1

INTRODUCTION

Gila Albert[1,2], Erwin A. Blackstone[3], Simon Hakim[3], and Yoram Shiftan[4]

[1] *The Ran Naor Foundation for the Advancement of Road Safety Research, Hod Hasharon, Israel*
[2] *Faculty of Technology Management, HIT – Holon Institute of Technology, Holon, Israel*
[3] *Center for Competitive Government, Fox School of Business & Management, Temple University, Philadelphia, PA, USA*
[4] *Transportation Research Institute, Technion – Israel Institute of Technology, Haifa, Israel*

1.1 OVERVIEW

Transportation systems are essential infrastructures for economic vitality, growth, and well-being throughout a country. These systems including airports, water ports, highways, tunnels and bridges, rail, and mass transit are inherently vulnerable to terrorist attacks, which dreadfully became an agonizing reality in the post-9/11 era. They might face various threats, namely, biological, chemical, nuclear (dirty bombs), cyber, and natural disaster. In fact, transportation systems continue to be a prime terrorist target (Carafano 2012).

Surface transportation is a soft target, offering terrorists relatively uncomplicated access and easily penetrable security measures. In addition, the large crowds at surface transportation facilities guarantee the attackers effectiveness and anonymity and facilitate their escape (Jenkins 2003; Potoglou et al. 2010). Therefore, terrorist attacks on various transportation systems are perceived an "efficient" means to hurt any civilization at its "soft belly."

Transportation systems are also essential for evacuation when a natural disaster, a terrorist attack, or a man-made failure occurs. All types of emergency response

Securing Transportation Systems, First Edition. Edited by Simon Hakim, Gila Albert, and Yoram Shiftan.

depend on the availability of functional roads and transportation assets (Edwards and Goodrich 2014). Efficient and effective evacuation can significantly mitigate the catastrophe consequences and therefore serves as one of the most promising means for response and recovery from such destructive incidents.

Terrorist attacks could lead to immediate and long-term catastrophic consequences. Terror, like other forms of disaster, could trigger adaptive behavior that reduces the risk of being involved in such a tragedy (Elias et al. 2013; Floyd et al. 2004; Kirschenbaum 2006). However, the changes in travel behavior may have broad and short- and long-term effects. In the short run, travelers may adopt new behavior, including changes in travel mode, routes, and destinations and even canceling some activities and postponing others (Elias et al. 2013; Exel and Rietveld 2001; Floyd et al. 2004; Holguin-Veras et al. 2003; Kirschenbaum 2006; Potoglou et al. 2010). Long-term effects may include a decrease in the market share of specific travel modes that are perceived as less secure (e.g., public bus transportation) and thereby may indirectly affect land-use patterns (Exel and Rietveld 2001; Holguin-Veras et al. 2003; Polzin 2002). Such changes can also impact ancillary industries dependent upon the affected modes of travel.

Security considerations may result in a multitude of changes in the planning, design, implementation, and operation of transportation systems (Holguin-Veras et al. 2003; Polzin 2002; Potoglou et al. 2010). In addition, they may affect financing and investments in transportation system security, which are an important tool available to decision- and policy makers in response to terrorist incidents (Polzin 2002; Sandler and Enders 2004). In this regard, the aviation security model and its security procedure in the post-9/11 era are not applicable to surface transportation, which cannot be protected in the way commercial aviation is protected. Trains and buses must remain readily accessible, convenient, and inexpensive (Jenkins 2001; Potoglou et al. 2010).

The objective of security procedures is to reach the level of security that will maximize net social benefits from the use of each transportation mode. It is recognized that various security procedures that relate to surface transportation may affect travelers' privacy and freedom (Potoglou et al. 2010). Therefore, transit agencies and security authorities have to consider the trade-off between security, mobility, and freedom and the expected negative effects of an attack. Policymaker should evaluate the overall costs of security precautions, the decline in service, and the adverse privacy consequences in comparison to the expected damage of an attack. The latter may be evaluated by the cost of various potential attacks multiplied by their probability of occurrence. No doubt, planning for prevention, deterring, response, and recovery of transportation infrastructures as well as resource allocation and priority setting is a major consideration of professionals and decision makers.

This chapter provides a comprehensive assessment of timely and challenging issues in securing transportation systems against various types of terror attacks and deals with the role of transportation networks in evacuation. It presents "state-of-the-art" efforts to improve technological and managerial security during and after natural disasters and incorporates some insights from this book.

The chapter reviews recent terror incidents targeting transportation modes and infrastructure. It also incorporates research findings on terrorist motivation and response to terrorist attacks. Then, the chapter discusses the role of efficient transportation in large-scale evacuation. The following section presents potential solutions, mainly technological and managerial improvements of how to deter, prevent, and detect these attacks and recover from severe consequences. Then, we discuss the role of not-for-profit volunteers and the private sector in securing transportation systems. The chapter concludes with evaluation issues and policy implications.

1.2 MAJOR TERRORIST ATTACKS TARGETING TRANSPORTATION SYSTEMS

Terror threats to transport systems and related infrastructure have become an agonizing reality. Before 9/11, isolated incidents all over the world may have appeared to be random: major terrorist attacks between the years 1920 and 2000 targeted surface transportation, mainly trains and buses, with bombing being the most common tactic (Jenkins 2003). This trend significantly increased after 9/11.

Lethal terror attacks on public transportation facilities occurred in the post-9/11 era in various countries. The March 2004 Madrid train bombing, the July 2005 London Underground and double-decker bus bombing, the July 2006 Mumbai train bombing, and the Moscow Metro bombing in March 2010 are all examples of the vulnerability of public transportation system and the catastrophic consequences of these attacks. At the end of 2013, three bomb attacks targeting mass transportation occurred in the city of Volgograd in southern Russia. In October 2013, suicide bombing took place on a bus; on December 29, 2013, at a railway station; and a day later, on a trolley bus. Overall, at least 40 innocent people were killed in these three attacks on Russian transportation.

Fortunately, some terrorist plots targeting subways and trains were averted: London in 2002 and 2003, Sydney in 2005, Milan in 2006, and Barcelona in 2008. New York City prevented two alleged terror attempts in recent years. In July 2006, the FBI announced that it had foiled a plot by foreign militants that was in its “talking phase” to detonate explosives in tunnels connecting New Jersey and Manhattan; and on May 1, 2010, a car bomb was discovered in Times Square. Indeed, New York’s subway system, which is uniquely attractive to terrorists, has repeatedly been the focus of briefings by counterterrorism agencies.

