

Models and Methods for Counter-Terrorism Resource Allocation and Risk Management

Don Kleinmuntz

There is widespread recognition that there is a need to development sophisticated and effective analytic approaches for risk-based allocation of resources to counterterrorism. Implementing these methods requires credible and accurate quantitative assessments of the threats, vulnerability, and consequences of terror attacks, as well as valid assessments of how countermeasures will impact the nature and degree of threat, vulnerability, and consequences. There are three topics associated with this project.

Topic 1: Robust Portfolio Methods for Resource Allocation

Experience suggests that efforts to implement these models will often encounter difficulties in obtaining credible inputs. Several difficulties are particularly salient:

1. Quantitative threat assessments expressed as the probability of an attack can be difficult to obtain, although it may be easier to express judgments of relative threat or to rank order threats.
2. Vulnerability assessments of potential targets require expert analyses that can be both expensive and time consuming, particularly when the list of potential targets is long. Resource allocation may have to depend on vulnerability assessments that are incomplete, out of date, or both.
3. Consequence assessments ought to include both direct consequences (fatalities, injuries, damage to property) as well as indirect economic consequences of an attack. While researchers at CREATE and elsewhere have made significant progress in the economic modeling of indirect consequences, it is not uncommon for different estimates to diverge, in some cases across a fairly wide range.

Decision analysis models can become difficult to use or interpret when model parameters are vague and incomplete. My approach is to identify robust solutions that perform well across a range of plausible parameter values. A traditional way to do this is through sensitivity analysis. A more powerful and compelling alternative is to extend a method called Robust Portfolio Modeling (RPM), previously applied to multi-criteria projects under certainty, to the area of risk-based resource allocation. This is a computationally intensive approach that relies on a dynamic programming algorithm for computing all non-dominated portfolios of counterterrorism measures, subject to incomplete information about risks and risk management plans (e.g., ordinal threat assessments and/or range-based rather than point estimates other parameters). A basic algorithm for RPM in infrastructure protection has already been developed and tested for a portfolio of approximately 30 sites. The Year 5 goal for this project is (a) to test and validate this algorithm in the domain of port infrastructure protection, using disguised real world data from the project currently under way with the Port of Los Angeles; (b) to test and validate this algorithm in the domain of Internet Information Technology Infrastructure security and disaster recovery planning, using disguised real world data from Strata Decision Technology, a software application developer based in the Midwest; and (c) develop a prototype for a working software tool that implements the algorithm and promotes its ease of use. This project is complementary to and provides methodological guidance to applied resource allocation and risk management efforts, including potential applied analyses in support of DHS or state/local agencies.

Major Milestones and Dates:

- Working paper describing RPM approach -- September 2008
- Computational work on port security data -- September 2008
- Working paper on port security application -- December 2008
- Computational work on IT security data -- December 2008
- Working paper on IT security application -- March 2009
- Software prototype -- September 2009

Topic 2: Endogenous Threats in Risk-Based Resource Allocation Models

One of the most challenging issues in counterterrorism resource allocation is the endogenous nature of terror threats: Since terrorists dynamically assess potential targets, making a target less vulnerable or mitigating the consequences of an attack may also reduce the threat against that target and make other targets, by comparison, more attractive to terrorists. Several CREATE projects have focused on game theoretic models that model terrorists as a rational opponent trying to anticipate counterterrorism measures and adapt their behavior accordingly. Other relevant work includes work by CREATE on formal modeling of terrorist preferences. The topic will focus on formulating optimization models that incorporate endogenous threat assessments based on plausible models of terrorist preferences. Specifically, the model will assume threat probabilities are affected by protective measures that impact the vulnerability or consequences of attacks on a set of targets. These models involve formulation and solution of nonlinear optimization problems. I will formulate several candidate models and evaluate them from the perspective of (a) availability and feasibility of solution methods; (b) assessment issues and challenges; and (c) more general questions of feasibility of practical implementation, including but not limited to these two points.

Major Milestones and Dates:

- Model formulation -- March 2009
- Development of test models using data from IT, port security or other settings -- June 2009
- Working paper describing analyses and evaluation of models -- September 2009

Topic 3: Why use Optimization Methods for Resource Allocation Decision Making?

A number of investigators have proposed using risk-based resource allocation methods that rely on various ad-hoc rules of thumb or heuristic methods to assess risk and prioritize counter-terror measures. This work will evaluate the value added from using optimization methods combined compared to these less formal approaches, with a particular focus on identifying situations where optimization will be of greatest use. The objective of this work is to provide practical guidance on when to use formal mathematical optimization versus when rules of thumb are likely to suffice. A secondary objective is to provide a tutorial on optimization methods for an audience for whom these techniques might not be familiar. The work will proceed by reanalyzing available data from other projects. An initial source is a RAND technical report on reducing terror risk at shopping centers.

Major Milestones and Dates:

- Shopping center analysis – September 2008
- Additional analysis of IT security data – June 2009
- Working paper describing analysis – September 2009