dollars, and an outage of approximately 18 months. The DAET in Figure 5 can readily be used to assess all these consequences by assigning the corresponding values to the outcome branches. The outcome is then given by a set of risk curves corresponding to the inflicted damage, crew injuries, loss of lives, and unavailability. The problem of comparing risk curves is further compounded by the challenging problem of dealing with different measures. One possible approach is to tie all outcomes to monetary figures using some established scale [DoD, 2000b], thereby avoiding the introduction of abstract utility measures. We consider this a political problem outside the scope of this paper.

5.2. Quantifying Attack Scenarios

As discussed in Section 2.1, we think that risk is too complex a concept to be quantified by a single number. We therefore do not apply the “folding back” procedure of standard decision tree analysis [Clemen and Reilly, 2001] whereby each option is characterized simply by its expected value. Instead, we explicitly evaluate the “conditional risk” profiles for the three attack options depicted by the DAET in Figure 5. The results presented in Figure 6 were obtained by performing Monte Carlo simulations for each individual sub-tree (Ex_Co, Av_Co, Po_Co) using Crystal Ball®. (We note that these calculations can be performed using a number of commercial software tools such as @Risk, Analytica, TreeAge, etc.). The defenders face the highest risk when attacked under poor visibility and rough sea conditions.

Alternatives to the DFA method based on high-fidelity models are highly desirable to achieve greater credibility. These include simulation tools such as the Naval Simulation System, NSS21 [Metron, 2006] with capabilities to (1) model the entire detect-to-engage sequence, (2) incorporate high-fidelity models of the sensors, weapons, and humans, and (3) generate fragility or damage curves based on realistic structural models. However, these detailed analyses require extensive efforts and are not well suited for analyzing the large variety of threats and options that need to be considered in support of needs analysis.

5.3. Comparing Counterterrorism Options

DAETs provide a useful tool for assessing the risk reduction benefits of counterterrorism options. We continue with the scenario of the attack on a destroyer by an explosive-laden speed boat detailed in the previous section. But we now consider three conceptual ship protection systems: “As-is”, P2, and P3. Option P2 consists of an improved detection and identification system that results in a greater probability of detecting and identifying the threat at longer ranges; all other systems are “as-is”. Option P3 consists of an improved gun-based weapon system that provides a greater probability of a hit and kill at short distances; all other systems are “as-is”. The conditional risks of attack under low visibility and rough seas given these three options are depicted in Figure 7. Options P2 and P3 both reduce the probability of a successful attack and the severity of the consequences. The curves for options P2 and P3 intersect each other. Option P2 is more effective at reducing the probability of a successful attack (22% vs. 30%) and dominates option P3 for damages less than $15M. Option P3 dominates option P2 for the low-
probability/high-consequence events because it provides a superior hit-kill capability for short distances. For example, the 95th percentile damages for options P2 and P3 are $35M and $30M, respectively. Although option P2 dominates option P3 for approximately 90% of the outcomes, it has the higher value for the mean conditional risk, $9.3M vs. $7.9M. This is interesting and valuable information; but based on our experience, lay decision-makers often find it difficult to deal with. As discussed in Section 3, the QPRAM provides a simplified representation of some key risk profile data.

The QPRAM corresponding to the risk profiles in Figure 7 is displayed in Figure 8. The risk to each of the three destroyers given the scenario attack is depicted by the following three points:

- $P_{50}$ ≡ (50th percentile outcome, estimated probability of the 50th percentile).
- $P_e$ ≡ (Expected outcome, probability of attack being successful).
- $P_{90}$ ≡ (90th percentile, estimated probability of the 90th percentile).

The estimated probabilities for the 50th and 90th percentiles are computed using Eq. (3). The curves are simply Excel interpolations between the three points.