Israel’s surface transportation has continuously been a main target of terror attacks since the establishment of the state in 1948. In the period 1994–2006, 17 severe terror attacks occurred on Israeli public buses and such related infrastructures as bus stations, with each attack resulting in 10 or more fatalities and dozens of injuries (Butterworth et al. 2012; Johnston 2010). In Jerusalem, the capital of Israel, 117 citizens were killed in transportation-related terror attacks, and more than 770 were injured between 2001 and 2003. However, the Israeli experience especially during the Second Uprising (Intifada), which started in September 2000 and lasted through the end of 2006, enabled training drivers and employees in preventing disasters and minimizing damages and caused changes in traveler behavior. Damages were also mitigated because the terrorists employed poor tactics and lacked professional bomb-making skills (Butterworth et al. 2012).

1.2.1 Terrorist Ideology and Tactics

Review of major terror attacks suggests that certain types of attacks are “preferred” by terrorists since they are considered “more fit” or “more legal.” Conventional wisdom asserts that terror acts stem from political, social, and economics causes. However, as Bar (2004) stated, it cannot be ignored that most devastating global terrorist attacks have been perpetrated in the name of Islam (Bar 2004). Moreover, as Bar further discusses in Chapter 2, the body of Islamic rulings relating to justification of modern mass killing of civilians serves as the guideline for many Islamic terror acts.

The Islamic terrorism takes into account its religious roots, the rulings of Islamic law (shari’ah), and the outline of Islamic legal experts (fatwas). The history of Islamic terrorism involved various tactics, while terrorists choose the course of action very carefully. Agonizingly somehow, the 9/11 terror attacks seem to indicate the end of the of aircraft hijackings, most probably due to the rigorous and robust changes in security practices at airports.

The maritime terrorism threat, although low in volume, is a worrisome contingency due to its vast and largely global, unregulated, and opaque nature (Szylionwicz and Zamparini 2013). Between the years 1967 and 2007, only 0.9% of terrorist attacks in the United States involved maritime transport (Nowacki 2014) and in the past 15 years only 2% of all terrorist attacks around the world (Roell 2009). These attacks target both passenger vessels and containerized shipping (RAND Database of Worldwide Terrorism Incidents 2014) or “choke points” and mega harbors (Roell 2009). Several initiatives and regulations have been developed in the United States post-9/11 including “Automated Targeting System” (ATM), “Container Security Initiative” (CSI), and “Security and Accountability for Every Port Act” (SAFE) as described in Chapter 12 of this book by Price and Hashemi. Many initiatives have been adopted worldwide, such as the Proliferation Security Initiative (launched by the United States in 2003), a global effort to stop the trafficking of weapons of mass destruction that was endorsed by over 100 nations (Bureau of International Security and Nonproliferation 2014).

The suicide attacks targeting surface transportation, mainly trains, subways, and train stations, seem to be an increasing tactic in the post-9/11 era. The improved explosive devices used by terrorists lead to greater lethality (MIPT 2007; RAND Database of Worldwide Terrorism Incidents 2014). Shmuel Bar concludes in his chapter in this book that to combat the radical trend in Islam what may be necessary is a “Kulturkampf” of the orthodoxy against the radicals, but in the short run, the Western political and legal arsenal needs to adapt itself to the existence of a religious war.

Transportation, and especially surface transportation, need to be highly accessible and will remain a soft target for terrorists. These systems may face various additional threats, namely, biological, chemical, nuclear (dirty bombs), and cyber.

The main challenge is therefore to evaluate and develop a long-term strategy to cope with potential, rather than current, threats. In this regard, special consideration should be given to the threat of cyber.

1.2.2 Cyberterrorism

Cybersecurity, a concept that was first used by computer scientists in the early 1990s to underline a series of insecurities related to networked computers, has moved beyond to threats arising from digital technologies, innovations, and changing geopolitical conditions (Nissenbaum 2005; Nissenbaum and Hansen 2009).

Although terrorists still employ the traditional tactics, they may target information technology and networking by creating damages to their applications and respective infrastructures (Janczewski and Colarik 2008). Cyberterrorism can be defined as the intentional use of computer, networks, and the Internet to cause destruction and harm (Matusitz 2005). Terrorists can convey encrypted messages, recruit supporters, acquire targets, gather intelligence, camouflage activity, etc., with only limited risk to the attacker. This limited risk is a function of difficulties in distinguishing between a simple malfunction and an attack, in connecting an event with a result, in tracking the source of the attack, and in identifying the attacker; the widespread use of inexpensive, off-the-shelf technologies; and the vulnerability of computer systems (Tabansky 2011).

Information and communication technologies (ICT) are rapidly penetrating all modes of transportation. Cyberterrorism is a tool of destruction that may lead to various devastating effects on the transportation system. Cyberattacks can cause serious damage to a critical infrastructure, which may result in significant casualties. For example, an act of sabotage caused financial and other damages when 800,0001 of untreated sewage were released into waterways in Maroochy Shire, Australia (Abrams and Weiss 2000).

Thus far, no incidents of cyberterrorism in the transportation system have been successful. However, in Haifa, the third largest metropolitan area in Israel, the Carmel Tunnels, a major road tunnel within the city, didn't function for several hours one day in September 2013. The common hypothesis is that the cause was a cyberattack that led to malfunctioning of the communication and control of the tunnel. In Chapter 15, Talarico et al. report that beginning in 2005 the number of documented cyberattacks against the computer-controlled pipeline systems has notably increased (a series of attacks in 2013 that targeted a gas compressor station, which is a key component in moving gas through pipeline networks in the United States). In Chapter 9, Plant and Young illustrate this threat to railroads. Commuter lines and regional railroads have computer-based signaling and communications systems, which are necessary for their operation and therefore are vulnerable to cyberattack. Moreover, as discussed by Pandolfi in Chapter 10, a sophisticated cyberattack against the computer platforms that operate the railroads is becoming more likely.

Zoli and Steinberg discuss in Chapter 4 emergent challenges for the transportation sector through adoptive notion of resilience as they apply to critical infrastructure security, including cyber control systems that are vulnerable to attacks and accidents.

As mentioned by Wachs et al. in Chapter 8, the subject matter of transit security is inherently dynamic, responding to the changing nature of threats and taking advantage of the availability of new technology. Cybersecurity, which was not a significant element of transit system operations just a decade ago, is widely viewed in 2015 as an important vulnerability that requires new forms of training as well as investments in new software and technology. As Zoli and Steinberg indicate, the 2013 US Department of Homeland Security (DHS) budget of $60 billion includes a 74% increase in cyber expenditures, while the overall department funding has remained the same as in earlier years.

The cyber threat is asymmetric; no great investment is required to perpetrate cyberattacks. In contrast, defense against cyber threats must encompass all channels of attack and keep up to date with new developments. Cyberattacks are often a sophisticated combination of sabotage, espionage, and subversion (Rid 2012). Defense from cyberattack requires more resources and is becoming more difficult to control (Tabansky 2011).

