A Survey of Operations Research Models and Applications in Homeland Security

P. Daniel Wright, Matthew J. Liberatore, Robert L. Nydick
Department of Decision and Information Technologies, Villanova University, Villanova, Pennsylvania 19085
{daniel.wright@villanova.edu, matthew.liberatore@villanova.edu, robert.nydick@villanova.edu}

Operations research has had a long and distinguished history of work in emergency preparedness and response, airline security, transportation of hazardous materials, and threat and vulnerability analysis. Since the attacks of September 11, 2001 and the formation of the US Department of Homeland Security, these topics have been gathered under the broad umbrella of homeland security. In addition, other areas of OR applications in homeland security are evolving, such as border and port security, cyber security, and critical infrastructure protection. The opportunities for operations researchers to contribute to homeland security remain numerous.

Keywords: government: agencies; planning: government, homeland security.

History: This paper was refereed.

Since September 11, 2001, the term homeland security has entered the vernacular of the United States and of countries around the world. In the US, it is defined as “a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur” (Office of Homeland Security 2002, p. 2). Despite the recency of the term, for decades the operations research community has been exploring issues that we now classify under homeland security. As far back as 1960, OR researchers were working on such issues. At the seventh international meeting of the Institute of Management Sciences (TIMS), Wood (1961) highlighted US vulnerability and potential responses to nuclear attack. He called on the OR community to develop techniques and programs to maintain freedom. Since that time, operations researchers have focused on such topics as emergency preparedness and response, airline security, hazardous material transportation, and cyber security. All of these areas are increasingly important to homeland security. While they have done much, operations researchers still have rich opportunities available.

The US Department of Homeland Security (DHS), formed in October 2001, has a broad set of responsibilities that contribute to securing the homeland. To form it, the government reorganized several agencies and programs and evaluated its existing security efforts (National Commission on Terrorist Attacks upon the United States 2004). It put several existing agencies under one domain to unite their efforts to better protect the country. The department is organized into five directorates: border and transportation security, emergency preparedness and response, science and technology, information analysis and infrastructure protection, and management. Each directorate contains several agencies that were formerly housed in different departments of the federal government. For instance, the border and transportation security directorate now includes the US Customs Service, the Transportation Security Administration, and the Animal and Plant Health Inspection Service, which were originally the responsibility of the Treasury, Justice, and Agriculture Departments, respectively. For all of its directorates, the Department of Homeland Security states its mission as follows:

We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. We will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce (Department of Homeland Security 2005).

The mission is reinforced by several strategic goals, including awareness, prevention, protection, response,
recovery, service, and organizational excellence. Both the mission and the strategic goals of the DHS provide exciting opportunities for operations research.

**Literature Framework**

Many research agendas contribute directly or indirectly to homeland security. Organizing the literature concerning homeland security is challenging. Research in homeland security falls under the science and technology directorate, which is the primary research-and-development arm of the DHS. It describes three main research areas that contribute to the state of the art in homeland security: (1) countermeasures portfolios, (2) component-support portfolios, and (3) cross-cutting portfolios. The science and technology directorate conducts and funds research in all of these portfolios. A few authors have reported on the impact of science and technology, including information technology, on terrorism response (Branscomb and Klausner 2003, Hennessy et al. 2003).

The main purpose of the countermeasures portfolio is to protect the US from weapons of mass destruction. Research in this area concerns vulnerabilities and risks surrounding biological, chemical, radiological, and nuclear weapons, and high explosives. The research invites collaboration between operations researchers and physical scientists.

The component-support portfolios focus on increasing the capabilities of DHS components and helping them to secure the homeland. The components include border and transportation security, critical infrastructure protection, cyber security, emergency preparedness and response, threat and vulnerability testing and assessment, the US Coast Guard, and the US Secret Service. In this portfolio, OR has the greatest history and perhaps the most potential to improve homeland security.

The cross-cutting portfolios focus on other vulnerabilities and risks that extend across the countermeasures and component support portfolios. They include emerging threats, rapid prototyping, standards, and university programs. Although OR could contribute to cross-cutting, most previous work is better categorized in the other two portfolios.

We focus on the first two portfolios because most OR-related research has fallen in those portfolios.

