PB2002-105914

MTI Report 01-14

Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview

October 2001

Brian Michael Jenkins

a publication of the
The Mineta Transportation Institute
College of Business
San José State University
San Jose, CA 95192-0219
Created by Congress in 1991

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA/CA/OR-2001-29		

4. Title and Subtitle	5. Report Date
Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview	October 2001
	6. Performing Organization Code
7. Authors Brian Michael Jenkins	8. Performing Organization Report No. 01-14
9. Performing Organization Name and Address Mineta Transportation Institute College of Business—BT500 San José State University San Jose, CA 95192-0219	10. Work Unit No. 11. Contract or Grant No. 65W136
12. Sponsoring Agency Name and Address California Department of Transportation Sacramento, CA 95819 U.S. Department of Transportation Research and Special Programs Administration 400 7th Street, SW Washington, DC 20590-0001	13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code

15. Supplementary Notes

This research project was financially sponsored by the U.S. Department of Tranportation's Research and Special Programs Administration and by the California Department of Transportation (Caltrans).

16. Abstract

Recent global events make it clear that the threat of terrorism is one to be taken seriously. For those who are attempting to kill in quantity and kill indiscriminately, surface transportation offers the ideal target. Because of the public nature of mass transit, there is often little security with no checkpoints as is the case with airports.

The practice of terrorism has moved in varying directions in recent years, depending upon different forms of transportation systems and venues of operation. Assaults on public surface transportation systems have continued to take place worldwide without any indications of abatement.

This executive overview summarizes three previous MTI documents: 96-1, *Terrorism in Surface Transportation-A Symposium* (March 1996); 97-4, *Protecting Public Surface Transportation and Patrons From Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks* (December 1997); and 01-07 *Protecting Public Surface Transportation Against Terrorism and Seriouis Crime: Continuing Research on Best Security Practices* (September 2001). It concluded with a checklist for use by transportation system operators.

NTIS is authorized to reproduce and sell this report. Permission for further reproduction must be obtained from the copyright owner.

REPRODUCED BY: NTIS
U.S. Department of Commerce
National Technical Information Service
Springfield, Virginia 22161

PROTECTED UNDER INTERNATIONAL COPYRIGHT
ALL RIGHTS RESERVED
NATIONAL TECHNICAL INFORMATION SERVICE
U.S. DEPARTMENT OF COMMERCE

17. Key Words	18. Distribution Statement
Buses; Public transportation; Safety; Terrorism; Violence	No restrictions. This document is available to the public through the National Technical Information Service, Springfield, VA 22161

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	40	$15.00

Form DOT F 1700.7 (8-72)

Reproduced from best available copy.

TABLE OF CONTENTS

EXECUTIVE OVERVIEW **1**
SCOPE OF THE RESEARCH 2
PATTERNS AND TRENDS IN TERRORIST ATTACKS 5
SECURITY AGAINST TERRORISM 7
Pre-Incident Preparedness: A Comprehensive Security Plan 9
Threat Assessment and Analysis 9
Station and Vehicle Design 10
The Security Force 14
Security Technology 17
Communications 19
Response and Recovery 20
Crisis Management Plans 20
Alert Levels with Predetermined Security Measures 20
Emergency Response Teams 22
Emergency Services 22
Exercises 23
Assistance for Victims and Their Families 23

ACRONYMS AND ABBREVIATIONS **25**

A. BEST PRACTICES CHECKLIST **A-1**
PLANS A-1
INTELLIGENCE AND THREAT ANALYSIS A-1
STATION AND TERMINAL DESIGN A-1
VEHICLE DESIGN A-2
PHYSICAL BARRIERS A-2
ACCESS CONTROL AND INTRUSION DETECTON A-2
CCTV COVERAGE AND CAPABILITIES A-2
TRACK AND SIGNAL MONITORING A-3
CHEMICAL AND BIOLOGICAL DEFENSE A-3
COMMAND CENTERS A-3
CAD LAYOUTS AND GPS LOCATORS A-3
SECURITY ORGANIZATION A-4
AUGMENTED SECURITY A-4
COMMUNICATIONS EQUIPMENT AND PROCEDURES A-4
PUBLIC COMMUNICATIONS A-4
TRAINING A-5
ADDITIONAL GUIDANCE A-5

CRISIS MANAGEMENT A-5
EXERCISES A-5
BOMB THREATS A-5
LEFT ITEMS AND SUSPICIOUS OBJECTS A-6
CARING FOR VICTIMS AND FAMILIES A-6
OTHER POST-INCIDENT ISSUES A-6

B. FIGURES 1 AND 2 . . . . . B-1

EXECUTIVE OVERVIEW

By Brian Michael Jenkins

Contemporary terrorists have made public transportation a new theater of operations. Algerian extremists set off bombs on the subways of Paris in 1995 and 1996; the Irish Republican Army has waged a long-running terrorist campaign against both passenger trains in England and London's subways; Palestinian terrorists have carried out suicide bombings on Israel's buses; an individual or a group calling itself "Sons of the Gestapo" derailed a passenger train in Arizona in 1995. Islamic extremists planned to set off truck bombs in New York's tunnels and bridges in 1993, and in 1997, they plotted suicide bombings in New York's subways. The nerve gas attack on Tokyo's subways by members of the Aum Shinrikyo sect in 1995 raised the specter that terrorists in the future might resort to weapons of mass destruction to which public transportation is uniquely vulnerable.