**Figure 7.** Comparison of the conditional risks of the terrorist attack depicted in Figure 4 carried out under poor visibility and rough sea conditions against identical destroyers equipped with three different ship protection systems. [Option “As-is” is identical to Figure 6 data labeled Po_Co. Option P2 is an improved detection/identification system with the following performance probabilities (see Fig. 5 for details and labels): DE_Gt_500y = 0.5, DE_500_300 = 0.4, DE_300 = 0.1. Option P3 is an improved gun-based weapon system with the following hit/kill at short distances: KE5 severity = Weib(0, 5, 15), KE6 probability = 0.7, KE6 severity = Weib(0, 10, 20), NKE6 probability = 0.3, NKE6 severity = Weib(20, 80, 200). All other parameters are as specified in Figure 5.] [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

**Figure 8.** Quantitative Probabilistic Risk Assessment Matrix corresponding to the risk profiles in Figure 7. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

The data are less cumbersome than the risk curves in Figure 7 and provide the decision-maker adequate information to make a sound decision. It is readily seen that options P2 and P3 reduce both the probability of a successful terrorist attack and its consequences. Option P2 is more effective at reducing the probability of a successful attack while option P3 is more effective at reducing the high-consequence outcomes. With this information lay decision-makers are no longer limited to making decisions based on single points as provided by the CSRAM. They can explicitly consider the extreme outcomes as decision criteria and select robust solutions thereby avoiding potential regret and disappointment [Lempert, Popper, and Bankes, 2003].

**6. PROTECTING AGAINST MULTIPLE TERRORIST THREATS**

A single scenario, such as described in Section 5, provides valuable insight into what a system needs to protect itself against a specific threat. However, a single scenario by itself is of limited value for choosing a robust counterterrorism protection system. As discussed in Section 4, the decision process needs to consider a comprehensive set of potential threats.

To proceed, we revisit the destroyer presented in Section 5 and address the many plausible terrorist threats that it faces. While the modern destroyer is a formidable weapon system in the open sea, it is vulnerable to terrorist attacks when transiting in confined waterways, moored at pier side, or at anchor [Cobian, 2002; CNO N76, 2004]. Standard open ocean sensors and weapons become ineffective due to the physical environment, safety considerations, and local restrictions. Key vulnerabilities include systems that can be
The conditional probability of threat [Vose, 2000]:

then be thought of as a generalized discrete distribution that represents the damage. For simplicity we assume that the relative frequencies of different terrorist likelihood of the different threats. To proceed we as-

duction options it is necessary to estimate the relative frequencies of different terrorist threats determined as discussed in Section 4.2, \( \{T_i\} \equiv \{T_1, T_2, \ldots, T_n\} \). Each threat \( T_i \) has a probability \( p_i \) of inflicting damage with a PDF \( C_i(x) \), where \( x \) is a random variable that represents the damage. For simplicity we define the probability of attack success as the probability that the attack penetrates the multi-layered defense zones (see Section 5.1) and inflicts some level of damage. The distribution for the attack outcome may then be thought of as a generalized discrete distribution associated with probabilistic branching [Kaplan, 1981; Vose, 2000]:

\[
T_i = \{ (p_i, C_i(x)), (1 - p_i, 0) \}. \tag{4}
\]

As discussed in Section 4, one cannot reliably predict the absolute frequency \( f_j \) of threat \( T_j \). However, in order to effectively allocate a constrained budget to risk reduction options it is necessary to estimate the relative likelihood of the different threats. To proceed we assume that the relative frequencies of different terrorist attack modes are proportional to the probability of attack success, \( p_i \), and potential consequences \( C_i(x) \). The conditional probability of threat \( T_i \) given an attack is then given by the following set of equations:

\[
f j f_j = p_j C_j(x, \text{ith percentile})/p_i C_i(x, \text{ith percentile}), \tag{5a}
\]

Equation (5a) represents the relative likelihood of each threat and Eq. (5b) provides the normalization. Given the terrorists’ preference for high impact threats and the present lack of definitive data, we think that the use of the 80th or a higher percentile is reasonable. This is a variation of the Paté-Cornell and Guikema [2002, p. 9] model, which assumes that the probability of a specific attack type is “directly proportional to the expected value of the attack scenario to the terrorists relative to all other attack possibilities that they could consider.”