<table>
<thead>
<tr>
<th>Countermeasures portfolios</th>
<th>Component-support portfolios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biological</td>
<td>Border and transportation security</td>
</tr>
<tr>
<td>Chemical</td>
<td>Critical infrastructure protection</td>
</tr>
<tr>
<td>Radiological and nuclear</td>
<td>Cyber security</td>
</tr>
<tr>
<td>High explosives</td>
<td>Emergency preparedness and response</td>
</tr>
<tr>
<td></td>
<td>Threat analysis</td>
</tr>
</tbody>
</table>

**Table 1:** The countermeasures and component-support portfolios of the Department of Homeland Security research portfolios protect against weapons of mass destruction and support department components, respectively (adapted from www.dhs.gov).

In addition, they offer the greatest opportunity for contributions combining OR and homeland security (Table 1).

We sought articles on OR and homeland security throughout the world published in academic journals. While some military research concerns homeland security, it does not fall under the US Department of Homeland Security and its research agenda. Jaiswal (1997) reviewed military OR models and techniques, and Miser (1998), Bonder (2002), and Hughes (2002) discussed the historical impact of OR on the military.

Operations researchers have contributed in many ways to homeland security. We use the DHS science and technology framework to discuss previous work.

**Countermeasures Portfolios**

Countermeasure efforts address the risks of biological, chemical, radiological, and nuclear weapons, and high explosives. The OR community has studied problems in this area with notable results. Sullivan and Perry (2004) developed a useful framework for
categorizing terrorist groups’ development of chemical, biological, radiological, and nuclear weapons. They investigated three classification approaches, including a heuristic pattern-recognition method, classification trees, and discriminant analysis. Dyer et al. (1998) and Butler et al. (2005) addressed the problem of disposing of weapons-grade plutonium. Dyer et al. (1998) used multiple attribute utility theory (MAUT) to develop a hierarchy of objectives, to evaluate 13 alternatives, and to conduct sensitivity analyses. Butler et al. (2005) used MAUT to help the US and Russia to evaluate alternatives for disposing of stockpiles of weapons-grade plutonium. They recommended converting the plutonium for use as fuel in nuclear power plants. Munera et al. (1997) described the safety and security concerns posed by transporting highly enriched uranium used in nuclear reactors. They used stochastic dominance to evaluate the risks of road and air alternatives.

Hupert et al. (2002) used discrete-event simulation to determine staffing levels for entry, triage, medical evaluation, and drug dispensing in a hypothetical distribution center under conditions of low, medium, and high bioterrorism attack. Craft et al. (2005) created a series of differential equations to determine the potential number of deaths from an aerosol bioterror attack. Their method included an atmospheric-release model, a spatial array of biosensors, a dose-response model, a disease-progression model, and an antibiotics model with a queue. Kaplan et al. (2002, 2003) also used differential equations to study response to a smallpox attack. Walden and Kaplan (2004) used a Bayesian approach to estimate the size and time of an anthrax attack to determine the number of persons who might require medical care. Wein et al. (2003) also modeled emergency response to an anthrax attack.

Jenkins (2000) used integer programming to identify a small subset of oil spills that are similar to all potential categories of spills to predict the type of pollutant a terrorist group might use. Buckeridge et al. (2005) classified bioterrorism outbreak algorithms and found that spatial and other covariate information can improve measures for detecting and evaluating outbreaks. Stuart and Wilkening (2005) used first- and second-order catastrophic decay models to study the impact of degradation of biological-weapons agents leaked into the environment.

Border and Transportation Security
Border and transportation security problems have been and continue to be of great interest to operations researchers particularly because these types of problems are a good match for OR techniques. Within the DHS framework, border security includes improving the security of the nation’s borders to prevent the entry of terrorists, criminals, and illegal aliens while maintaining the safe flow of commerce and travelers. Transportation security includes the safety of airlines, railroads, ships, and trucks.

Border Security
Papers on border security are just beginning to appear. Wein and Baveja (2005) studied two programs: the US visitor program and the immigrant-status-indicator-technology program. These two programs aim to reduce visa fraud and detect the entry of watch-listed criminals and suspected terrorists into the United States. Using a game-theoretic model, the authors show that the quality of fingerprint images is important to detection probability and thus system performance. They discussed fingerprint-scanning strategies that help counter terrorists’ attempts to minimize detection.