1.3 THE ROLE OF TRANSPORTATION IN EVACUATION

Transportation systems are essential for evacuation when a terrorist attack, a natural disaster, or a man-made failure occurs. The bushfires in Victoria, Australia (2009); the nuclear accident in Fukushima, Japan (2011); the floods in the United Kingdom (2014); and the Hurricanes Katrina (2005), Rita (2005), Gustav (2008), Irene (2011), and Sandy (2012) in the United States showed the need for efficient large-scale evacuation methods. All types of emergency response depend on the availability of functional roads and transportation assets (Edwards and Goodrich 2014). There is no doubt that well-functioning, robust, and flexible managed transportation systems can significantly contribute to mitigate catastrophe consequences.

Large-scale evacuation utilizes existing transportation infrastructure, which requires early and continuous planning and training. In this regard, multimodal transportation networks for emergency evacuation scenarios are also in the forefront. For example, road tunnel evacuations have been studied through different evacuation models (Ronchi et al. 2012). Effective traffic management is also essential for efficient evacuation, for example, converting some roads to one way in the direction of evacuation.

Regardless of the cause or the type of disaster, various factors shape the procedure of evacuation. Among the most important are jurisdiction features (e.g., geographical area, population size, and density) and characteristics of the transportation systems (e.g., state of infrastructure, alternative modes of transport, and transport control). In evacuation, whether mandatory or voluntary, citizens with privately owned vehicles may evacuate in a timely manner, while public transportation-dependent residents remain behind. This is not always the case as when there is insufficient fuel supply in existing gas stations. In the case of public transit users, school bus systems, especially in rural areas, are ideal mode to evacuate people without a car. As Chaudhari et al. discuss in Chapter 18, school buses should be incorporated into a local emergency management plan. Hess and Farrell in Chapter 16 suggest that oversight of emergency planning by national and state governments is justified; however, local officials are usually best positioned to manage disaster preparedness, response, and recovery efforts. Our proposal for improving disaster policy questions such belief.

Heller in Chapter 17 discusses lessons learned in the aftermath of Hurricanes Katrina, Rita, Irene, and Sandy. Effective emergency planning and response requires extensive interagency coordination and collaboration, involving a multitude of professional talents. While advances in technology and social media have provided emergency managers powerful tools to enhance emergency preparedness and response, it will take a continued collaborative effort between government, the private sector, and the public to ensure a truly resilient evacuation management system.

Furthermore, evacuation procedure will benefit from innovations in communication network, social media, and joint operation centers. As stated by Daniel Hess and Christina Farrell in Chapter 16, an effective emergency response system must have resilient methods of communication and consistent messaging, as communication is often the first system to fail in the chaos of an extreme event. Hess and Farrell emphasize the importance of clear messages and redundancy in communication systems, as disasters often cause accidental technological breakdowns due to infrastructure damage or intentional shutdowns as public security measures. To address these challenges, a disaster communication plan should possess multiple channels, including websites, social media, television, radio and print, and in the recent years, especially smartphones and emergency specialized apps.

1.4 MARKET FAILURE LEADING TO A NEW MODEL OF PPP

Hurricanes Katrina and Rita showed how government at the federal, state, and local levels failed to provide adequate services to the impacted areas (US Senate 2006: Executive Summary). Mobile telecommunications trailers and the staff to operate them were offered by a private company within few hours from the start of the flood. Buses were needed to evacuate people from the disaster neighborhoods, while available school buses were unused and left on flooded parking areas to be later disabled by the flood. The State of Louisiana requested desperately needed forklifts from out of state even though they were available from local businesses. Home Depot, Walmart, and other retailers had supplies necessary to protect residents and businesses from the flood delivered from other locations (Boaz 2005). The supplies were ready for sale at the impacted areas well before the hurricane arrived. Evacuees at the gathering places lacked adequate food and essential supplies, while truckloads of major suppliers were stopped along the way. Indeed, delivery was suspended or delayed by local law enforcement officers even for trucks just outside the stadium (Business Executives for National Security (BENS) 2006; Lieberman 2005; Theroux 2005). Some “learning by doing” was evident in the response and recovery efforts to Hurricane Sandy in October 2012. However, it is likely that businesses in a competitive environment are more adaptive to such occurrences than is monopolistic government.

Another problem in responding to disasters emanates from what is termed "peak time demand" for local police, fire, and ambulance services. Specifically, greater staffing is needed during disasters than in normal "nonpeak" periods. Moreover, a severe shortage in first responders to Katrina resulted, since some workers chose to help their families and did not report for their duties (US Senate 2006: 12).

The outcry that followed Hurricanes Katrina and Rita prompted federal, state, and local governments to improve delivery of response services. The accumulated "learning by doing" and diffusion of information made governments improve first response services to Hurricane Sandy in October 2012. However, we did not experience any structural changes that assure "built-in" incentives for improved services when disaster occurs. Five major reasons prevent socially optimal allocation of resources for homeland security services.

First, government's monopolistic position in the delivery of emergency services impedes efficient homeland security services. Government often produces a given level of services at higher cost than could be produced under more competitive conditions. This phenomenon is not peculiar to government. Monopoly or noncompetition even in the private sector often leads to costs being higher than they should be or what economists call x-inefficiency (Shepherd and Shepherd 2004). Prior to their becoming more competitive, the automobile and airline industries had such a problem. Government often allocates resources to various services arbitrarily, which does not necessarily address societal preferences (Homeland Security News Wire 2011).

Second, existence of "peak time demand" for emergency personnel and equipment that is significantly greater than what government possesses for regular activities suggests that supply should closely follow the demand trends. Energy consumption is high in Northeast America during the winter peak of January–February and again in the height of the summer in July–August. These peak time demands are generally consistent over the years, and therefore electric companies can accommodate them by increasing capacity to satisfy peak time demand, by purchasing electricity from electric companies in other regions or by differentiated cost-based prices to avoid expensive investment in power plants. A similar problem exists for homeland security. However, unlike the electric power case, both the probability of occurrence and the costs of homeland security are uncertain.

A third factor that prevents a "built-in" improvement in government provision of emergency services is the rigid territorial boundaries of localities and states that dictate the availability of personnel and equipment. When a disaster occurs, local first responders are the first to respond. The state government later provides additional support with the National Guard and necessary supplies. When the president declares an area has suffered a disaster, FEMA then provides major assistance. It is important to note that all federal resources are channeled through the state and are not provided directly to the affected community. In most disasters, the local mayor is in charge of response and recovery activities. However, most events and their required response and recovery services are not confined to the legal boundaries of a locality, but become instead a regional disaster with similar necessary response and recovery efforts. Mayors and their subordinates usually have the experience and the knowledge for providing regular services and are less knowledgeable in dealing with emergency events. The National Weather Service predicted that a major storm would batter New Orleans on Friday, 3 days before it did, and will topple the levees in New Orleans. The mayor did not order a mandatory evacuation until the following Sunday, a day before the storm hit the city (Moynihan 2009).

