Defending a country against terrorist threats raises new challenges and opportunities for risk analysis, different from those that are familiar from risk analysis of natural disasters and complex technological systems. Terrorists can be informed, deceived, deterred, or distracted – options that are not available for managing the risks from hurricanes or unreliable systems and workers. This special issue of Risk Analysis: An International Journal examines recent progress in understanding, modeling, and managing the threats from terrorism, emphasizing some of the most useful and important papers on this subject published in the journal over the past five years. We hope to prepare similar special issues on other timely and important subjects, so please tell us of your ideas about how to use this special “virtual” issue format to maximize reader benefits.

1. DEFINITIONS AND AN EXAMPLE

Some papers in this special issue define terms and concepts, and others assume them. So that all readers begin in a similar place, we begin with some conventional definitions used in risk analysis, many of which are challenged by risk analysis of terrorism. There are no generally accepted standard definitions, and we do not expect every reader to agree with these definitions, but they are our starting point.

Dozens of definitions of risk exist in the literature. William Lowrance’s 1976 definition is perhaps the most widely quoted: “Risk is a measure of the probability and
severity of adverse events.” (1) Risk analysis is commonly divided into risk assessment and management. Risk assessors answer three broad questions:

(1) What adverse events might occur?
(2) How likely are they to occur?
(3) What are their probable consequences, if they do occur?

Risk managers address multiple questions, which we have simplified into three:

(1) What actions can reduce the likelihoods (or expected annual frequencies) or mitigate the adverse consequences of events? Answers may range from engineering and security precautions to insurance arrangements that pool, spread, or transfer the financial losses from events.

(2) What can be done to recover from an event, should it occur?

(3) What communications and organizational and institutional structures and functions facilitate successful risk management decisions and operations? (2-4)

Vulnerability, mitigation, prevention, resilience, threat, intelligence and system state are additional key terms. “Vulnerability” is a weakness in the physical, organizational, or human attributes of a system that allow its performance to be degraded by a hazard event. (A “hazard” is a source of risk, and is sometimes called a “threat” in security and terrorism risk analysis. Natural hazards include hurricanes and earthquakes; man-made hazards include deliberately provoked failures in reliability systems and cyberattacks on power grids. A “threat” arises from the intent or assumed intent of an attacker to degrade a target during some time interval.) “Mitigation” is a deliberate investment in technology, organization and people to reduce the adverse consequences of events. “Prevention” (or “avoidance”) refers to actions taken to make adverse events less
likely or frequent. “Resilience” is the ability to cope with and recover from an event quickly and fully. “Intelligence” consists of obtaining critical information about the threat to support prevention or mitigation. “System state” is the status of all system attributes at any given moment that determine its response (or probabilities of responses) to inputs.

To illustrate the complexity of risk analysis, consider attacks on buses. The Mineta Transportation Institute (MTI) has extensively studied criminal attacks on buses around the world.\(^{(5)}\) Their reports include data from the year 1920 and are complete through 2009. They report on attacker tactics and weapons, concentrating on those that have been most successful for attackers. They also report actions by security, bus operators, and passengers that prevented attacks from succeeding, or that reduced their impact. The MTI database lists 37 types of targets, 26 categories of attacks, numbers and types of devices, and how they were delivered to the target. Only three attacks in the database occurred in North America,\(^{(5)}\) two in Mexico and one in Canada. Most bus-related attacks are by guerilla groups and occur in countries in Asia and the Middle East, where buses are a primary mode of transportation. The attackers typically use military ordnance, for example mines.

By contrast, terrorist attacks in the United States involve very different means and motives. Data from the period 1997-2007 show that over 40% of US terrorist attacks were by anti-abortionists, 25% by the Earth Liberation Front and another 16% by animal liberation groups.\(^{(5)}\)

These data do not mean that bus-related terrorist attacks are to be ignored in areas where they have not yet occurred. For example, in 1997, 2003, 2004, and 2007, plots to
attack the New York City subway system and tunnels between New Jersey and New York City were foiled. It is not much of a leap to assume that plotters have also considered buses. This assumption is strengthened by the MTI group’s conclusion that terrorists place priority on causing at least some damage, and by the fact that buses are relatively easy targets. MTI observed that the vast majority of surface transportation attacks have occurred since 1970 and that the annual average of attacks has increased by a factor of over eight, from fewer than 10 to over 80 a year. Buses and bus stations account for more than half of all the attacks, and these averaged 10 deaths per attack, or about half of the average deaths associated with attacks on trains and train stations.