Airline Security
After the hijacking of commercial airlines that led to the catastrophic events of September 11th, 2001, the US Federal Aviation Administration and Transportation Security Administration tightened security measures at airports around the country. Barnett (2004) described a dynamic computer system that uses probability models and data-mining techniques to classify airline-passenger threats. However, many airline security issues still need attention (Turney et al. 2004). Coincidentally many OR researchers addressed airline security before 2001, focusing primarily on scanning passengers or baggage. Gilliam (1979) employed queuing theory for passenger screening. Kobza and Jacobson (1997) discussed the design of access security systems in airports. They developed performance measures based on the probabilities of false alarms and false clears that determine the effectiveness of single-device and multiple-device security systems. Jacobson et al. (2000) developed a sampling procedure that estimates false-alarm and false-clear probabilities.
Kobza and Jacobson (1996) studied security-system design by addressing the dependence between the responses of security devices in multiple-device systems. These articles could help managers to improve decisions on airport security systems and are somewhat generalizable to other types of security systems.

Jacobson et al. (2001) described aviation security as a knapsack problem and proposed a model that determines how to minimize the false-alarm rate of a given security system. Barnett et al. (2001) conducted an experiment to evaluate the costs of bag-match strategies to the airlines and to the passengers in terms of monetary cost and passenger delay. Jacobson et al. (2003) discussed three important performance measures of baggage screening: the number of passengers on flights with unscanned bags, the number of flight segments with unscanned bags, and the total number of unscanned bags. Using examples based on real data, they showed how a greedy algorithm can minimize the performance measures. Jacobson et al. (2005) discussed the optimization of the first two measures through the allocation and utilization of screening devices.

The cost of airline security concerns airports and commercial airlines. Candalino et al. (2004) discussed a software system for screening checked baggage that uses data on purchase and operating costs to allocate security devices around the country. They proposed an alternative cost function that includes indirect costs related to scanning errors. Virta et al. (2003) considered the direct and indirect costs of scanning policies based on the passengers selected by the screening software.

Long customer waits are an important issue for airports who want to keep passengers happy and reduce congestion. Leone and Liu (2003) developed a simulation model that investigates passenger traffic and throughput rates for scanning devices. They discovered that the machines’ throughput rates were far lower than their advertised scan rates.

As policies and scanning technologies change, operations researchers should find further opportunities in airline security.

Port and Rail Security
Currently, little operations research deals with the security of ports and railroads. Harrald et al. (2004) identified US ports as vulnerable and as very attractive targets for terrorists. Lewis et al. (2003) formulated a shortest-path model for container-security operations at US seaports. They identified and analyzed trade-offs between the number of containers inspected and the costs of delayed vessel departures.

The US railway system must be protected to prevent the sabotage of passenger or cargo trains and to prevent terrorists’ gaining control of hazardous shipments. Glickman and Rosenfield (1984) formulated models to evaluate the risks associated with train derailments and the release of hazardous materials, issues that could become important in the event of a terrorist attack.

Truck Security
The main issue for the trucking system is the transportation of hazardous materials. Many of the articles in the OR literature on transporting hazardous materials do not focus on homeland security, that is, preventing terrorists from hijacking these materials and using them in weapons. The literature focuses on two related issues: routing vehicles and analyzing risk. Routing hazardous vehicles involves determining what paths vehicles should take to minimize population exposure in the event of an accident. Many authors have developed algorithms and heuristics for solving various cases of the routing problem (Batta and Chiu 1986, 1988; Berman et al. 2000; Beroggi and Wallace 1994, 2005; Erkut and Ingolfsson 2000; Giannikos 1998; Jin et al. 1996; Karkazis and Boffey 1995; Lindner-Dutton et al. 1991; List and Turnquist 1998; van Steen 1987; Zografos and Androutsopoulos 2004). Related to the routing problem are methods for treating and analyzing risk (Erkut and Ingolfsson 2005, Erkut and Verter 1998, Gopalan et al. 1990, Kara et al. 2003, Raj and Pritchard 2000).