Recent events make it clear that the threat continues: 1998 saw an attempt to derail Japan's bullet train and a threatened poison gas attack on Moscow's subway. In 1999, a bomb injured three persons at a Sydney rail station. In 2000, bomb threats shut down London's Underground; one bomb injured nine in Dusseldorf's Underground; another bomb killed nine and injured 60 on the Metro in Manila.

For those determined to kill in quantity and willing to kill indiscriminately, public transportation is an ideal target. Precisely because it is public and used by millions of people daily, there is little security, with no obvious checkpoints like those at airports to inspect passengers and parcels.

Passengers are strangers, promising attackers anonymity and easy escape. Concentrations of people in contained environments are especially vulnerable to conventional explosives and unconventional weapons. Attacks on public transportation, the circulatory systems of urban environments, cause great disruption and alarm, which are the traditional goals of terrorism.

The United States has not experienced ongoing terrorist campaigns like those waged by the IRA in the United Kingdom or by various Palestinian extremist groups in Israel. Incidents here have been isolated and statistically rare although sometimes of great consequence, in particular, the terrorist bombings at the World Trade Center in 1993 and at the Oklahoma City federal building. A number of terrorist bombings have been thwarted by vigilant authorities.

These incidents, however, confirm that the terrorist threat in the United States is real, although there is no consensus on the nature and magnitude of that threat.

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 inadequate. The risk of death to any individual citizen from terrorism in any venue is minuscule, making it difficult to argue for any security measure solely on the grounds that it will save lives. The problem is exacerbated by the fact that *the costs of security are not determined solely by the number or capabilities of the potential attackers; they also are determined by the size and number of targets to be defended.*

Surface transportation cannot be protected in the way we protect commercial aviation. Trains and buses must remain readily accessible, convenient, and inexpensive. Passenger profiling, the elaborate deployment of metal detectors, X-ray machines, explosives sniffers, hand searches, and armed guards, which have become features of the landscape at airports, cannot be transferred easily to subway stations or bus stops. The delays would be enormous, the costs prohibitive. Rail lines, like power lines or pipelines, are extremely difficult to protect.

This does not mean, however, that nothing can be done. Transportation operators and security officials in areas that have been subjected to terrorist attacks have developed some effective security countermeasures. Although they cannot entirely prevent terrorist attacks—*no security system can stop terrorists from setting off bombs in public places*—good security measures can make terrorist operations more difficult, increase the terrorists' likelihood of being detected and identified, keep casualties and disruptions to a minimum, reduce panic, and reassure alarmed passengers in a crisis.

SCOPE OF THE RESEARCH

In order to meet the threat posed by terrorism and other forms of violent crime effectively, it is essential that transportation system operators have a thorough understanding of the security measures employed by other operators, especially by those transportation entities that confront high levels of threat.

Since 1996, the Mineta Transportation Institute (MTI) has supported a continuing research program aimed at identifying the "best practices" for protecting public surface transportation—facilities, equipment, and

passengers—against terrorist attacks and other major violent crimes. This research has been supported by the United States Department of Transportation, Caltrans, and the Mineta Transportation Institute's own funds.

The effort began with a symposium held in 1996 that brought together security experts from transportation entities, law enforcement, and other government agencies. The results of their discussions were published by MTI in *Terrorism in Transportation–A Symposium* (San Jose: Norman Y. Mineta International Institute for Surface Transportation Policy Studies, March 1996). For convenience, this report will be referred to in the text as Volume I.

The following year, MTI launched a more formal research program aimed at identifying the best security practices. The first phase of this effort included four case studies that reviewed transportation security measures in Paris, Atlanta, New York, and on the Amtrak rail system. The Paris case study focused on the immediate aftermath of the 1995 terrorist bombing at the St. Michel Station. Further terrorist bombings occurred in France in the fall of 1995 and again in December 1996, obliging authorities to increase security. The Atlanta case study focused on the security preparations connected with the 1996 Olympics and the aftermath of the Centennial Park bombing, although this bombing was not directed against public transportation. The Amtrak case study focused on the response to the deliberate derailing of the Sunset Limited in Arizona in November 1995. New York was included because of the size and complexity of its transportation systems and the various incidents and threats that have affected it, including the 1993 World Trade Center bombing, the subsequent plot to blow up bridges and tunnels, and the 1996 explosion at the Battery Park subway station. As these case studies were being completed, police in 1997 discovered a terrorist plot to carry out suicide bombings on the New York City subways.

