Paper No. 03-4495

Antiterrorism Security and Surface Transportation Systems

Review of Case Studies and Current Tactics

Camille N. Y. Fink

The events of September 11, 2001, brought the issue of transportation security and terrorism to the forefront of policy and government. Public surface transportation systems are especially vulnerable because they are by nature open and accessible. They also serve large numbers of people in extensive networks. Case studies of transit systems and terrorist incidents offer examples of effective planning and response as well as gaps in security systems. Systems in London and Paris have experienced bombing attacks. Tokyo was the site of a chemical attack. Preparation against terrorist attacks involves assessments of vulnerabilities, mitigation of weaknesses in the system, and the development of effective response and emergency plans. Cost factors are a particular concern for transit officials. The use of design elements, closed-circuit television, training, and exercises, together with the establishment of close relationships with other local, state, and federal agencies, appears to be the most cost-effective security option.

While transportation security officials have been aware of the threat of terrorist attacks on transportation networks for some time, the events of September 11, 2001 (9/11), revealed both vulnerabilities in security systems and the unimaginable consequences of such breaches. Surface transportation systems are especially attractive targets for would-be terrorists wanting to cause the maximum amount of disruption and harm. This paper reviews pertinent literature about terrorism security and emergency-response planning for surface transportation systems. Case studies of several international terrorist incidents involving these systems provide extremely useful insight into the kinds of effective measures now in place as well as the ways in which security can be further improved. Several of these studies examine the more common threats against transit systems, particularly bombing incidents on larger urban transit networks. Others chronicle incidents involving emerging threats such as chemical attacks on subway systems.

In contrast to some earlier reviews of transit terrorism incidents, this analysis also considers the cost-effectiveness of various antiterrorism security measures and argues that such an approach should be employed in evaluating options to be implemented. Security personnel can draw from work conducted in other sectors, including highway vulnerability assessments, to develop useful cost–benefit guidelines. These types of considerations are especially important in post-9/11 transit security planning in which transit operators must contend with both increases in security needs and decreases in available funding for these activities.

Department of Urban Planning, University of California, Los Angeles, 3250 Public Policy Building, Box 951656, Los Angeles, CA 90095-1656.

HISTORICAL OVERVIEWS OF TERRORISM AND SURFACE TRANSPORTATION SYSTEMS

The first step in developing a strategy for securing transit systems is understanding and defining the scope of activities that fall under the term "terrorism." The Federal Bureau of Investigation (FBI) uses the following definition:

> The unlawful use of force or violence committed by a group(s) of two or more individuals, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (*1*)

Many transit agencies, however, use a broadened definition that includes quasi terrorism. Quasi-terrorist acts have the following characteristics: a criminal, ideological, or religious objective; one person committing the act; and the threat of force or violence (*1*). Although terrorist acts are clearly outlined as those involving specific perpetrators, targets, and motives, the definition of quasi terrorism is more vague and ambiguous. The notion of quasi terrorism may perhaps reflect the somewhat uncertain boundary and relationship between terrorism and more general crime and safety issues.

Analyses of trends of all terrorist attacks in recent years indicate that while the number of acts of terrorism has decreased, their lethality has increased. In addition, the number of attacks against transportation systems increased in the 1990s. In 1991, transportation systems were the target of 20% of all violent attacks. This rose to almost 40% in 1998 (*1*). Jenkins' comprehensive chronology of 900 terrorist attacks involving surface transportation from 1920 to 2000 provides an analytical model useful in identifying the most salient patterns and trends (*2*). He finds that about two-thirds of attacks were intended to kill, with 37% involving fatalities. Of these incidents, about three-fourths involved more than 1 fatality and 23% involved 10 or more fatalities (*2*).

Jenkins and Gersten also examine the public system targets and tactics used worldwide by terrorists from 1920 to 2000 (*3*). These results show that the largest percentage, 46%, of terrorist attacks against public surface transportation systems was carried out on subways and trains, subway and train stations, and rail (Figure 1). The use of bombs was overwhelmingly the most common tactic (60% of all attacks) (Figure 2). Although chemical, biological, and radiological attacks made up a very small percentage of all tactics used (about 1%), a later section of this paper will discuss the ways in which subway systems are particularly susceptible to these threats.

Surface transportation systems are in general easy and effective targets for terrorists; this fact is reflected in the relatively significant proportion of attacks occurring on these systems. The vulnerabilities

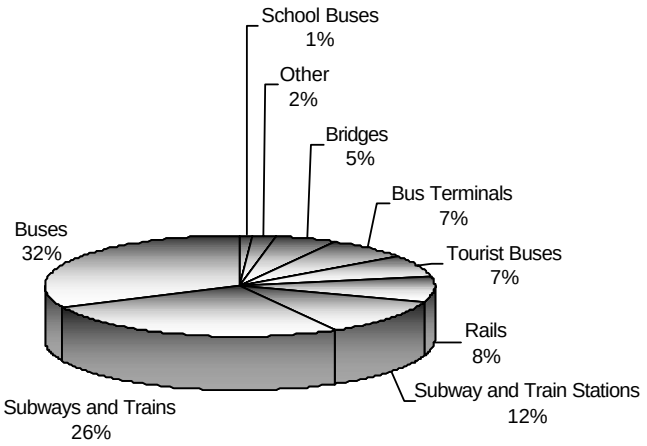

FIGURE 1 Targets of attacks on public surface transportation systems, 1920–2000 (*3*).

lie in the fact that these systems are very public, convenient, and accessible. They carry large numbers of people daily through extensive networks of stations, stops, and facilities (*4*). The volume of passengers and, in particular, the very high number of system access points make it impossible for transit operators to employ many of the security tactics used in commercial aviation. Preventive security measures such as the screening of passengers and luggage with X-ray machines and metal detectors, hand searches, passenger profiling, explosives sniffers, and armed guards would lead to intolerable public transit delays and costs. As a result, surface transportation security tends to focus more on mitigation, quick response, and the rapid restoration of services after an incident (*5*).