Critical Infrastructure Protection
To protect the critical infrastructure, analysts develop tools to anticipate, identify, and assess the risks in the nation’s critical infrastructure and attempt to reduce the risks and the consequences of an attack. Potential infrastructure targets include agriculture and food, banking and finance, dams, high-profile events, information systems, public health, national monuments, nuclear power plants, and water systems.
Apostolakis and Lemon (2005) used MAUT to prioritize the vulnerabilities in an infrastructure that they modeled using interconnected digraphs and applied graph theory to identify candidate scenarios. Brown et al. (2004) applied simulation to study the impacts of disruptions and used risk analysis to assess infrastructure interdependencies. Their purpose was to identify infrastructure risks and ways to reduce them. Baskerville and Portougal (2003) developed a possibility model that suggests that, during an optimal length of time, the possibility of attack on information system infrastructures is very low.

The risk associated with major utilities, such as water systems, is important to homeland security (Grigg 2003). Zografos et al. (1998) developed a data-management module, a vehicle-monitoring and communications module, and a modeling module and applied them to an emergency-repair operation for an electric utility company. They used a combined optimization and simulation approach to minimize service unavailability. Salmeron et al. (2004) developed a max-min model to help determine weaknesses in the electric grid to prepare for terrorist attacks. Through decomposition, they solved the problem with a heuristic on two test systems.

Cyber Security

Research in cyber security helps prevent, protect against, detect, respond to, and recover from large-scale cyber attacks on the information infrastructure. Although many studies concern network security, few can be considered operations research. Krings and Azadmanesh (2005) developed a model for transforming security and survivability applications so that they can be solved with graph and scheduling algorithms. Chen et al. (2005) explained how shared networks and the Internet have focused interest on IT security, particularly intrusion detection. They used data-mining methods (artificial neural networks and support vector machine) to identify potential intrusions. Abouzakkar and Manson (2002) addressed network security using two intelligent fuzzy agents to respond to denial-of-service attacks. Shindo et al. (2000) generated fault-tree and event-tree structures between a computer-network access point and a process plant. They applied their analysis to a chemical plant failure and showed that they could greatly improve risk assessment.

Chowdhury et al. (1999) used linear programming to limit the availability of confidential information in a database while providing access to those who need it. They developed two transportation flow algorithms that are computationally efficient and insightful. Muralidhar et al. (1999) developed a model to explain how to use data-perturbation methods to protect information from unwanted access while allowing maximum access to genuine inquiries and maintaining the relationships between attributes.

Emergency Preparedness and Response

Emergency preparedness and response include such topics as planning for, preventing, responding to, and recovering from natural disasters and terrorism. Larson (2004, 2006) reviewed the literature on police, fire, and emergency medical services, and provided some coverage of hazardous materials, bioterrorism, and private-sector response to emergencies. The literature can be categorized into (1) early work, (2) location and resource allocation, (3) evacuation models, and (4) disaster planning and response.

Early Work

Green and Kolesar (2004) described a number of papers on emergency-response systems. Much of the OR work on managing emergency services originated with the New York City–Rand Institute. Its work with the New York City Fire Department included a simulation model of firefighting operations (Carter and Ignall 1970); queuing models of fire company availability (Carter et al. 1972); the “square root law” for the location of fire companies based on response distance, with a response time-distance function to predict response time (developed by Kolesar and Blum 1973 and applied by Rider 1976); an empirically based decision model to predict response time (developed by Kolesar and Blum 1973 and applied by Rider 1976); an empirically Bayes approach to alarm forecasting (Carter and Rolph 1974); a stochastically based integer linear programming model and a heuristic algorithm for fire company relocation (Kolesar and Walker 1974); a set covering approach for locating two types of ladder fire trucks (Walker 1974); heuristics for identifying high-priority alarm boxes (Ignall et al. 1975); Markovian decision models of initial dispatch of fire companies (Ignall et al. 1982, Swersey 1982); and a
book pulling together the accumulated work on fire deployment analysis (Walker et al. 1979) under support from the US Department of Housing and Urban Development (HUD).