With these data as background, we look again at the typical risk analysis process and the definitions noted earlier. The typical attack (threat) was a single non-suicide attack on a single bus. However, there were many other forms of terrorist attack on buses, bus stops and bus stations. We can’t rule out other modes of attacks against buses. Nor can we assume that explosives will be the weapon of choice, especially in the United States where guns and semiautomatic weapons are relatively easy to obtain.

With regard to likelihood, the chances of an attack per passenger-hour are extremely low, even in Asia and the Middle East. The consequences in terms of deaths and injuries can be estimated from the MTI data. Indirect consequences, such as reduced rider confidence in buses, loss of confidence and security forces to protect people, and other indirect effects can be determined by follow-up research.

Existing data are most informative about risk management. About 60% of the attacks failed to kill or injure people. Some of these failures were caused by poorly built
explosive devices, but others were prevented or reduced in magnitude by bus security, operators and passenger actions.

Buses clearly are vulnerable to terrorist attacks, and given recent international history, many can be prevented by intelligence efforts and training. For example, Israel and the United Kingdom have developed programs, and the US DHS has developed a training program for bus operators and managers. Providing the training is a challenge because of the expense during a period when transportation companies are hard-pressed to maintain their basic services and are reluctant to invest in an activity that has no history in their area. The potential contribution of risk analysis in such a realistically complex case would be to quantify where training programs are most likely to be beneficial, and how much difference they might actually make in changing behaviors to reduce risks.

2. ARTICLES IN THIS SPECIAL ISSUE

This special issue has four sections. Part 1, on Probabilistic Risk Assessment (PRA) of terrorist attacks, features papers that have helped the risk analysis community start to bridge the gap between traditional PRA and terrorism risk analysis methods that acknowledge and respond to the need to model the behaviors of intelligent adversaries. Many of our publications focus on this challenge, and consequently Part 1 is the longest section. Part 2 presents thinking at the intersection of decision analysis, risk analysis, and operations research, exploring new ways to understand terrorist values and motivation. Ideally, sufficient understanding of attacker values, goals, and priorities would help defenders understand the threats and figure out not only what attackers are likely to do,
but also what changes could reduce the chances of attack or make attacks less likely to achieve their goals. Part 3 confronts the reality that, despite our best efforts to prevent attacks and/or anticipate and mitigate their consequences, some may still occur and succeed. How we respond can greatly affect not only the immediate consequences of an attack, but also incentives for further attacks. Part 4 presents a variety of practical applications, including terrorism risk analyses for aviation, trains, vehicles carrying bombs, ports, power grids, and food supply chains. Part 4 also considers how small communities might rank the various risks to critical infrastructures from natural, accidental, and malicious sources. Each section is described in more detail next. (See article list for full citations.)

2.1. Part 1. PRA and Terrorist Risk Assessment

The focus throughout Part 1 is on setting priorities and allocating scarce defensive resources to achieve maximum risk reduction, based in part on what adversaries might do in response. Several articles in this section critically examine the potential for decision-analytic and game-theoretic models, as well as proposed alternatives, to improve anti-terrorism risk management decisions. For example, Vicki Bier uses game theory to study how defender actions might influence attacker’s choice of targets. Bilal Ayyub et al. develop and illustrate the concept of a critical asset and portfolio risk that includes the traditional elements of threat, vulnerability, and consequence. Tony Cox critiques the traditional model of \( \text{risk} = \text{threat} \times \text{vulnerability} \times \text{consequence} \) for terrorist attacks and advocates optimization models. Bier et al. develop and test a model that includes
defender actions prior to an attack, attacker actions during the attack, and defender actions after the attack.

Two sets of inter-linked papers further explore and debate the use of these concepts in practice. The first set, beginning with a paper by Dillon et al., examines the allocation of defensive resources to defend specific targets, and then goes on to discuss whether and how resources can be allocated effectively when intelligent adversaries are present. Cox, Dillon, Hall, and then Cox again debate the issue of traditional probabilistic risk assessment (PRA) vs. game theory in response to Dillon’s original article. The second set of articles begins with a paper by Parnell et al. that considers whether and how operations research modeling and decision analysis methods can improve our capacity to understand and model terrorist events. It is followed by papers by Ezell et al., Brown and Cox, and Merrick and Parnell. Part 1 concludes with a more theoretical paper, by Bulleit and Drewek, showing how agent-based modeling (ABM) might be used to gain new insights into characteristics of terrorist risks, viewed as emergent phenomena in large-scale self-organizing systems.