Boyd and Sullivan conducted a 1997 TRB survey to assess both the perceptions of transit operators about terrorism and security and the status of agencies' existing emergency preparedness, planning, and response procedures (*4*). Forty-two U.S. transportation agencies participated in the survey, including 31 agencies that provide some sort of rail service. Most of these agencies also operate bus service. Urban and commuter rail systems rank highest in perceived risk as targets of terrorism: about 2.2 and 2.6, respectively, on a scale from 1 (most likely) to 6 (least likely) (Figure 3). In addition, detonation of explosive devices ranks highest: about 2.4 on a scale of 1 (most likely) to 7 (least likely) as the act perceived to pose the greatest threat in the next 5 years (Figure 4). Figure 5 shows that a majority of these agencies (88%) have dealt with bomb threats in addition to a variety of other security threats. Clearly, the security of subways as part of urban rail systems and the threat of explosives are of significant concern to a majority of transit agency operators. These perceptions of risk have almost certainly heightened in the post-9/11 era, although, to date, no follow-up survey of perceived transit security risks has been conducted.

CASE STUDIES OF TERRORIST ATTACKS ON PUBLIC SURFACE TRANSPORTATION SYSTEMS

Case studies of surface transportation systems that have suffered terrorist attacks offer examples of effective measures as well as gaps in antiterrorism security plans. Jenkins has conducted a series of case studies of both international and domestic surface transportation systems, including networks in London, Paris, Tokyo, New York City, Atlanta, and the San Francisco Bay Area (*3*, *5*). The analyses examine particular incidents and responses as well as general security strategies, procedures, and training. Jenkins' case studies are extremely useful, particularly in compiling lessons-learned lists that can be applied to other transportation systems with similar physical and organizational characteristics. The following discussion provides a summary of three international case studies involving bombing and chemical terrorism attacks at subway systems in London, Paris, and Tokyo. The preparedness, response, and recovery lessons are highly applicable and relevant to many public transit systems in the United States.

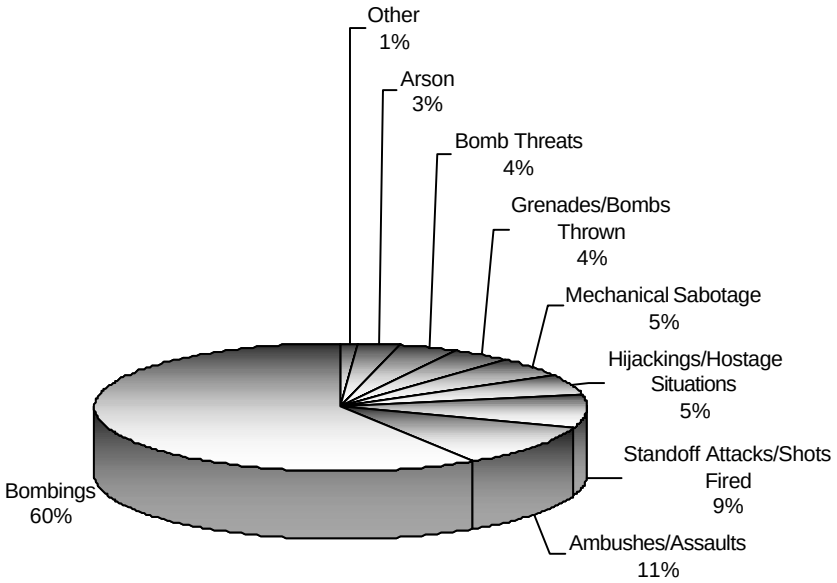

FIGURE 2 Tactics used against surface transportation systems, 1920–2000 (*3*). (NOTE: numbers are rounded to nearest whole number.)