The New York City–Rand Institute’s work with the New York Police Department included work on deployment related to the 911 emergency telephone system (Larson 1972, 2002); scheduling patrol cars using queuing and linear programming (Kolesar et al. 1975); and the patrol car allocation model (PCAM) based on queuing and linear programming (Chaiken and Dormont 1978a, b). The multicar dispatch queuing model (Green 1984) was later incorporated into a revised version of PCAM (Green and Kolesar 1989) and applied to the proposed mergers of police and fire departments in several cities (Chelst 1988, 1990). Chaiken and Larson (1972) reviewed methods for allocating emergency units (vehicles). Chaiken (1978) described six models (including PCAM) developed with HUD support for fire and police operations and the challenges of implementing them.

**Location and Resource Allocation**

The early literature on locating emergency service facilities is based on the location set covering problem (LSCP) formulated by Toregas et al. (1971). In this problem, a population is served or covered when a facility is located within an acceptable service distance. The objective is to minimize the number of facilities while covering all demand points. Walker (1974) applied the LSCP to the location of ladder trucks in the boroughs of New York City. Plane and Hendrick (1977) applied the LSCP to the location of fire companies in Denver, Colorado. Daskin and Stern (1981) extended the LSCP to address multiple coverage of demand nodes.

The maximal covering location problem (MCLP) developed by Church and ReVelle (1974) relaxes the LSCP’s requirement that all demand nodes are covered. The MCLP seeks to maximize the total population served within a maximum service distance, given a fixed number of facilities. Because Church and ReVelle leave some population uncovered, they include mandatory closeness constraints in their formulation. The MCLP is related to the p-median problem (Hakimi 1964), which seeks to locate p facilities to minimize total demand-weighted travel distances between demands and facilities.

Eaton et al. (1985) applied the MCLP model in Austin, Texas when EMS officials sought to improve operating efficiency. Saccomanno and Allen (1988) used a modified MCLP algorithm to locate emergency response capability for potential spills of dangerous goods on a road network. Belardo et al. (1984b) extended the MCLP to locate oil-spill-response equipment on Long Island Sound. Chung (1986) described other applications of the MCLP.

Hogan and ReVelle (1986) modified set covering models to maximize the percentage of the population that receives backup coverage. Pirkul and Schilling (1988) developed a backup coverage model for facilities with limited workloads or capacities. Batta and Mannur (1990) extended the set covering models to include some demand points requiring responses from multiple units (for example, fire trucks or ambulances).

Church et al. (1991) formulated a bicriteria maximal covering location model that maximizes the demand covered within the maximal distance and also minimizes the distance traveled from the uncovered demand to the nearest facility. Schilling et al. (1979) developed the tandem equipment allocation model (TEAM) and the facility location, equipment, and emplacement technique (FLEET) model to allocate equipment with varying capabilities and demands. The FLEET model has been effectively applied to locate fire stations and allocate equipment. With some modifications, Tavakoli and Lightner (2004) applied Bianchi and Church’s (1988) multiple coverage, one-unit FLEET model (MOFLEET) to Cumberland County, North Carolina’s emergency medical services (EMS) system.

Several authors have developed optimization models that include stochastic elements. Daskin (1983) developed the maximal expected coverage location
model (MECLM), which seeks to locate emergency vehicles to maximize the expected coverage area, even when multiple vehicles are in use. Batta et al. (1989) offered an extended version of MECLM. They assumed that the probability that a randomly chosen vehicle is busy is independent of any other vehicle in use. ReVelle and Hogan (1989) proposed a variation of MECLM called the maximum availability location model (MALM) in which each constraint guarantees that the probability that a demand point receives service within an acceptable time is no less than a required value. In these latter two models, the analysts estimated probabilities that vehicles are busy in advance. Ball and Lin (1993) developed a model similar to MALM except that they directly model the source of the randomness. Goldberg and Paz (1991) developed an optimization model that seeks to maximize the expected number of emergency callers reached within a specified time.

Analytical queuing models have been used to evaluate the performance of emergency service systems. In his hypercube model (1974, 1975, 2001), Larson characterizes the operation of an emergency service system as a multiserver queuing system in which the states correspond to all combinations of servers busy and idle. This model provides a set of output measures, such as vehicle utilization and average travel time, and has been used to deploy ambulances and police cars in various cities (Brandeau and Larson 1986, Larson and Rich 1987). Extensions include improving the accuracy of the model’s output measures by allowing the service rates to be server dependent (Halpern 1977), estimating the probability distribution of travel times (Chelst and Jarvis 1979), and allowing the dispatch of multiple units (Chelst and Barlach 1981). Researchers have suggested that these queuing models can be used as subroutines in optimization heuristics (Berman and Larson 1982, Benveniste 1985, and Berman et al. 1987). Carter et al. (1972), Hall (1972), and Chelst (1981) developed other analytic approaches.