2.2. **Part 2. Understanding Intelligent Adversaries**

Part 2 signals growing interest in understanding terrorist motives, goals, and values in order to better anticipate what terrorists hope to achieve and how to discourage them. Keeney’s first article develops a list of objectives for the Department of Homeland Security and another for terrorist groups, and then applies these to creating value models to increase understanding about terrorist motives and likely actions. The article by Keeney and von Winterfeldt extracts key values from Al-Qaeda publications toward this
same end. Finally, Keeney and von Winterfeldt consider how to construct a mean-end network and a value model for the Department of Homeland Security, to assist in making value trade-offs and in subjectively evaluating decisions. Eventually, we hope that this work might be integrated with agent-based modeling of emergent terrorist threats to help figure out how best to disrupt terrorist networks and shape incentives to reduce the frequency of attack attempts.

2.3. **Part 3. Coping with Attacks**

The discussion in Part 3 of how best to respond to a successful attack to minimize its adverse consequences resonates with Part 2’s discussion of terrorist motives, goals, and incentives to undertake further attacks. A measured, carefully thought-out response may not only save lives (and dollars and quality of life) in the short run, but may make us less attractive as targets in the longer run. Whicker et al. make the case for adaptive management of responses to attacks (such as the anthrax attacks on office buildings) to enable public buildings to be restored to safety relatively quickly, while accounting for realistic imperfections and uncertainties in the responses of different stakeholders. Flexible adaptation to attacks provides a way to avoid over-reacting, helping us to avoid creating more harm by our reactions than by the terrorist event itself.

The paper by Wein et al. points out that simply sheltering in place, especially in basements, may be much more effective that attempting evacuation in reducing casualties and other losses in the dreadful event of a successful detonation of a nuclear bomb in Washington D.C. We hope to receive many more papers on these subjects.
2.4. **Part 4. Applications**

The main purpose of thinking about and debating better approaches to terrorism risk analysis in Parts 1-3 is to enable better risk management decisions. The diverse applications in Section 4 illustrate the current state-of-the-art in anti-terrorism risk analysis, and help to define and clarify the continuing need for better methods to address the practical realities of terrorism risks. Papers by Barnett, Rosoff and von Winterfeldt, Atkinson et al., Simonoff et al., Rose, and Greenberg et al. assess risks from threats associated with air, cargo ship, vehicles, electric power and trains, respectively. Not only do these articles focus on specific applications, but they also demonstrate the difficulty of building decision support models that both acknowledge the complexity of science and that are usable by the policy and risk management community. Screening is imperfect, and attackers may be persistent, although not blind to chances and costs of mounting a successful attack. Rationally assessing, deterring, preparing for, and responding to terrorist threats carried by these different routes requires quantitative analysis of the effects and trade-offs among risk management alternatives, as discussed in Part 1 and illustrated throughout the papers in Part 4.

Transportation and power systems are not the only way by which threats can reach target populations, however. Hartnett et al.\(^{(31)}\) consider food-borne attacks. They show how public health systems can minimize the adverse effects of such attacks, or fail to do so, based largely on vigilance and speed of recognition and response to an attack. Finally, a paper by Li et al.\(^{(33)}\) reminds us that risk management is not (or should not be) just a matter for individual precautions and large-scale city, state, or Federal government
programs, but also requires small communities to decide which of the many hazards facing them are most worrisome and most worth allocating resources to address them.

3. SUMMARY

This collection of papers illustrates the progress that contributors to Risk Analysis: An International Journal have made recently in terrorism risk analysis. The papers collected here were selected by the editors as being especially promising, influential, or useful – in the editors’ best judgment – for understanding and improving society’s ability to manage terrorism risks. Many other excellent papers have also been published in the journal that extend, complement, or provide background for those we selected. Although length constraints preclude including all of them in this special issue, we also recommend the additional papers listed with this special issue to readers of Risk Analysis: An International Journal. Together with the ones in this special issue, these papers provide a solid foundation for understanding and advancing the present state-of-the-art in terrorism risk analysis.
REFERENCES