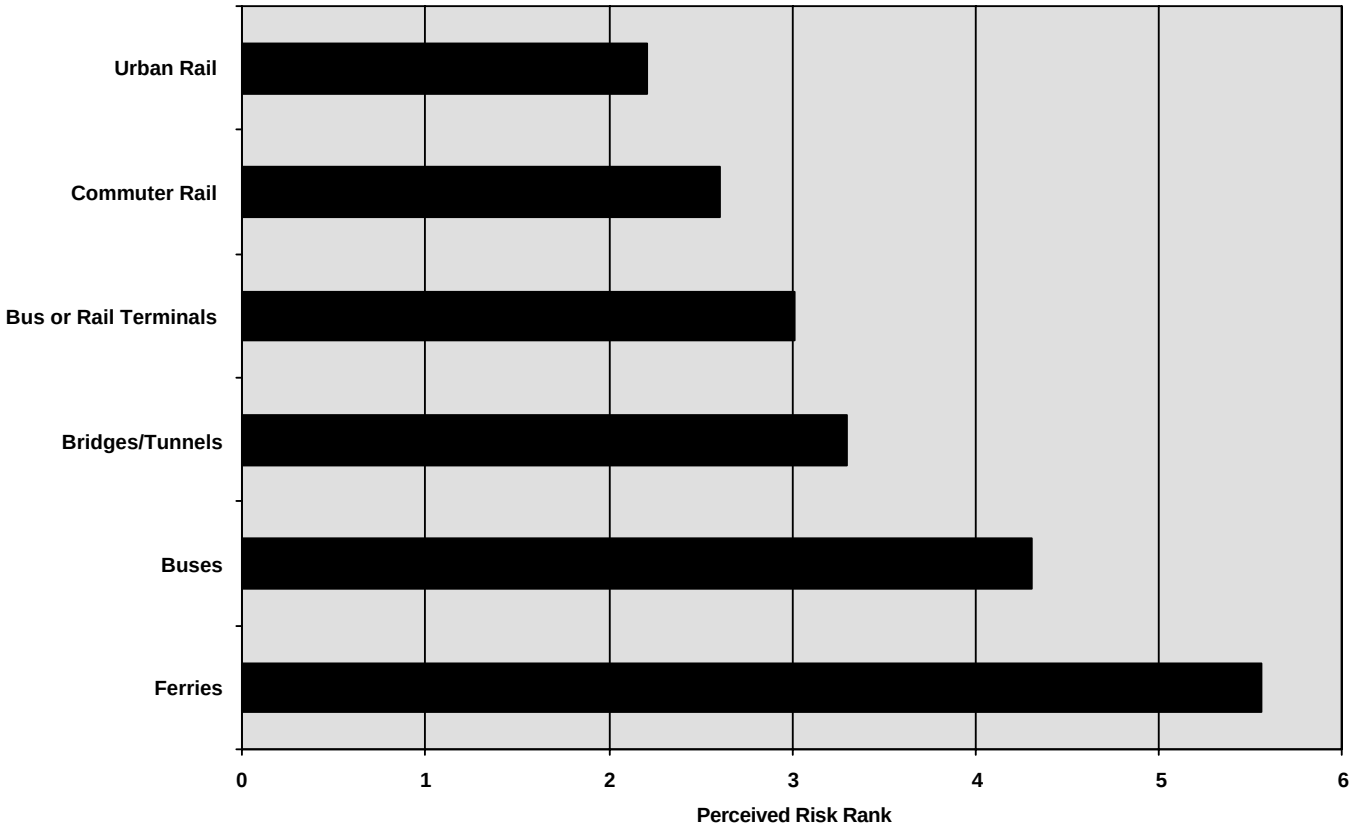

FIGURE 3 Transit modes perceived by participating transit agencies as presenting the greatest risk of becoming targets of terrorism (*4*), ranked from 1—most likely to 6—least likely.

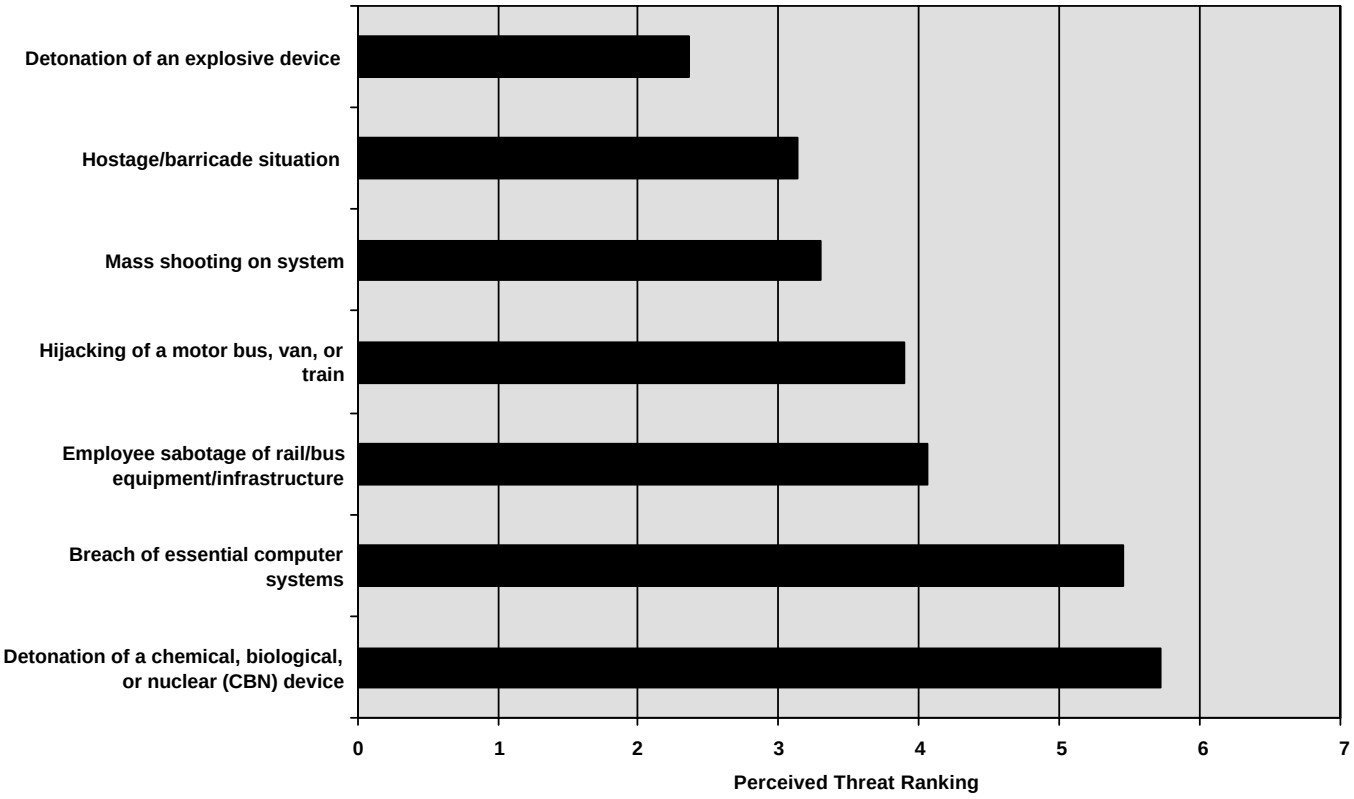

FIGURE 4 Types of terrorist and quasi-terrorist events perceived by transit agency personnel to present the greatest threats over the next 5 years (*4*), ranked from 1—most likely to occur to 7—least likely to occur.