Savas (1969) used simulation analysis to evaluate proposed changes to the number and location of ambulances in New York. Fitzsimmons (1973) combined queuing and simulation to estimate the probabilities of particular ambulances being busy. This approach was combined with a pattern search routine in the ambulance deployment method CALL (computerized ambulance location logic), which located ambulances to minimize mean response time. CALL was successfully applied in central Los Angeles to locate firehouses and in Melbourne, Australia to plan an emergency ambulance system. Later CALL was combined with a contiguous zone search routine (CZSR) that uses an existing database on interzone travel times to locate ambulances in Austin, Texas (Fitzsimmons and Srikar 1982). Swoveland et al. (1973) used simulation coupled with optimization to locate ambulances in Vancouver, Canada.

**Evacuation Models**

Researchers have developed optimization, queuing, and simulation models to plan emergency evacuations of buildings and areas. Most of such work relies on queuing or simulation, although some uses optimization. Chalmet et al. (1982) applied transshipment and dynamic network optimization models to planning the evacuation of large buildings. They applied the models to the evacuation of 322 people from an 11-story building with four elevators and two stairwells and compared the results with an observed evacuation to reveal possible improvements.


 Analysts have developed micro-, macro-, and mesosimulation models for planning evacuations. Micro-simulations track the detailed movements of individual entities (cars, trucks, or people) on the road network. Pidd et al. (1996) and de Silva and Eglese (2000) describe their development of a spatial decision-support system (SDSS) for contingency planning in emergency evacuations using a micro-simulation model linked to a geographical information system (GIS). Mould (2001) used discrete-event simulation to plan the emergency evacuation of an
offshore oil installation. He considered environmental conditions, such as wind speed and wave height, while using a prespecified routine for evacuation and assessed the use of helicopters alone or in conjunction with fast rescue craft. He applied the model to a fictitious incident using randomly generated weather data. Jha et al. (2004) developed a micro-simulation model to evaluate five scenarios for evacuation planning at Los Alamos National Laboratory. Helbing et al. (2005) developed simulation models of pedestrian flows and used the results of these models as well as experiments to recommend designs to increase the efficiency and safety of facilities and egress routes. Using behavioral information, Stern and Sinuany-Stern (1989) used micro-simulation to plan evacuation under a radiological event.

Macro-simulations do not track individual entities but use equations based on analogies with fluid flows in networks (Sheffi et al. 1982). Southworth and Chin (1987) used macro-simulation to study the evacuation of a population threatened by flooding from a failed dam based on empirical data from urban and rural areas. A compromise approach is to use meso-simulators that usually track the movement of groups of entities.

**Disaster Planning and Response**

How individuals and organizations respond to disasters is important in preparing for emergencies. Belardo et al. (1984a) discussed response problems faced by four organizations: the American Red Cross, the US Coast Guard, the Regional Emergency Medical Organization in Albany, New York, and the New York State Office of Disaster Preparedness. Averett (2005) discussed four examples of responding to and preparing for disasters using various modeling tools: (1) discrete optimization and simulation models for locating and configuring vaccination centers and redirecting the flow of patients, (2) a graphics tool for visualization and collaboration, (3) simulation for disaster management training, and (4) game theory to anticipate terrorist attacks and defend against them. Kananen et al. (1990) extended standard input-output models and used multiobjective linear programming to evaluate the potential impact of emergencies or disasters on the Finnish economy.

Routing emergency vehicles is important in responding to emergencies. Recognizing the importance of considering the stochastic and time-varying nature of travel conditions in emergency situations, Miller-Hooks and Mahmassani (1998) developed and tested two algorithms for determining the shortest path under such conditions. Several authors have modeled the problem of transporting vital first-aid commodities and emergency personnel to disaster-affected areas. Haghani and Oh (1996) used a deterministic multicommodity, multimodal network flow model to plan disaster relief. Barbarosoglu and Arda (2004) extended this approach to include random arc capacity, supply, and demand. They formulated the problem as a two-stage stochastic program and used data from the August 1999 earthquake in Marmara, Turkey.