The rigidity of government boundaries and bureaucratic structure that may accommodate “peace time” events is likely not to suit emergency conditions. A homeland security occurrence may cross counties and state boundaries, requiring coordinated and even unified response and recovery efforts, which would probably be more efficient and achieve better results.

A fourth reason why households, businesses, and government devote too few resources to homeland security is its perceived low probability of occurrence and high cost. Households and businesses are ready to spend more on high probability of occurrence events with lower costs than on a homeland security event where the expected costs are the same. Households purchase homeowners insurance, compensating mostly when a burglary occurs—an event that has a high probability of occurrence but low costs. At the same time, households are reluctant to purchase flood insurance with low probability but higher costs even though the expected costs are probably higher for floods. Indeed, even with federally subsidized flood insurance premiums, 50% drop their coverage after 3–4 years (Michael-Kayan and Kunreuther 2012). Moreover, homeowners are typically unwilling to spend mitigation measures to reduce damages from flood or other disasters. For example, in earthquake prone areas of California a 1989 survey reported that only 5–9% of respondents adopted any damage mitigation measures (Kunreuther et al. 2013).

Businesses behavior is similar, since its executives are judged by the immediate annual or even quarterly profits; a natural or man-made disaster is likely to be faced by the future managers of the firm. Corporate managers thus have been criticized for being obsessively concerned with the short-run instead of long-run interest of the firm (Blodget 2012). They arguably reduce capital investment and other long-run projects.

Government behaves similar to the firm. Elected officials serve for a stipulated period of time and need to show their short-term achievements. Spending on homeland security is likely to benefit future officials, and therefore, current budget underspending is likely to occur. Underfunding of pensions by government (and by business firms) illustrates the focus on immediate concerns. Thus, both business and governments underfund homeland security efforts. Noteworthy, exposure to competition will not bring the actual allocation closer to its socially desired level. However, public exposure to the threat to homeland security can increase efficiency. In general, citizens should be educated about the importance of taking the long-run view. It is appropriate for households, business leaders, and government officials to take the long-term view. Achieving the socially desired spending should be addressed by the provision of appropriate incentives. Such remedies are appropriate for all cases where the probability of an event is low, while the cost is very high. In the business world, stock and stock options for the managers that can be redeemed only after several years have become an important part of their compensation, promoting a longer-run view. An efficient mandatory insurance requirement could also help insure the adoption of appropriate security precautions. Lower premiums would be attained by adopting the appropriate mix of security.

A fifth reason for government's ineffective response to disasters is the desire by officials to avoid mistakes. This is the familiar type 1 and type 2 errors where type 1 involves an action that is clearly wrong and type 2 involves a decision to delay that impose costs but is less clearly wrong (Sobel and Leeson 2006). In the case of disasters, this means taking actions prematurely could be clearly shown to be a mistake so the cautious behavior approach is to wait until the disaster is imminent. Profit-motivated businesses would be expected to take the more socially appropriate action as they evidently did in the case of Katrina (Sobel and Leeson 2006).

BENS, which is an interesting solution for this problem, started following 9/11 where business and government join forces in preparing and responding to disasters. This program promotes private participation in sharing security information and joining the state's emergency operations center. It created, among other things, a registry for business resources available in a disaster and a sharing of secured communication channels. New Jersey, Georgia, Missouri and Kansas, Southern California, Iowa, and Massachusetts have all established such partnerships.

Contracting out addresses the problem of inefficiency of monopolistic government. Business monopolies are often concerned with losing their dominance through entry to their markets of close substitute producers. Therefore, monopolistic firms often charge lower than short-run profit maximizing prices to prevent such entries. Government does not face such threat and thus could retain inefficient production and pay higher than competitive wages. Contracting out the services requires clear and quantitative definition of outputs. The more vendors compete, the greater efficiency in production and the closer the price is to marginal and average cost. However, as mentioned earlier, greater competition has no bearing on the other factors.

Contracting out services that leads to competition does not address the "peak time demand" issue. Local governments then need, usually without much advance notice, labor, equipment, specific expertise, and material resources that are beyond their regular capacity. Clearly, such resources must be planned for before disasters occur. Exposure to markets to satisfy peak time demand can only partially make the missing resources available. The electric company's alternative solutions of building power plants with excess capacity, buying power from other companies, or using price differentiation are irrelevant here. We propose for consideration a homeland security model that relies on the management and entrepreneurship of volunteers or what is commonly referred to as the third sector.

Many successful leaders who have completed their business or military careers are interested in contributing their talent to the public sector, sometimes as a precursor for a political career. Such leaders are often financially secure, have high integrity, and a proven record of building an enterprise or managing an organization. Examples include Michael Bloomberg who initiated and managed a huge telecommunication company. Then, for a dollar a year, he served for 12 years as mayor of the city of New York. He contributed to the city both his talent and equipment from his companies. The late Senator Frank Lautenberg pioneered in building ADP, a firm that managed wage payments for large companies. He was elected five times to the US Senate and initiated many successful socially oriented campaigns. Mitt Romney was a successful business consultant and later was a successful head of Bain Capital. He is widely acclaimed for saving the winter Olympics at Salt Lake City and later turn to public service as the governor of Massachusetts and as a candidate for the presidency. There are numerous examples of generals who managed large military or subsequently other organizations who later devoted their efforts to public service. Business and military leaders who succeeded in their careers are likely to succeed and benefit the public. They are likely to perform at least as well as government civil servants who often lack business and entrepreneurship skills and experience. On occasion, such leaders volunteer for public service as a stepping stone toward an elected position. Involvement of such leaders in regional homeland security positions may provide new ideas and methods to existing public bureaucracy.

When a renowned business or military leader heads a regional homeland security voluntary entity, it will attract other midlevel managers to join in order to enhance relationships with other leaders and become members of such an “elite club.” It is likely that most regions include such leaders as residents. We propose that all homeland security issues including transportation infrastructure and services within a region will be under the control of this leader. We recognize the inherent difficulties and challenges of implementing such a proposal but recommended consideration as a potential vehicle to enhance homeland security.

As we suggested earlier, when a disaster occurs, localities face significant shortages in semiskilled workers including, among others, law enforcement officers, firefighters, and heavy equipment operators (Blackstone and Hakim 2013). Such usually low-paid workers cannot and should not be expected to volunteer their services. Nationwide, there are more than three times the number of private security officers than the combined federal, state, and local law enforcement agents (Blackstone and Hakim 2013). These private security officers are trained for their jobs and are usually registered with the state. Again, as in the case of equipment, most commercial establishments are closed during disasters and these officers are not being paid. It is possible to train and register those who want to be of such service during disasters. When an emergency occurs, private guards could be deputized to fulfill temporary duties of law enforcement agents.