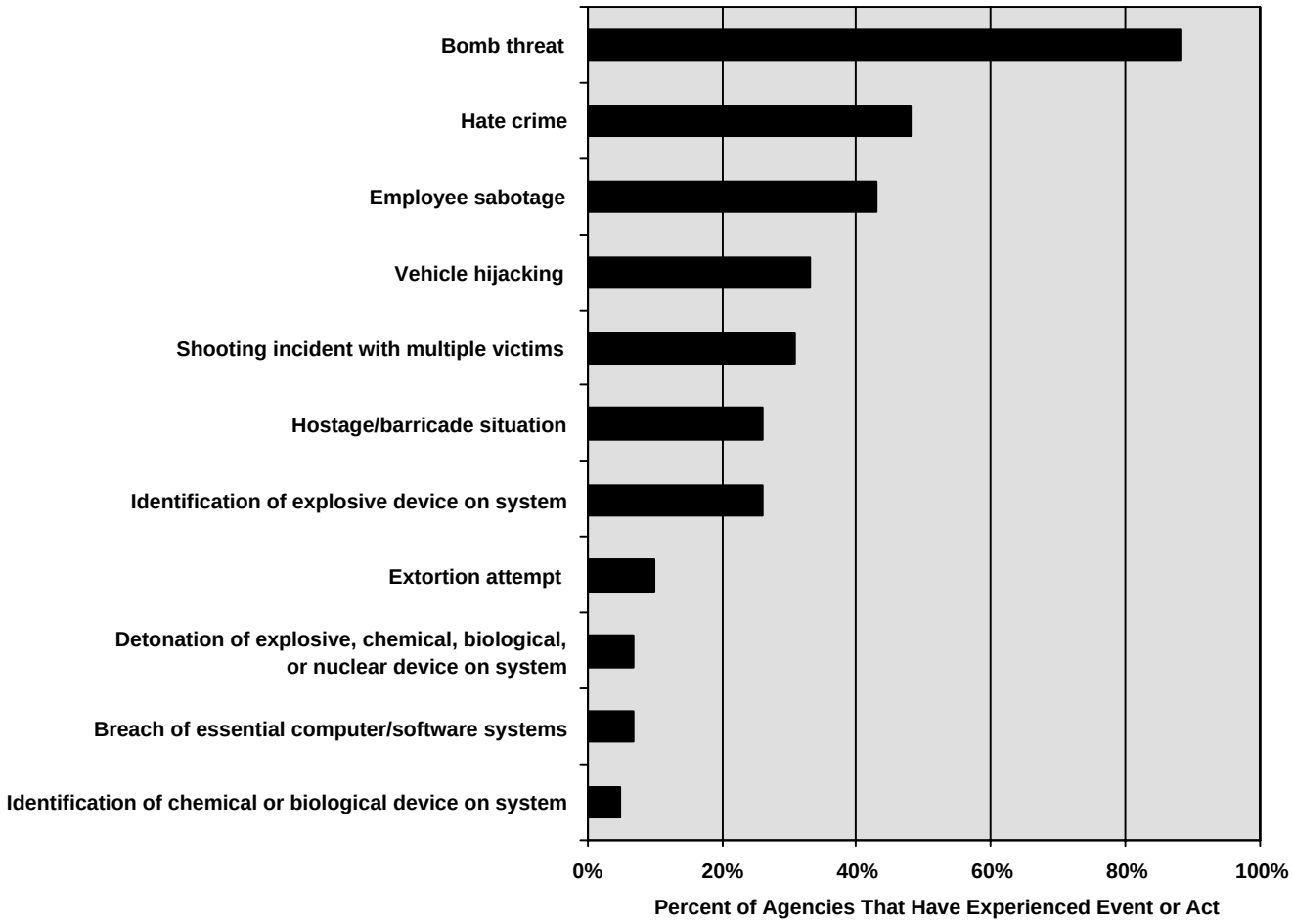

FIGURE 5 Participating transit agencies' experiences with terrorist events and acts of extreme violence (*4*).

London and Paris: Terrorist Bombing Attacks

The provisional wing of the Irish Republican Army (IRA) waged a terrorist campaign in England, primarily involving the London Underground and commuter rail network, from 1973 to 1998, when the group agreed to a cease-fire. The goal of the IRA appears to have been largely one of disruption rather than casualties: "Between 1991 and 1997, there were 41 IRA attacks on transportation targets in England involving 81 devices, 29 explosions, and 3 deaths" (*3*). The explosions, telephone bomb threats, investigation of suspicious objects, copycats, and pranksters proved to be an enormous burden on transportation security forces.

Officials worked to devise a security strategy whose primary goals were to protect lives and minimize the service disruption caused by the attacks. One program, crime prevention through environmental design (CPTED), included strategies such as improving visibility, lighting, and fencing as well as installing bomb shelter areas, blast-resistant trash cans, expanded closed-circuit television (CCTV) networks, and passenger communications systems. In addition, extra staff and patrols were trained and deployed to increase surveillance and handle unattended items. Authorities also worked to analyze "each and every terrorist incident and threat to look for patterns that would enable them to more easily distinguish hoaxes from genuine terrorist threats. . . . All threats were treated seriously initially and then, depending on the available information, downgraded to probable hoaxes but not dismissed until after the deadline expired" (*5*). These security tactics had the effect of minimizing casualties by forcing terrorists to choose more remote targets as it became more difficult to successfully execute attacks intended to generate casualties.

France also has a lengthy history of terrorist activity. During the period from 1970 to 1995, terrorists from various Middle Eastern countries carried out 22 attacks on French surface transportation systems (*5*). Algerian terrorists set off a bomb at the St. Michel train station in Paris in July 1995. The blast killed 7 people and injured more than 80. The Régie Autonome des Transports Parisiens (RATP)—the agency that oversees Metro, bus, and tramway services in the metropolitan Paris area—had preparedness plans to deal with terrorism. Response and recovery happened quickly and effectively, with train service resuming within 12 hours. Immediately after the incident, the security force was increased by 3,000 agents, trash cans in all stations were sealed (to eliminate easy hiding places for bombs), and a series of exits and entrances were closed (*5*).

The RATP has also put into place physical barriers, alarm systems, and a more extensive CCTV network with sophisticated software that allows operators to bring up an image from any one of more than 4,000 cameras. Other security measures employed include a program designed to reduce fire hazards (through the installation of

fire doors and blinds, detection devices, ventilation shafts, and reversible fans), radio networks, and continued training and exercises (*5*). The post–St. Michel attack security tactics proved to be relatively effective. The terrorists began to choose target areas where the number of potential fatalities was lower. Although a second bomb was detonated at the entrance to a Metro station about 3 weeks after St. Michel, "a third bomb was found on the track of the high-speed train (TGV) that runs between Paris and Lyon, a less risky location for a bomber. After that, terrorists shifted their targets to outdoor markets, public restrooms, and a school" (*5*).

