Meeting the Challenges of Terrorism Risk Analysis

Vicki M. Bier
University of Wisconsin–Madison, bier@engr.wisc.edu

Detlof von Winterfeldt
University of Southern California, winterfe@usc.edu

Follow this and additional works at: http://research.create.usc.edu/published_papers

Recommended Citation
http://research.create.usc.edu/published_papers/37
This special issue is devoted to efforts being made to meet the new challenges posed to the field of risk analysis as a result of the increased focus on risks of terrorism. The articles contained in this special issue demonstrate that substantial progress is being made by risk analysts in meeting those challenges, even though much remains to be done and many researchers have begun working in this area only in the last few years.

In the economic area, Gordon et al. study the effects on the U.S. economy of a seven-day shutdown of the commercial aviation system (as might occur, for example, following an attack on a commercial airplane using a surface-to-air missile), as well as the economic impact of reduced airline passenger volume. The discussion of these issues is timely in light of the efforts by the U.S. Department of Homeland Security to evaluate possible defenses against such attacks. Similarly, Rose et al. use computable general equilibrium analysis to quantify the economic effects of a terrorist attack on the electrical transmission system of Los Angeles. In particular, they document that customers would have significant resilience and ability to adapt to a blackout (through measures such as conservation, reliance on other forms of energy, and use of on-site electrical generators), and identify ways in which such resilience could be improved in future.

In an applied case study, Rosoff and von Winterfeldt use project risk analysis and input-output modeling to analyze the risks of a dirty-bomb attack on the ports of Los Angeles and Long Beach. Their analysis shows that while the health risks of such an attack would be limited, the economic impacts might be sufficient to justify preventive measures such as radiation detection and perimeter control. Similarly, Simonoff et al. compile and analyze incident data about disruptions to the electrical grid. They show how these data can be useful to generate potential scenarios involving electrical outages, and to estimate the risks, consequences, and costs of such outages.

Ezell proposes a method for vulnerability assessment of critical infrastructure, taking into account the ability to deter attacks, detect them before they do significant damage, delay the attackers in achieving their goals, and respond (e.g., to minimize damage or commence recovery efforts). His method is applied to a hypothetical example involving a water utility. Ayyub et al. present a practical portfolio-based framework for allocating security investments to critical assets. One desirable feature of their model is that it can be applied at varying levels of detail, depending on the level of information available to the decisionmaker and the importance of the problem; their approach also provides a way of capturing interdependencies between assets (where, for example, the loss caused by damage to one asset may depend on which other assets are damaged, if any).

Keeney discusses how structuring of objectives can help in understanding the incentives faced by both terrorists and defenders. He indicates many areas in which such objectives could be useful, including appraisal of security policies, evaluating the relative attractiveness of different targets, generating plausible scenarios for potential terrorist attacks, and identifying creative ways to reduce terrorism. In another application of decision-theoretic ideas, Willis presents a method by which the allocation of defensive resources can be guided by estimates of terrorism risk. Moreover, he argues that even if those risk estimates are too low by several orders of magnitude, we may be spending money to reduce levels of risk from terrorism that would routinely be tolerated if they were due to other causes.

Bier discusses the results of a game-theoretic model for allocating defensive resources (viewing security as a game between an attacker and a defender), in light of the fact that terrorists may be able to observe those defenses and revise their attack strategies accordingly. Results support Willis’s claim that defensive resources should be focused on protecting the most attractive targets. In another application of game theory, Heal and Kunreuther view security as a game
between defenders, in which security investments by one defender can alter the risks and incentives faced by other defenders. Applications considered in their work include both aviation security and vaccination against infectious diseases.

The articles in this special issue indicate substantial progress in the development of better methods for risk analysis and risk management, ranging from practical methods that are ready for application today, to more theoretical models that may guide research and decision making in future. However, significant challenges still remain, indicating that terrorism risk analysis is likely to remain a fruitful area for both researchers and practitioners for many years to come.

Vicki M. Bier and Detlof von Winterfeldt

*Guest Editors*