Volunteers can be used for semiskilled tasks. Volunteers can be signed up at colleges and universities, churches and fraternal organizations, retirees, and emergency response groups. It is essential that volunteers register long before a disaster occurs, their background checks are performed, and specific training conducted. Usually, one-third of volunteers are assigned for medical tasks. Volunteers should be engaged periodically and not merely when a disaster occurs. The state usually provides localities with volunteers. Thus, registration should be made on the state’s website. Two such effective registry programs are the California Disaster Volunteer Network and the Washington State Emergency Registry of Volunteers. Volunteers that show up spontaneously at a disaster site without prior registry and training usually cause complications. The site for these volunteers should be away from the disaster area. Some can still be used in a planned fashion for certain jobs like filling sandbags and cleaning ruble (Steen 2014).

When disaster occurs, there is excessive demand for buses, trailers, lift trucks, and other heavy equipment that is beyond the available equipment of municipal and county governments. At times of disaster, similar equipment in the private sector may be idle. Registry of all public and private equipment should be prepared along with clear delivery options, leasing agreements, and payments.

The leading volunteer team relies on a PPP council that aids and advises the leading team. This council includes the mayors and the directors of emergency services of the region's cities and executives of major regional businesses and transportation companies. The council may change depending on the level and geographical spread of the disaster.

The success of establishing a new organization for homeland security depends on few factors. First, it should not be an addition to existing public entities but rather should replace them. It is especially true when existing entities are part of different hierarchical jurisdiction, like local governments, while the new entity is a regional entity. Second, public budgets for homeland security should be directed to the newly created regional entity. The regional entity will be responsible for the allocation of homeland security appropriations within their jurisdiction. Third, the state should provide a legal foundation to the regional entity so that it could sign contracts with public, private, and volunteer organizations. Fourth, when a disaster condition is announced, all powers and responsibilities are shifted from the various government agencies involved in first response and related services to the regional entity. Fifth, this new entity is not constrained by government rules and regulations. It is created as an entity that behaves like a business with flexibility in all activities. Again, we do not address the difficulties or legalities involved in creating such an organization but simply propose it as a vehicle to stimulate thought and discussion about this important issue.

The discussion so far shows that both the business sector and personal short-run preferences could prevent attaining a long-run solution, which may be preferred. For example, a long-run solution where the business spends more on R&D may lead to greater discounted present value of profits. Thus, even in a market environment, businesses do not necessarily allocate resources in a manner that maximizes long-term profits. The same inefficiency exists for government resource allocation aimed to maximize societal welfare. Elected and top government officials focus on short-term rather than long-term achievement. Local governments, for example, are likely to underfund homeland security programs. On the other hand, volunteer organizations and personnel usually take the long-run view. Volunteers are likely to stay active in their positions for long periods because of both lack of a hierarchical structure and the "spirit of the job."[1] However, use of volunteers could improve the societal use of resources.

This book deals with the security of transportation systems. All modes of transportation incorporate their own security forces whether part of the organization itself

[1] A good example is the long-term service of local volunteer firemen, and auxiliary policemen.

or contracted out to private security companies. Over 80% of all infrastructures in the United States are privately owned. This is also true for most of our rail system, water ports, and bus services. Regular security services should remain under the jurisdiction of their owners or operators. In a disaster, all responsibilities within the region are transferred to the regional entity. Representatives of these transportation systems should be part of the council. Transportation systems, unlike most other infrastructures, possess the following significant attributes:

- Bus, rail terminals, and airports generally include masses of people. Since the terrorists' goal is to inflict a major impact, such infrastructures clearly become prime targets.
- Immediate first response is to evacuate people from affected areas. Attacking or disabling major evacuation systems would yield additional loss of life, human suffering, and economic damages.
- Operating transportation systems are essential for recovery efforts and the longer-term economic and social return to normal state. Thus, targeting transportation facilities prolongs recovery. The 9/11 attack led to a significant decline in air travel, tourism, and an economic slowdown of many direct and indirect industries. The decline in GDP is estimated to have lasted a full 2 years (Jackson 2008).
- Terrorist access to major public transportation targets is relatively easy in comparison to power, water, and other infrastructures. Transportation systems are usually accessible, while access to other critical infrastructure is limited and can be easier guarded. Current technologies are still limited in detecting explosives or individuals who might approach critical points in targeted areas to inflict maximum damage.
- Maritime commerce involves hundreds of thousands of containers a year. Many of these containers move through several water ports before reaching a US harbor. Existing technology does not allow thorough checking of these containers even though an undetected dirty bomb poses a high threat. These containers are often immediately transferred to trucks for transit to various US destinations where the explosion may occur.

Government on its own cannot secure transportation facilities and cannot allocate sufficient resources for such efforts. Also, 85% of infrastructures are owned by private companies that are responsible for their own security. Government can initiate, cultivate, and encourage such efforts by providing appropriate incentives for the creation of the three sectors' joint regional homeland security authority.

1.5 SECURITY STRATEGY

Homeland security obligations are categorized into preparation, response, and recovery from terrorist or natural disasters. Preparation is the planning and building of effective force for the two tasks of response and recovery. Preparation involves all activities prior to a disaster including management, deterrence, and prevention. Responses are the activities conducted immediately during the disaster and its immediate aftermath where the main goal is to save lives. Recovery activities extend over the long term and are intended to yield a quick return to normalcy. Our model in the previous section suggests that the authority is responsible for all three tasks with a major role in the preparation phase. The authority controls and coordinates all involved entities.

The authority is in charge of resource allocation to all three tasks and among all involved entities. In most regional jurisdictions, like metropolitan areas, several critical infrastructures could be subjected to terrorist attacks. Examples include airports, water ports, power stations, railway stations, bus terminals, and schools.

The objective is to allocate the available resources to the three tasks of preparation, response, and recovery in a manner that minimizes the expected value of all damages.

In preparation, the main expense is on deterring and preventing an attack. Deterring activities are indication that the place is well protected and the probability of a successful attack is low. Prevention activities are physical measures that make entry difficult, time consuming, and increase the probability of apprehension. In protecting structures from burglary, these activities entail relatively high probability for avoiding an actual burglary. However, deterrence is minimal for terrorists who target an infrastructure, and "conventional" preventive measures are easily overcome. Routine prevention measures are unlikely to prevent entry by well-trained terrorists. For example, an armed guard and a high fence are unlikely to deter or prevent terrorists who intend to capture children. Even routine security of a power station is unlikely to deter terrorists who intend to detonate an explosive. Professional terrorists can chose a region in which to attack, the target, the time, and the method, among many possible targets. At the same time, in the absence of precise intelligence, the "legal" community has limited information and budget to protect all potential targets against professional terrorists in any given region. Great asymmetry exists between the terrorists that initiate an attack and the "legal" community that protects against it. A "thin" level of protection of all potential targets will not deter and will provide insignificant protection against professional terrorists. The same principle holds in protecting against a major natural disaster. Thus, most public resources should be spent on effective mobile response units that could be dispatched to any location in the region.