With Eqs. (5) the design of robust counterterrorism systems has been transformed from a decision-making problem under uncertainty (unknown probabilities) to a decision-making problem under risk (known probabilities). One may think of the set of threats as a portfolio of threats given by a generalized discrete PDF, \( T_p \), which is built up as a composite of the individual threat risks with probability values \( f p_i \) and consequences with PDFs \( C_i \):

\[
T_p \equiv \left\{ \langle f_1 p_1, C_1(x) \rangle, \langle f_2 p_2, C_2(x) \rangle, \ldots, \langle f_n p_n, C_n(x) \rangle \right\}. \tag{6}
\]

We compute the Eq. (6) portfolio risk profile using a Monte Carlo simulation where the output of each trial is an event with severity \( C_i \). The resulting portfolio risk profile therefore properly captures the extreme outcomes of the individual threats. As discussed by Vose [2006], this would not be the case if one were to combine the individual risk profiles by multiplying them by their probabilities and summing them.

We propose to use the portfolio risk profile \( T_p \) as a surrogate for the design-basis threat set. The complex problem of dealing with multiple threats is thereby reduced to a single composite threat. That is, instead of comparing different design options against multiple threats separately, a single comparison can be made once a threat portfolio risk profile is established. Different counterterrorism options can then be compared as described in Section 5.3. The approach is graphically depicted in Figure 9.

We illustrate the proposed approach for the hypothetical case of three threats, \( T_1, T_2, \) and \( T_3 \). For simplicity, we assume that each threat has a severity profile characterized by a Weibull distribution. There is no loss
of generality since the proposed approach applies equally well to the hard-data risk profiles described in Section 5. The three threats risks and the surrogate portfolio risk profile given by Eq. (6) are plotted in Figure 10. The portfolio risk profile exhibits the appropriate characteristics. As expected, the portfolio risk profile has extreme outcomes with the magnitudes of the individual threats, principally T1 and T2, but lower corresponding probabilities of occurrence.

For completeness, we note that if one were to assume a lack of information about the terrorists’ preferences, one could model the conditional threat probabilities as random variables using probability distributions such as the uniform, Dirichlet, Beta distribution, or multinomial distributions [Moskowitz and Tang, 2000]. Another approach is to use decision-making strategies that require knowledge of only the possible outcomes and not their probabilities. These include the minimax regret criterion that is driven strictly by the worse outcome [Sage and Armstrong, 2000] or the hybrid Hurwicz criterion that weighs the best and worse outcomes [Chicken and Hayns, 1989]. These heuristic-based approaches have limitations and may lead to irrational decisions [Hazelrigg, 1996]. They are not appropriate substitutes for the use of models for assessing terrorism threats and designing cost-effective robust protection systems.

Figure 9. Process used to generate the threat risk portfolio by aggregating multiple risk profiles. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

Figure 10. Example of aggregating three terrorism-threat risk profiles into a terrorism-threat portfolio risk profile. The individual risk profiles are assumed to be given by Weibull distributions with location, 50th, percentile, and 90th percentile as follows:

- T1: PDF = Weib(0, $20M, $120M), \( p_1 = 0.35 \)
- T2: PDF = Weib(0, $40M, $100M), \( p_2 = 0.45 \)
- T3: PDF = Weib(0, $10M, $15M), \( p_3 = 0.65 \)

[Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]
7. CONCLUDING REMARKS

This paper develops a realistic as well as practical quantitative risk-based approach for the justification and selection of military counterterrorism systems. The key elements of the approach are (1) Decision-Attack Event Trees (DAETs) for modeling and analyzing scenarios, (2) a portfolio model approach for analyzing multiple threats, (3) a Quantitative Probabilistic Risk Assessment Matrix (QPRAM) for communicating the results, and (4) risk expressed in absolute quantities such as the number of fatalities, the number and category of injuries, and the monetary value of material damage. DAETs address temporal relationships among events and are therefore well suited for modeling and analyzing terrorist attacks where the sequence of events and outcomes are time-sensitive. The multithreat portfolio models the set of plausible threats as a probabilistic aggregate of the different threat risk profiles. The complex problem of dealing with multiple threats is thereby reduced to a single composite threat. The complex problem of selecting a robust protection system is thereby reduced to analyzing a single composite threat. By protecting against a set of plausible threats rather than against a worst-case scenario, the defender maintains the flexibility to protect himself against enemies when they act differently than expected. This helps avoid the decision trap of overconfidence in judgment [Russo and Schoemaker, 1989]. We therefore advocate the proposed approach which focuses on robustness and flexibility rather than approaches that seek mathematical optimal defenses. The QPRAM is an enhancement of the classic safety risk assessment matrix. It provides confidence levels rather than simply point estimates of risk while maintaining simplicity. Quantifying terrorism risks in absolute terms rather than abstract utility measures facilitates thinking of risk reduction options as insurance policies and balancing the threat risks against cost and risk reduction. The paper thereby provides a useful approach for choosing cost-effective robust counterterrorism systems.