Srinivasa and Wilhelm (1997) and Wilhelm and Srinivasa (1997) developed a model that prescribes an effective response to an oil spill, which requires such decisions as which components to dispatch, how many, and when. They formulated the problem as a general integer program, using graph theory to generate response systems (components and their locations) needed by the model. They applied their approach to actual data representing the Galveston Bay area. They applied a heuristic (Wilhelm and Srinivasa 1997) and an exact procedure based on strong cutting-plane methods (Srinivasa and Wilhelm 1997).

A few researchers have modeled human behavior in emergency situations. Reer (1994) developed a probabilistic procedure to analyze human reliability in emergency situations using time windows and organizational input data. Reer used the loss of main feedwater at a pressurized water reactor plant as an example to investigate several organizational alternatives. Doheny and Fraser (1996) developed a software tool that can be used to model human decision making during emergency situations. Their model includes frames to represent a person’s characteristics and perception of the environment, and scripts to define typical behaviors for particular situations. They used their model to simulate an offshore emergency scenario.

**Threat Analysis**

Threat analysis develops the capabilities to evaluate and disseminate extensive information about threats
and to identify planned attacks. The US government obtains extensive information on threats daily, and threat analysis research attempts to detect and document terrorists’ intentions. Raghu et al. (2005) discussed a collaborative decision-making framework for homeland security and a connectionist modeling approach that fuses disparate information from several sources.

Popp et al. (2004) approached threat analysis from an information technology (IT) perspective. They argued that improved IT can reduce the time needed for searching for data, harvesting data, preprocessing data, and turning the results into reports and briefs. They discussed three core IT areas in depth: collaboration and decision tools, foreign-language tools, and pattern-analysis tools. These areas offer operations researchers opportunities to work in conjunction with information technologists to reduce terrorist attacks and their effects.

Wang et al. (2004) developed an algorithm that looks for similarities in criminal identities. Using real data from a police department, they created a model that develops disagreement values for each pair of criminal records. The intent is to use IT to determine whether two criminal records represent the same person. Sheth et al. (2005) devised a process of semantic association that links disparate information to establish relationships between terrorists. They incorporated this methodology into a program that provides a 360-degree look at each passenger boarding a flight and develops a threat score for use in deciding about additional security screening.

Pate-Cornell (2002) studied the fusion of intelligence information from different sources and used Bayesian analysis to rank threats and to prioritize safety measures. Dombroski and Carley (2002) used Bayesian analysis and biased network theory to estimate patterns of links between different cells of a terrorist organization to predict the structure of the terrorist network. Other researchers who developed Bayesian methods to aid in decision making are Santos (1996), Santos and Young (1999), and Santos et al. (2003). Santos and Haimes (2004) used input-output and decomposition analysis to provide a framework for describing how various terrorist activities are connected. They prioritize sectors based on the economic impact of terrorist activities. Haimes and Horowitz (2004) modeled counterterrorism intelligence using a two-player hierarchical holographic modeling game. Kaplan et al. (2005) introduced a terror-stock model that estimates the size of terrorist groups and how that size changes when the terrorists themselves are attacked.

### Discussion and Future Research

Operations research has contributed to issues related to homeland security in the United States even before 2001, when homeland security was defined. We adopted the research framework used by the US Department of Homeland Security’s science and technology directorate to classify the literature. As a result, we have not included some topics, such as the military that in some cases could be considered homeland security.

We used a two-dimensional framework in examining the previous OR work in homeland security: the areas specified by the US Department of Homeland Security and the four phases in the disaster life cycle: planning, prevention, response, and recovery (Table 2). Planning is generally strategic and long term in nature and relates to preparing for a disaster. Planning examples include policy analysis, risk analysis, systems design, and resource allocation. Prevention efforts aim to identify and eliminate threats, for example, screening airline passengers or patrolling borders. Response activities occur immediately after a disaster and include stabilizing affected areas, immediate medical care, and evacuation. Finally, recovery focuses on returning the affected areas and populations to their pre-event status and includes restoring critical infrastructures, assisting affected persons, and coordinating relief efforts.