Further, with existing data-mining activities and electronic surveillance, a major land attack on a critical infrastructure is almost impossible. A cyberattack that is prepared and executed from a distance requires significantly fewer financial resources and is likely to inflict greater damage without endangering terrorist lives. Even highly sophisticated cybersecurity could be ineffective for a few high-impact attacks. Thus, resources are better spent on response, preventing aftermath damages, and recovery efforts than on deterrence and physical preventive measures.

At the same time, some deterring and preventive measures are effective against less professional, self-motivated terrorists or people with emotional disturbances. Such minimal efforts are the responsibility of the infrastructure's owners. Government's role is to encourage owners and managers of critical infrastructures to protect their facilities by linking damages to self-inflicted costs. A basic level of protection against an attack of nonprofessional terrorists is an integral part of “reasonable” protection by the owners of the facility. The incentive for such self-funded security arises from the prospect of liability suits against the property by third-party victims of an attack. The courts usually find commercial owners liable in law suits for damages when “reasonable” protection is lacking. It is reasonable to assume that these practices of the courts lead commercial and industrial establishments to undertake the minimum required level of protection.

1.6 BOOK STRUCTURE AND CHAPTERS

This handbook focuses on how to protect our transportation systems and how to better plan evacuation when severe disasters occur. It contains insights and recommendations from a group of internationally recognized experts and provides guidelines for policy and public decision making as well as suggestions for IT companies for possible new products. The following issues are addressed in the book:

- Technological measures and innovative solutions to target protection and response provisions to protect our transportation infrastructure, consider their feasibility, and provide an economic evaluation
- Institutional restructuring that may increase security for critical infrastructure, for example, public–private partnerships
- Changes in travel behavior as a response to terrorism and natural disaster
- Policy implication and recommendations for preparation, response, and system recovery

The book consists of 17 invited original chapters, which are categorized into three sections.

1.6.1 Section 1: Motivation and Challenges

This section includes six chapters explaining the motivation for terrorist attacks against transportation modes and infrastructure and derived challenges. It describes radiological, cyber, and nuclear threats; demonstrates the impact of fear of attack on the general public; and presents prevention as well as recovery challenges.

This section starts with Chapter 2 by Bar that describes the nature of Islamic ideology, the tactics, and the justification for attacking mass transportation. This leads to the conclusion that the tactical appeal for terrorists will not vanish, and therefore, the main challenge is how best to protect mass transportation from attacks or more likely to mitigate their damages.

In Chapter 3, Altshuler et al. consider efficient deployment schemes of surveillances and monitoring units in key locations of the network for homeland security purpose. Zoli and Steinberg explore in Chapter 4 emergent challenges for the transportation sector through adaptive notions of resilience as they apply to critical infrastructure security. In Chapter 5, Valeri et al. analyze the impact of security on long-distance travel behavior and investigate changes in travel and mode choices in response to variations in security levels and features. In Chapter 6, Rubenstein et al. review radiological and nuclear weapon threats to transportation systems and discuss methods to mitigate them. The first section ends with Yaar et al. who describe in Chapter 7 a comprehensive experimental program that was conducted in Israel to evaluate the consequences of a radiological dispersive device explosion.

1.6.2 Section 2: Security Consideration for Modes of Transportation

The second section includes seven chapters presenting the vulnerability of the various modes of transport. It describes and evaluates security consideration of public transportation, airports, seaport, railroads, and pipelines.

This section starts with Chapter 8, authored by Wachs et al., which describes and categorizes security risks and prevention tactics in public transport systems on streets and amid mixed traffic that include stations and exclusive rights-of-way. Similar prevention strategies are addressed to terrorism and common criminal activities. In Chapter 9, Plant and Young illustrate threats and vulnerabilities to passenger and rail freight operations. Key policies and programs designed to address these security issues with an emphasis on the role of the DHS, information sharing, and public–private partnerships are discussed. In Chapter 10, Pandolfi considers steps that can be taken to improve or to change the security management in order to advance the overall operations of the American freight railroad system. Then, Poole discusses in Chapter 11 productive resource allocation in homeland security, with a primary focus on measures implemented at airports to protect passengers and planes. The chapter compared and contrasted US airport security policies and practices with those of Canada and the European Union. It also discusses whether it is feasible to use forms of cost–benefit analysis and cost-effectiveness analysis for resource allocation on a risk-based basis and explores the question of who should pay for airport security. In Chapter 12, Price and Hashemi introduce seaport operations, port and security infrastructure, shipping container logistics, and the need to secure the ports with minimum cargo disruption. Security strategies and technology are examined, along with a “great debate” on nonintrusive scanning of all or only high-risk containers. In Chapter 13, Inman and Morris discuss the Transportation Worker Identification Card (TWIC) program compliance as a mean to help secure the nation’s vital maritime transportation infrastructure, problems, evaluation, and the role of privatization. In Chapter 14, Polydoropoulou and Tsirimpa analyze port users’ attitudes and perceptions regarding security threats, as well as modeling travelers’ choice of port under alternative security scenarios, based on a case study for the island of Chios in Greece. The section ends with Chapter 15 by Talarico et al. who investigate security issues related to the pipeline systems. Traditional and advanced security measures used in pipelines are presented as well as future developments of new emerging technologies and recent applications. They also provide a support decision model aimed at increasing the effectiveness of the set of selected countermeasures for the pipeline infrastructure security within a limited budget.

1.6.3 Section 3: The Role of Transportation in Evacuation

This section includes three chapters dealing with the role of transportation in evacuation as a supporting response operations in large national disasters. The section starts with Chapter 16, authored by Daniel Hess and Christina Farrell who explore the factors and outcomes of mandatory and nonmandatory evacuation related to non-noticed and limited noticed disasters in nonurban settings with the purpose of improving evacuation policy and planning. Two examples—bushfires (in 2009) in Victoria, Australia, and a nuclear accident (in 2011) in Fukushima, Japan—are provided. In Chapter 17, David Heller discusses how better evacuation plans and procedures can significantly reduce hurricanes and other natural disaster impacts, based on lessons learned from Katrina (in 2005), Rita (in 2005), Irene (in 2011), and Sandy (in 2012), all in the United States. The section ends with Chapter 18 by Jaydeep Chaudhari et al. focusing on how public transportation can perform multiple roles and can be an effective partner in the four tasks of emergency management planning: mitigation, preparedness, response, and recovery. The chapter discusses how adequately transit systems are prepared and the challenges and issues that may arise in the event of an emergency evacuation.