Tokyo: Terrorist Chemical Attack

In 1995, members of the Aum Shinrikyo cult, led by Shoko Asahara, carried out a notorious sarin (nerve) gas attack on the Tokyo subway system. The assault involved five attackers boarding at different stations. They each had two or three plastic bags filled with sarin that they then punctured with sharpened umbrellas to start the release and vaporization process. Although the terrorists were relatively incompetent in executing the terrorist plan (bags were not punctured properly and some perpetrators inhaled sarin fumes), 12 people were killed, with over 3,000 more becoming ill. Had the nerve gas been less impure and more lethal, the number of deaths would probably have been considerably higher. The number of people exposed, however, would have been lower because passengers likely would not have continued to board trains—as was the case with this attack—if there were corpses (rather than ill people) on arriving cars (*3*).

Although emergency crews responded quickly, it was initially unclear to rescuers that they were dealing with a chemical attack, and many became ill upon entering underground stations. In fact, the attacks took place around 8:00 a.m. (peak hour), but it was not until 10:30 a.m. that officials actually identified the cause of the incident as sarin gas (*3*). Police recovered the plastic bags and started decontamination procedures by the early afternoon. The subway system was running again later that day. Ten thousand police officers were deployed "to increase security at and around locations where crowds gathered, including subway stations, major shopping areas near train stations and government buildings, and sports arenas" (*3*). Police immediately searched the offices, facilities, and headquarters of the group and by mid-April had taken more than 100 members into custody. Following the sarin gas attack, law enforcement officials had to contend with a series of attempted assassinations, hydrogen cyanide gas (used in Nazi concentration camps) attacks, and parcel bombings. Jenkins and Gersten credit the response of Japanese law enforcement in the aftermath of this attack—an aggressive crackdown on the suspected attackers—as one of the most effective security measures against this type of terrorist tactic (*3*).

The Tokyo incident pointed to several important lessons for future antiterrorism emergency planning. It appears that more police and CCTV cameras might have acted as a deterrent, but likely would not have prevented the attack (*3*). Response time is actually the most critical factor in dealing with chemical and biological attacks. Figures 6 and 7 show that the estimated number of fatalities rises considerably as response times to these attacks become longer ("no action" refers to the continued operation of the train system). In the case of a sarin gas attack, a response time of even 30 min will decrease the number of fatalities by almost 50%. The same response time for an anthrax attack will result in 75% fewer fatalities. Detection systems, more cameras, alarms, training, and better coordination between police and the military would have helped rescuers and transit agency officials identify the cause of the incident more quickly.

PREPARING SURFACE TRANSPORTATION SYSTEMS AGAINST TERRORIST ATTACKS

As the case studies show, the securing of a surface transportation system consists of several key components. Transit operators need to assess the vulnerabilities of systems, mitigate the weaknesses, and develop an effective overall security plan, including an emergency response plan.

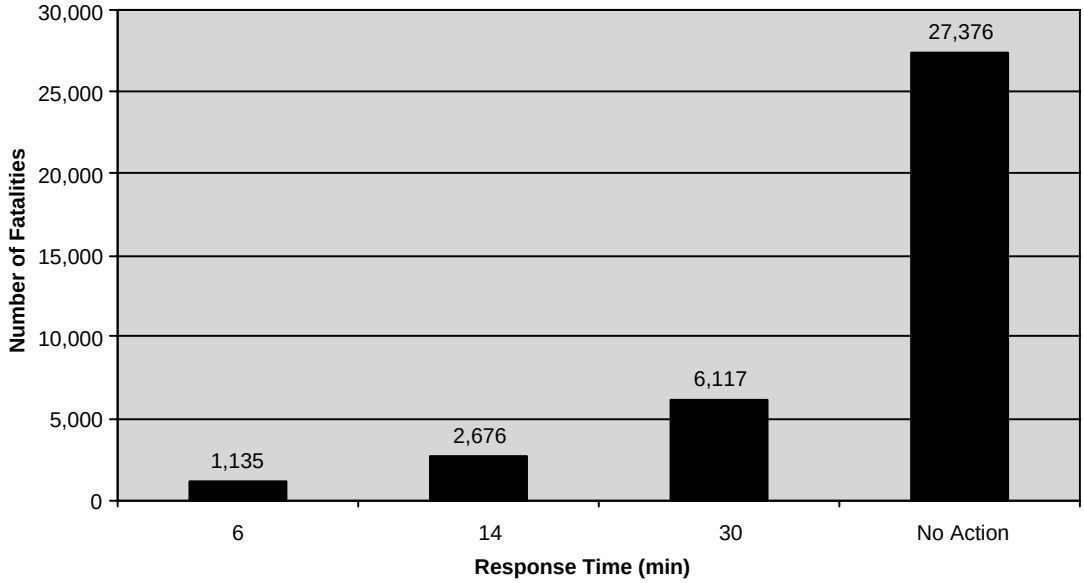

FIGURE 6 Fatality rates after an anthrax release on a subway system (*6*).