Despite the attention paid to component support, many critical issues remain to be addressed within this category. Green and Kolesar (2004) described how component support problems are evolving. They suggested that analysts need to work on nonroutine emergencies and coordinating emergency service providers, and preparing for and responding to terrorist acts.

A wealth of literature concerns the security of trucks transporting hazardous materials, largely such issues as routing them to avoid exposing populations...
Table 2: Homeland security literature classified along two dimensions reveals opportunities for future research. We show where each paper fits within the Department of Homeland Security’s research framework and its position within the disaster life cycle. The two-dimensional framework in this table illustrates where the bulk of OR models and applications in homeland security exist. This table also highlights important gaps for future research. Focusing first on the rows in the table, we see that the topics that have received the most attention fall under the component support portfolios. Emergency preparedness and response contains significant amounts of work, with emphasis on emergency services location and resource allocation. Other highly important issues that have seen significant attention are evacuation models and disaster planning and response.
unnecessarily and analyzing risks. Researchers should extend these models to incorporate homeland security issues, for example, protecting trucks against terrorist hijacking.

Much of the extensive research on airline security has limited applicability because of changes in security systems and policies. Operations researchers have many new opportunities to contribute in this area.

The countermeasures and component support portfolios offer many other opportunities for contribution. The literature on the countermeasures portfolio is increasing, but many issues still need exploration. Some would benefit from collaboration between operations researchers and physical scientists, similar to that of Craft et al. (2005). OR methods are well suited for problems pertaining to cyber security, critical infrastructure protection, threat analysis, and border security; however, work in these areas so far is limited (Table 2).

We classified papers in the disaster life cycle based on their main focus (Table 2). The literature has gaps with respect to some phases in the disaster life cycle. Most OR research in homeland security concerns planning. Some concerns prevention, but we uncovered no papers on the recovery phase and very few on the response phase. There is a need for more research on

<table>
<thead>
<tr>
<th>Category</th>
<th>Planning</th>
<th>Prevention</th>
<th>Response</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sheth et al. (2005), Wang et al. (2004)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Santos (1996), Santos and Young (1999), Santos et al. (2003)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chalmet et al. (1982)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Continued.
decision making after the disaster. As the 2005 hurricanes made clear, we need to respond effectively to large-scale disasters. Operations research modeling incorporating the complex interconnections between relief agencies and government entities can clarify these chaotic situations and help relief agencies to coordinate their efforts. Operations researchers have not developed models that support real-time decision making, such as those proposed by Tien (2003, 2005) in the decision informatics area. In addition, operations researchers should extend to disaster response such collaborative decision-making frameworks as Raghu et al. (2005).

Research has begun on supply chain security, an important topic for many corporations. Chopra and Sodhi (2004) categorized supply chain risk and risk-mitigation strategies. Russell and Saldanha (2003) discussed increased costs and the changes needed in operating supply chains as a result of terrorist threats. Asbjørnslett and Rausand (1999) described how to reduce the vulnerability of production systems. Another important issue in need of OR work is private sector response to disasters. For example, Larson (2006) discussed the need for corporations, such as commercial airlines and manufacturers, to resume normal operations quickly after a disaster.

The failures of critical infrastructures subjected to hurricanes and other natural disasters highlight the need for research exploring the interdependence of critical infrastructures and for OR models to predict the likelihood of subsequent failures. Most models assume that infrastructures operate in isolation. We need to understand the relationships among infrastructures to prevent one failure from causing additional failures.

Research on homeland security can have far-reaching effects because of its importance to government and private agencies. Although these agencies offer research funding for homeland security research, the resulting studies may be classified or published in technical reports, and not released for publication in traditional academic outlets. The funding agencies may also see the details of the work as beneficial to terrorist groups. For instance, in a *Washington Post* article, Weiss (2005) reported that a paper concerning the security of the US milk supply by Lawrence M. Wein and Yifan Liu was removed from the *Proceedings of the National Academy of Sciences* Web site. Despite such possible restrictions, operations researchers have many opportunities to contribute to homeland security.

References


Hall, W. K. 1972. The application of multifunction stochastic service systems in allocating ambulances to an urban area. Oper. Res. 20(3) 558–570.