1.7 CONCLUSION: RESOURCE ALLOCATION AND POLICY IMPLICATION

Transportation systems including airports, airlines, water ports, ships, highways, pipelines, buses, rail, and mass transit are inherently vulnerable to different types of terror attacks. Bus, rail terminals, and airports generally include masses of people. Since the terrorists' goal is to inflict a major impact, such infrastructures are perceived by terrorist as "efficient" targets to hurt any civilization at its "soft belly." Therefore, it is likely to assume that transportation systems will continue to be a prime terrorist target. While bombing is the most common, the threats are various: biological, chemical, nuclear (dirty bombs), and cyber.

Terrorist access to major public transportation targets is relatively easy in comparison to power, water, and other infrastructures. Transportation systems should be highly accessible and accordingly are usually open to people, while access to other critical infrastructure is limited and can be easier guarded. In this regard, the aviation security model and its security procedure in the post-9/11 era are not applicable to surface transportation, which cannot be protected in the way commercial aviation is protected. Current technologies are still limited in detecting explosives or individuals who might approach critical points in targeted areas to inflict maximum damage. Maritime commerce in containers involves hundreds of thousand a year. Many of these containers move through several water ports before reaching the US harbor. Existing technologies do not allow thorough checking of these containers even though undetected dirty bombs cause a high threat. These containers are often immediately transferred to trucks for transit to various US destinations where the explosion may occur.

Even highly sophisticated infrastructure protection could be ineffective for a few high-impact attacks. Thus, resources are better spent on response, preventing aftermath damages, and recovery efforts than on deterring and physical prevention measures. Operating transportation systems are essential for recovery efforts and the longer-term economic and social return to normal state. Thus, targeting transportation facilities prolongs recovery.

Review of major terror attacks suggests that certain types of attacks are "preferred" by terrorists since they are considered "more fit" or "more legal." It cannot be ignored that most devastating global terrorist attacks have been perpetrated in the name of Islam, and as Bar discusses in Chapter 2, the body of Islamic rulings relating to justification of modern mass killing of civilians serves as the guideline for many Islamic terror acts. Bar concludes in his chapter that to combat the radical trend in Islam, what may be necessary is a "Kulturkampf" of the orthodoxy against the radicals, but in the short run, the Western political and legal arsenal needs to adapt itself to the existence of a religious war.

Transportation systems are essential for evacuation when a terrorist attack, a natural disaster, or a man-made failure occurs.

Efficient and effective evacuation can significantly mitigate the catastrophe consequences and therefore serves as one of the most promising means to response and recovery from such destructive incidents. Large-scale evacuation utilizes existing transportation infrastructure, requiring early and continuous planning and training and a well-managed and well-coordinated process once an evacuation starts. In this regard, multimodal transportation networks for emergency evacuation scenarios should also be in the forefront. In the case of public transit users, for example, school bus systems, especially in rural areas, are ideal for providing evacuation. As discussed by Chaudhari et al. in Chapter 18, school buses should be incorporated into a local emergency management plan. Hess and Farrell in Chapter 16 suggest that oversight of emergency planning by national and state governments is justified; however, local leaders are usually best positioned to manage disaster preparedness, response, and recovery efforts. Furthermore, evacuation procedure will benefit from innovations in communication network, social media, and joint operation centers. As stated in this chapter, an effective emergency response system must have resilient methods of communication and consistent messaging, as communication is often the first system to fail in the chaos of extreme events.

Five major reasons prevent socially optimal allocation of resources for homeland security services. First, government's monopolistic position in the delivery of emergency services impedes efficient homeland security services. Second, "peak time demand" exists for emergency personnel and equipment. Third, rigid territorial boundaries of localities and states dictate the availability of personnel and equipment and often prevent efficient efforts. Fourth, perceived low probability of occurrence and high cost discourage appropriate spending. A fifth reason is the desire by officials to avoid mistakes. In the case of disasters, this means taking actions prematurely could be clearly shown to be a mistake so the cautious behavior approach is to wait until the disaster is imminent. The objective is for households, business leaders, and government officials to take the long-term view. Achieving the socially desired spending should be addressed by the provision of appropriate incentives.

Profit-motivated businesses would be expected to take the more socially appropriate action as they evidently did in the case of Katrina (Sobel and Leeson 2006). Contracting out addresses the problem of inefficiency of monopolistic government. Some private guards could be deputized when an emergency occurs to fulfill temporary duties of law enforcement agents. Volunteers can be used for such semiskilled tasks. At times of disaster, similar equipment in the private sector may be idle. Registry of all public and private equipment should be prepared along with clear delivery options, leasing agreement, and payments.

The success of establishing a new organization for homeland security depends on few factors. First, it should not be an addition to existing public entities but rather should replace them. Second, public budgets for homeland security should be directed to the newly created regional entity. Third, the state should provide a legal foundation to the regional entity to sign contracts with public, private, and volunteer organizations. Fourth, when a disaster condition is announced, all powers and responsibilities are shifted from the various government agencies involved in first response and related services to the regional entity. Fifth, this new entity should not be constrained by government rules and regulations.

REFERENCES

Abrams, M. and Weiss, J. 2000. Malicious control system cyber security attack case study—Maroochy water services, Australia. Available at http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf. Last visited October 17, 2014.

Bar, S. 2004. The religious sources of Islamic terrorism. *Policy Review*, 125: 27–37.

Blackstone, E.A. and Hakim, S. 2013. Competition versus monopoly in the provision of police. *Security Journal*, 26(2): 157–179.

Blodget, H. 2012. We need to stop maximizing profit. *Business Insider*, December.

Boaz, D. 2005. Catastrophe in big easy demonstrates big government's failure. *Commentary*, September 19. Available at http://www.cato.org/publications/commentary/catastrophe-big-easy-demonstrates-big-governments-failure. Last visited October 20, 2014.

Bureau of International Security and Nonproliferation. 2014. Proliferation security initiative participants. US Department of State, Washington, DC, June 14. Available at http://www.state.gov/t/isn/c27732.htm. Last visited October 20, 2014.

Business Executives for National Security (BENS). 2006, November. Regional public–private partnerships: The next wave in homeland security. BENS, Washington, DC.

Butterworth, B.R., Dolev, S., and Jenkins, B.M. 2012. Security awareness for public bus transportation: Case studies of attacks against the Israeli public bus system. Report no. 11-07. Mineta Transportation Institute, San Jose State University, San Jose, CA.