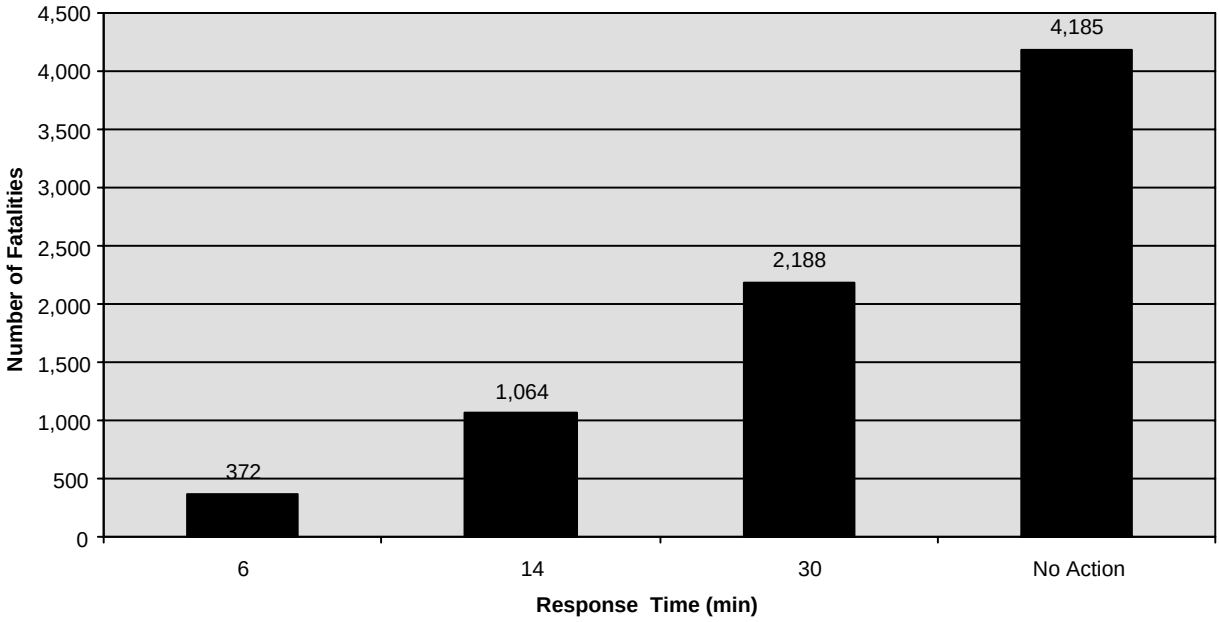

FIGURE 7 Fatality rates after a sarin gas release on a subway system (*6*).

Initiating the Terrorism Prevention and Mitigation Process

The initial step in developing a security strategy for any surface transportation system is to conduct a threat assessment and analysis. This assessment is "a comprehensive study of a system that involves identifying those components most vulnerable to disruption and assessing the likely impact of such disruption or destruction on passengers, employees, and the system" (*1*). It should also include an examination of the relationships between the vulnerabilities and impacts on the components of the transit system. Table 1 is an example of such an assessment conducted by the General Accounting Office (GAO) for a rail system. The assessment is useful in that it allows assessors to evaluate the security needs for the separate components of a larger transportation system. For example, an attack on a rail car has a high impact on people but a relatively low impact on the overall agency. The assessment can include a variety of other impact considerations, including the temporal and geographical nature of an incident.

The assessment should be done in conjunction with the establishment of an incident-command system outlining "procedures for incident notification, deployment of personnel to the scene, chain-

TABLE 1 Transit System Assessment of Risk and Vulnerability (*1*)

Transit Components	Criticality (Level of Impact) People	Agency	Vulnerability
Stations	High[a]	High[b]	High
Rail			
Track	Low	High[b]	High
Cars	High[b]	Low	High
Maintenance Yards	Low	Medium	Medium
Switching Stations	Low	Medium	Medium
Electric Power			
Source for Agency	Medium	High	Medium
Substations	Low	Medium	Medium
Command Control Center	Low[c]	High	Medium
Revenue Collection Facilities	Low	Medium	Low
Bridges, Aerial, and Tunnel Structures	Medium	Medium[b]	Medium
Fans, Vents, and Emergency Hatches	Low	Medium	Medium

[a] Depends on time of day incident occurs: greatest impact would be experienced during rush hours rather than off-peak periods.

[b] Depends on where incident occurs: an incident at a crossover or main junction would have greater impact than one at an outlying station or track segment.

[c] Affects employees only.

of-command and interagency relations and communication, triage and treatment of casualties, and improved agency recovery of operations" (*1*). It is also crucial for a transit agency to develop relationships with local, state, and federal law enforcement and security agencies to stay informed about potential terrorist threats and establish clear jurisdictional roles (*4*).

Addressing and Resolving Vulnerabilities

After conducting a risk assessment, an agency can begin to implement counterterrorism procedures and strategies. There are a variety of vehicle design, surveillance, detection, and security force tactics that can be utilized. The CPTED programs described earlier in the London case study involve specific design measures that help bolster security, including improving lighting, signage, and visibility; removing niches and corners; improving (or removing) restrooms; designing structures that control access and movement; and keeping floors, walls, and elevators clean. Many of these tactics were designed to address general crime and security issues, but they are extremely effective and necessary in antiterrorism campaigns as well (*4*). Deterrent measures such as alarms, CCTV systems, and an increased presence of security personnel are also useful active security-enhancing tactics. Table 2 outlines and summarizes some of these vulnerability-resolution techniques.

Security against chemical and biological attacks involves mitigation techniques that overlap with response and recovery measures. Subways are especially susceptible to chemical and biological attacks because of their closed-system design. The movement of trains through tunnels and stations as well as the heating, ventilating, and air conditioning systems facilitates the spread of agents (*6*). As discussed earlier, effective detection systems are central to establishing a defense against these terrorist tactics. Identification of the particular agent and containing it are the next steps in the process. Examples of containment and detoxification technologies include air curtains, aqueous foam, fume burners, high-temperature catalytic converters, wet scrubbers, carbon beds, and water sprays (*6*).

Developing Terrorism-Response and Emergency Plans

Transportation agencies should have detailed emergency action plans that establish procedures to be used when a situation deemed threatening occurs in or near a transit system. Some agencies address terrorism as part of the general emergency plan; others have specific plans that focus on terrorism. The plan should not just outline a chain of command during response to an incident. It should also describe specific actions, duties, and activities for all individuals involved in the crisis response, including

> train and bus operators, dispatchers, maintenance personnel, track/signal/engineering personnel, media staff, police and security officers, and safety personnel. Emergency procedures may address any of the following issues:
>
> - How to report an act of terrorism or extreme violence,
> - How to determine and evaluate the facts of the incident at the scene,
> - How to verify incident notification,
> - How to protect the scene of the incident,
> - How to properly ventilate the scene,
> - How to restrict trains from the scene,
> - How to remove and restore third-rail power, and
> - How to assist in rescue and evacuation operations. (*4*)

TABLE 2 Security Measures Used to Deter Terrorism (*4*)