We recognize that there are limitations to what we have presented and that additional research is warranted. We are looking to this paper as a springboard for such research. In this paper we consider only a single mode of attack per event. Even the concept of a “portfolio of threats” is merely a compilation of several attack modes all occurring separately. In reality, an enemy could combine threats in “waves,” such as coordinated subsurface and air attacks which arrive at the same target nearly simultaneously. A high-fidelity battle simulation tool would then be better suited than DAETs to produce the necessary damage curves. However, the final QPRAM would look the same as presented in the paper. We also limited the discussion and example a to point-defense solution. In actuality, application of command and control warfare, nonlethal engagements, and other means to disrupt the planning and preparation for an attack before its execution would further reduce terrorism risk [Drozdova and Kunz, 2007]. The consequences of incorrectly identifying and engaging a neutral or friendly platform as an attacking enemy have not been addressed. The requirement to avoid collateral damage is a significant design driver. Further work will consider such occurrences.

Although the proposed approach is illustrated for terrorist threats to a destroyer operating in inland restricted waters, it can be applied to the protection of any system, including infrastructure systems and threats associated with accidents and acts of nature. We think that the paper provides a useful framework for the development and implementation of quantitative risk-based needs analysis for a large class of protection systems. Communication is a particularly important aspect of risk analysis, and we propose the QPRAM as a robust and straightforward means to represent and communicate results and compare different risk-reduction options.

ACKNOWLEDGMENTS

This work was performed as part of the Naval Postgraduate School institutionally funded research. The authors thank David Lum and Michael Terry, two Naval Postgraduate Students who worked on the Deterrence of Naval Threats MSSE capstone project, for their inputs to the scenario presented in Section 5. They also gratefully acknowledge five anonymous reviewers, who through their thorough reviews, insightful comments, and excellent suggestions have significantly contributed to the quality and content of the paper.

REFERENCES


Department of Defense Instruction 6055.7, Accident Investigation, Reporting and Record Keeping, DoD, Washington, DC, 2000a.

Department of the Navy, NTPP 3-07.2.1, Antiterrorism/force protection, Washington, DC, 2006.


Edouard Kujawski is an Associate Professor in the Systems Engineering Department at the Naval Postgraduate School. His research and teaching interests include the design and analysis of high reliability/availability systems, risk analysis, and decision theory. He received a Ph.D. in physics from MIT following which he spent several years in research and teaching physics. He has held lead positions at General Electric, Lockheed-Martin and the Lawrence Berkeley National Laboratory. He has contributed to the design of particle accelerators and detectors, space observatories, commercial communication systems, the Space Station, and nuclear power plants. He was a participant and contributor to the Lockheed Martin LM21 Risk Management Best Practices and the original INCOSE Systems Engineering Handbook. He is a member of the San Francisco Bay Area Chapter of INCOSE, where he serves on the board of directors.

Gregory Miller is a Lecturer in the Systems Engineering Department at the Naval Postgraduate School in Monterey, CA. He teaches courses in C4ISR Systems, Weapons Systems Technology, Sensor Systems Technology, Systems Engineering, Systems Software Engineering, and Project Management. He was recently awarded the Wayne E. Meyer Award for Excellence in Systems Engineering. He has 20 years active-duty and civil service experience in ship system life cycle engineering and acquisition. This included tours at public shipyards, at in-service engineering agents, and at PEO (C4 & Space). He has a B.S. in Electrical Engineering from the U.S. Naval Academy (1987) and a M.S. in Electrical Engineering from the Naval Postgraduate School (1992). He is a member of the Department of Defense Acquisition Corps. He is also an Engineering Duty Officer in the U.S. Navy Reserves.