Carafano, J.J. 2012. Next step for transportation security. Testimony before Subcommittee on Transportation Security, Committee on Homeland Security, US House of Representatives, September 11.

Edwards, F.L. and Goodrich, D.C. 2014. Exercise handbook: What transportation security and emergency preparedness leaders need to know to improve emergency preparedness. Report no. CA-MTI-14-1103. Mineta Transportation Institute, San Jose State University, San Jose, CA.

Elias, W., Albert, G., and Shiftan, Y. 2013. Travel behavior in the face of surface transportation terror threats. *Transport Policy*, 28: 114–122.

Exel, N. and Rietveld, P. 2001. Public transport strikes and traveller behaviour. *Transport Policy*, 8(4): 237–246.

Floyd, M., Gibson, H., Pennington-Gray, L., and Thapa, B. 2004. The effect of risk perceptions on intentions to travel in the aftermath of September 11, 2001. *Journal of Travel and Tourism Marketing*, 15(2–3): 19–38.

Holguin-Veras, J., Paaswell, R.E., and Yali, A.M. 2003. Impact of extreme events on intercity passenger travel behavior: The September 11th experience. TRB 2003 annual meeting, challenges. *Homeland Security Affairs*, 8(October): Article 18.

Homeland Security News Wire. 2011. Counterterrorism financing: Analysts question wisdom of DHS spending, May 20. Available at http://www.homelandsecuritynewswire.com/analysts-question-wisdom-dhs-spending. Last visited October 10, 2014.

Jackson, O. 2008. The impact of the 9/11 terrorist attack on the U.S. economy. March 3. Available at http://www.journalof911studies.com/volume/2008/OliviaJackson911andUS-Economy.pdf. Last visited October 10, 2014.

Janczewski, L.J. and Colarik, A.M. 2008. *Cyber warfare and cyber terrorism*. IGI Global, Hershey, PA.

Jenkins, B.M. 2001. Protecting public surface transportation against terrorism and serious crime: An executive overview. Report no. 01-14. Mineta Transportation Institute, San Jose State University, San Jose, CA.

Jenkins, B.M. July 2003. *Improving public surface transportation security: What do we do now?* The Lexington Institute, Arlington, VA.

Johnston, W.R. 2010. Chronology of terrorist attacks in Israel: Introduction. Available at http://www.johnstonsarchive.net/terrorism/terrisrael.html. Last visited October 24, 2014.

Kirschenbaum, A. 2006. Terror, adaptation and preparedness: A trilogy for survival. *Journal of Homeland Security and Emergency Management*, 3(1): 23–48.

Kunreuther, H., Michael-Kayan, E., and Pauly, M. 2013. Making America more resilient toward natural disasters: A call for action. *Environment*, 55(4): 15–23.

Lieberman, J. 2005. Hurricane Katrina: What can government learn from the private sector's response. Presentation at the US Senate, November 16. http://www.hsgac.senate.gov//imo/media/doc/111605JILOpen.pdf?attempt=2. Last visited October 6, 2014.

Matusitz, J. 2005. Cyberterrorism. *American Foreign Policy Interests*, 2: 137–147.

Michael-Kayan, E. and Kunreuther, H. 2012. Paying for future catastrophes. *New York Times, Sunday Review*, November 24.

MIPT. 2007. *The MIPT annual 2006*. National Memorial Institute for the Prevention of Terrorism, Oklahoma City, OK.

Moynihan, D.P. 2009. *The response to hurricane Katrina*. In *Risk governance deficits: An analysis and illustration of the most common deficits in risk governance (Report)*. International Risk Governance Council, Geneva. Available at http://irgc.org/wp-content/uploads/2012/04/Hurricane_Katrina_full_case_study_web.pdf. Last visited October 10, 2014.

Nissenbaum, H. 2005. Where computer security meets national security. *Ethics and Information Technology*, 7(2): 61–73.

Nissenbaum, H. and Hansen, L. 2009. Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, 53: 1155–1175.

Nowacki, G. 2014. Threat assessment of potential terrorist attacks to the transport infrastructure. *TransNav*, 8: 219–227.

Polzin, S.E. 2002. Security considerations in transportation planning. A white paper prepared for the Arizona Department of Transportation. Southeastern Transportation Center.

Potoglou, D., Robinson, N., Chong, W.K., Burge, P., and Warnes, R. 2010. Quantifying individuals' trade-offs between privacy, liberty and security: The case of rail travel in UK. *Transportation Research Part A*, 44: 169–181.

RAND Database of Worldwide Terrorism Incidents. 2014. Terrorism incidents database search. Available at http://smapp.rand.org/rwtid/search_form.php. Last visited April 23, 2014.

Rid, T. 2012. Cyber war will not take place. *Journal of Strategic Studies*, 35(1): 5–32.

Roell, P. 2009. Maritime terrorism—a threat to world trade? Statement by Dr. Peter Roell at the International Conference on Comprehensive Security in the Asia-Pacific Region, November 30–December 1, 2009, Tokyo, Japan.

Ronchi, E., Colonna, P., Capote, J., Alvear, D., Berloco, N., and Cuesta, A. 2012. The evaluation of different evacuation models for road tunnel safety analyses. *Tunnelling and Underground Space Technology*, 30: 74–84.

Sandler, T. and Enders, W. 2004. An economic perspective on transnational terrorism. *European Journal of Political Economy*, 20(2): 301–316.

Shepherd, W.G. and Shepherd, J.M. 2004. *The economics of industrial organization*. Waveland Press, Long Grove, IL.

Sobel, R.S. and Leeson, P.T. 2006. Government's response to hurricane Katrina: A public choice analysis. *Public Choice*, 127: 55–73.

Steen, M. 2014. Volunteer force: How to recruit, retail and organize volunteers. *Emergency Management*, September: 23–25.

Szylionwicz, J.S. and Zamparini, L. 2013. *Maritime security: issues and challenges*. In *Maritime transport security* (Eds. Bichou, K., Szylionwicz, J.S., and Zamparini, L.). Edward Elgar Publishing, Glos: 13–23.

Tabansky, L. 2011. Basic concepts in cyber welfare. *Military and Strategic Affairs*, 3(1): 75–92.

Theroux, M.L.G. 2005. Public and private responses to Katrina: What can we learn? The Independent Institute, October 20. Available at http://www.independent.org/newsroom/article.asp?id=1589. Last visited October 7, 2014.

US Senate. 2006. Hurricane Katrina: A nation still unprepared. Special Report of the Committee on Homeland Security and Governmental Affairs. Special Report 109-322. Available at http://www.gpo.gov/fdsys/pkg/CRPT-109srpt322/pdf/CRPT-109srpt322.pdf. Last visited October 13, 2014.