General Category	Type of Measure	Particular Measure
Law Enforcement Activities	Police patrols (routine and special)	Uniformed (bicycles, carts, and motorcycles)
	Random and scheduled facility inspections	Plainclothes Canine
	Recommendations at design stage of construction or reconstruction of security enhancements	Officers trained in CPTED (Crime Prevention Through Environmental Design)
Physical Security Equipment	Closed circuit television (CCTV)	Constant monitoring; video recording; alarm-activated recording; monitored safety zones
	Intrusion-detection alarms	Electro-mechanical; microwave; ultrasonic
	Access control	Electronic access control systems; biometrics; employee badges; magnetic key cards; employee sign-in procedures; work order procedures; fences and gates; locks; vaults
	Communications	Radios; public address systems; emergency station and rail car phones; train annunciator systems; silent alarms
	X-ray equipment	Portable explosive detection equipment
	Blast-resistant containers	Specialized materials for trash can construction
	Vehicle barriers	Concrete barriers strategically placed to protect agency and access facilities
	Under-vehicle surveillance	Fixed devices that scan the underside of vehicles and can be used to check for bombs
	Gas-detection devices	Portable devices and agencywide installation
	Lighting	Halogen, fluorescent, infrared, and spotlights; lighting redundancy

Emergency preparedness experts also suggest that transit agencies have contingency plans available for such activities as assessing an incident and gathering evidence; conducting emergency field operations; and establishing operational sectors or zones (*4*).

As the case studies demonstrate, emergency preparedness training is crucial in the successful execution of response plans. The 1997 TRB survey (*4*) indicates that about 40% of respondents felt their agency was very well prepared or well prepared for an attack. However, 17% did not consider themselves well prepared. In addition, half of the agencies had not ever conducted terrorism response drills. Training procedures may include orientation and education sessions, tabletop exercises, functional drills, and full-scale exercises. The goal of training is to streamline the response process and create an effective and integrated command, control, and intelligence structure (*4*).

COST CONSIDERATIONS AND COST-EFFECTIVENESS DETERMINATIONS

The security of a surface transportation system focuses on two primary priorities: minimizing the risk to patrons and restoring services quickly following an incident. Because the design and implementation of security measures tend to be very costly, the challenge for transit operators is to identify the most cost-effective counterterrorism tactics available. According to Jenkins, these decisions are complex and multilayered:

> Because terrorist threats are not easily quantifiable, it is difficult to determine the "right" level of security. Using cost–benefit analysis as the sole criterion to determine the level of security is not very helpful. The risk of death to any individual citizen from terrorism is miniscule, making it difficult to argue for any security measure on the grounds that it will save lives. The problem is exacerbated by the fact that the perceived burden of security is not determined by the number or capabilities of the potential attackers but by the size and number of targets. Since the threat of terrorism is murky and security measures are costly, it is hard to justify the expenditures before an attack. (*5*)

However, Siegrist and Lejeune's attempt to quantify the economic impact of a biological attack suggests that the costs of an incident could run into the hundreds of millions of dollars: "If one thousand workers in a building were exposed [to anthrax], the cost in terms of lost lives would be $395 million; lost output during clean up $13–20 million; cost of response $5 million; cost of clean up at least $1 million; and medical costs approximately $200 thousand. The number of people who could be exposed in a subway attack could greatly exceed 1,000 with potential total costs increasing commensurately" (*7*).

Transit officials must also contend with the frequent financial constraints around implementing terrorism security measures. During a 1996 symposium, *Terrorism in Surface Transportation*, Thomas Savage, New York City Transit's Chief Security Officer, acknowledged the funding difficulties and described the ways in which he was working to maximize resources: "The budget is a real problem in New York. I have a very limited budget to put in sophisticated security systems in existing facilities. Where I have more flexibility is in the capital budget. . . . Everything that we buy or build—whether it be a new subway car, a bus, or a new facility—reflects design effort from the beginning" (*8*). In addition to the use of environmental design tactics (such as CPTED strategies), many of the antiterrorism measures described earlier can also be incorporated into the existing general crime prevention and emergency planning programs of agencies to reduce costs and avoid the duplication of activities.

A publication entitled *A Guide to Highway Vulnerability Assessment* (*9*) is an example of a set of guidelines that transit personnel could adapt for use in developing security strategies for public transit systems. The guide includes a systematic set of exercises for conducting critical asset identification, vulnerability and consequence assessments, and countermeasure development for highway systems. In addition, the guide provides state department of transportation staff a means to inventory countermeasures and determine preliminary costs. By packaging the countermeasures, assessors can determine the sets of countermeasures that "make sense operationally and from a vulnerability reduction perspective. In some cases, a single measure will apply to multiple assets . . . ; in others, multiple countermeasures will be applied to a single asset" (*9*). Subsequent steps involve estimating capital investment, annual operating, and annual maintenance costs (e.g., low, medium, high) and matching these criteria with countermeasure functions (e.g., deter, detect, defend). Agency personnel can then group the countermeasures to calculate approximate unit costs; these costs estimations can guide the development of appropriate and effective investment strategies and decisions.

A review of available security measures suggests that the following strategies are cost-effective, relatively easy to implement, and often part of larger crime and security strategies (*1*, *3*–*5*):

- Upgrading and expansion of CCTV systems (this technology is less expensive than personnel expenditures);
- Use of enhanced radio and communications systems;
- Incorporation of environmental design elements and features into new structures and trains;
- Implementation of regular training and exercises, including drills, tabletop exercises, no-notice responses, and full-scale simulations for regular and security staff (a generally low-cost option);
- Establishment of close relationships with local, state, and federal law enforcement to monitor and assess potential threats; and
- Development of a unified command system with coordination between transit and other integral agencies.

Because the threat of chemical and biological attacks is increasing, the installation of fast, accurate biological and chemical detection systems is becoming increasingly important. Much of the technology is still being developed and enhanced; the associated costs remain unclear.

POST-9/11 TRANSIT SECURITY ACTIONS, CHALLENGES, AND FUTURE RESEARCH

In December 2002, GAO released a report entitled *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges* (*10*). Using interview and survey results, the report outlines the current challenges involved in securing transit systems as well as agency efforts to address safety and security needs. Many domestic transit agencies started to examine security issues more intensely after the sarin gas attack in Tokyo and other incidents, such as natural disasters. However, agency officials clearly focused more substantial attention on system security after 9/11. The GAO interviews and survey find that "many transit agencies in large and small urbanized areas have implemented new safety and security measures or

increased the frequency or intensity of existing activities" (*10*). These include a variety of tactics: vulnerability or security assessments; fast-track security improvements; immediate, inexpensive security improvements (e.g., the removal of bike lockers and trash cans and the locking of underground restrooms); an intensified security presence; increased emergency drills; revised emergency plans; and additional training (*10*).

In terms of challenges, the GAO report finds that funding issues remain a primary difficulty for transit agencies in securing their systems: 44% of survey respondents indicated that insufficient funding is the most significant challenge to securing their transit systems, and 64% said that it had limited their ability to fully address security issues identified during vulnerability assessments (*10*). The findings point to several specific factors that contribute to funding as a challenge, including the high cost of security measures; budget constraints and overall decreases in transit revenue; the balancing of agency priorities (capital and operating versus security improvements); and federal limitations on using urbanized area formula funds for security purposes (*10*). In addition, the report indicates that transit agencies are facing challenges in coordinating their emergency planning and response activities with various governmental entities. Most agency respondents (77%) reported working with local governments, and 65% said that they felt adequately integrated into the emergency plans of their local governments. However, some respondents did identify factors that made local coordination a difficulty such as insufficient funding, limited awareness of terrorist threats, and a lack of time to coordinate (*10*). A majority also stated that they had not directly coordinated with regional, state, and federal agencies.

The securing of any surface transportation system is an ongoing process that draws on a variety of sources and constantly changing information. Collectively, Boyd and Sullivan (*4*) and Policastro and Gordon (*6*) find that the following topics and issues require further research:

- Improvement of the information flow between local transit authorities and federal intelligence and law enforcement agencies (most notably the Transportation Security Administration, the Department of Homeland Security as a whole, and the FBI);
- Development of a national transit terrorism warning system to alert agencies to critical threats (similar to the systems used by the FAA);
- Creation of regional transit terrorism working groups that allow agencies and personnel from various jurisdictions to exchange and maximize resources;
- Development of modeling and training software, including computer-based decision support tools and virtual reality simulation exercises; and
- Development of more sophisticated surveillance and chemical and biological detection systems that utilize artificial intelligence, sensing, and video technology.

Furthermore, transit agencies would benefit from future research that acknowledges and addresses funding concerns and constraints at the local level. This issue suggests two different sets of policy and research questions. First, how can agencies acquire more funds for the purchase, installation, and maintenance of new technology? In other words, researchers and policy makers should examine those institutional changes, particularly at the federal level, that will result in more effective fund allocation processes. Second, how can agencies identify the cost-effective, long-term strategies most appropriate for their particular transit environments and needs?

CONCLUSIONS

The events of 9/11 thrust the issue of transportation security to the forefront of public policy and media affairs as well as the public conscience. Although the focus has remained largely on commercial aviation, surface transportation systems are especially vulnerable to any of a number of terrorist tactics. Case studies of terrorist attacks on subway systems in London, Paris, and Tokyo offer transit officials invaluable insight into the ways in which security measures and planning both succeed and fail. In the case of public transit, however, the issue of cost-effectiveness is inevitably a concern, and countermeasures must be assessed and adopted with these financial constraints in mind. The development of highway-vulnerability assessment guidelines can be adapted to transit systems. These guidelines would allow transit personnel to weigh and balance the effectiveness of measures and their implementation, operation, and maintenance costs. While public transit systems face a unique set of challenges, a shift away from limited modal security perspectives to ones that incorporate and recognize the intermodality of contemporary transportation systems is likely to prove most beneficial.

REFERENCES

1. Boyd, A., and J. P. Sullivan. Emergency Preparedness for Transit Terrorism. *TR News*, No. 208, May–June 2000, pp. 12–17, 41.
2. Jenkins, B. M. *Protecting Surface Transportation Against Terrorism and Serious Crime: An Executive Overview.* MTI Report 01-14. Norman Y. Mineta International Institute for Surface Transportation Policy Studies, San Jose, Calif., 2001.
3. Jenkins, B. M., and L. N. Gersten. *Protecting Public Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices.* MTI Report 01-07. Norman Y. Mineta International Institute for Surface Transportation Policy Studies, San Jose, Calif., 2001.
4. Boyd, A., and J. P. Sullivan. *TCRP Synthesis 27: Emergency Preparedness for Transit Terrorism.* TRB, National Research Council, Washington, D.C., 1997.
5. Jenkins, B. M. *Protecting Surface Transportation Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks.* IISTPS Report 97-4. Norman Y. Mineta International Institute for Surface Transportation Policy Studies, San Jose, Calif., 1997.
6. Policastro, A. J., and S. P. Gordon. The Use of Technology in Preparing Subway Systems for Chemical/Biological Terrorism. *Proc., Commuter Rail/Rapid Transit Conference*, Toronto, Ontario, Canada, APTA, Washington, D.C., 1999.
7. Siegrist, D., and P. Lejeune. Defending Subways Against Biological Terrorism. *Transit Policing*, Vol. 8, No. 2, Fall 1998.
8. *Terrorism in Surface Transportation: A Symposium.* HSTPS Report 96-1. Norman Y. Mineta International Institute for Surface Transportation Policy Studies, San Jose, Calif., 1996.
9. Smith, M. C., S. Rowshan, S. J. Krill, Jr., J. E. Seplow, and W. C. Sauntry. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection.* NCHRP Project 20-07/Task 151B. Science Applications International Corporation, Vienna, Va.; AASHTO, Washington, D.C., May 2002.
10. *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges.* GAO-03-263. U.S. General Accounting Office, Dec. 2002.