All the case studies were conducted with the full cooperation of the operating entity and are based on reviews of plans and after-action reports, interviews with company officials and public authorities, and media accounts of the events.

During this phase of the research, an additional task was performed. The Federal Transportation Agency (FTA) previously had examined security practices at nine public transportation systems in the United States. The systems included multimodal transportation systems, medium-sized and large bus systems, and small and rural bus systems. The FTA reviews were based not on case studies but on surveys, and they did not focus exclusively on terrorism

but included a broader spectrum of crimes against property (that is, objects thrown at vehicles, arson, and hate crimes), crimes against persons (assaults on passengers, attacks on operators or drivers, weapons offenses, and homicides), and dramatic impact crimes such as bomb threats and terrorism. This material was reformatted and included so that it could be compared more easily with the four case studies.

In addition to preparing the case studies, the author compiled a chronology of terrorist attacks and major criminal assaults on surface transportation and added an annotated bibliography of publications dealing with surface transportation security. The results were published by MTI in *Protecting Surface Transportation Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks* by Brian Michael Jenkins and Dr. Larry Gerston (San Jose: Norman Y. Mineta International Institute for Surface Transportation Policy Studies, December 1997). In the text, this report will be referred to as Volume II.

Further research added four more case studies, updated the chronology through 2000, and expanded the annotated bibliography. The new case studies included the United Kingdom's response to the IRA's long-running terrorist campaign against mainland surface transportation; the 1995 sarin attack on Tokyo's subways, the first large-scale terrorist use of a chemical weapon, which provoked growing concern elsewhere; and security at the Bay Area Rapid Transit District (BART) and the Santa Clara Valley Transit Authority (VTA). Results of this research were reported in *Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices* by Brian Michael Jenkins and Dr. Larry Gerston (San Jose: Mineta Transportation Institute, 2001). This will be referred to in the text as Volume III.

Taken together, the three volumes present a comprehensive review of surface transportation security covering fourteen transportation systems in the United States and three systems abroad. They offer an opportunity to examine how operators of different systems—subways, commuter rail, and intercity and city buses—have dealt with different kinds of threats, from ordinary crime to isolated sabotage to long-term bombing campaigns to chemical attacks.

The effort will now focus on distilling the lessons learned from these experiences and cataloging the best security practices. This executive summary identifies these lessons and practices. Future workshops and symposia will

offer opportunities for system operators and authorities charged with security responsibilities to discuss them in greater depth.

PATTERNS AND TRENDS IN TERRORIST ATTACKS

Only by understanding the threat can we develop effective security measures. Although the United States has been largely spared the kinds of terrorist campaigns waged against public surface transportation in the United Kingdom, France, Japan, and less-developed countries, the unfortunately rich history of violence elsewhere can be used to better understand terrorist tactics, targets, and techniques.

Volumes II and III contain a chronology of approximately 900 terrorist attacks and other significant criminal incidents involving public surface transportation systems. The chronology runs from 1920 to 2000; however, all but 14 of the events listed occurred after 1970, the year that marks the beginning of modern terrorism.

Despite efforts to include all significant incidents, the chronology should be considered representative rather than comprehensive. Thousands of incidents of ordinary crime, such as individual murders, rapes, armed robberies, and other assaults, are not included. Nor does the chronology report all the many bomb threats that are a common headache for transportation system operators. The chronology includes guerrilla and terrorist attacks in which a transportation system or its passengers were the principal target. It excludes acts of open warfare, such as aerial bombing and artillery fire.

The chronology shows that contemporary terrorists view public surface transportation as a killing field. While roughly 20 percent of all incidents of international terrorism involve fatalities, the proportion of attacks on surface transportation systems involving fatalities is significantly higher. About two-thirds of the attacks on surface transportation have been intended to kill, and about 37 percent of the total involve fatalities.

A further indication of lethality is the percentage of incidents with multiple fatalities: 74 percent of the attacks with fatalities involve more than one fatality, and 23 percent involve 10 or more. Attacks are roughly evenly split between rail systems (trains, subways, stations, and rails) and bus systems (buses of all types and bus depots—see Appendix B, Figure 1).

Our count of bomb threats, although far from complete, indicates that bombings predominate as the most frequent mode of terrorist attack (see Appendix B, Figure 2). Overall, bombings account for 60 percent of all incidents; ambushes and armed assaults account for 11 percent; standoff attacks, 9 percent; hostage situations, 5 percent; and mechanical sabotage, 5 percent.

By definition, the chronology includes only attacks on public surface transportation, thereby excluding terrorist attacks involving other targets. However, in many instances, the chronology refers to ongoing conflicts, including civil wars, guerrilla wars, and terrorist campaigns. Often these combatants bring their violence to the capital cities to obtain international attention and to remind complacent populations that they will have no peace while wars rage in distant lands.

Of course, attacks on public transportation are only one facet of these conflicts. Under the circumstances, they are to be expected. The threat level is high. The violence is ferocious. Governments and transportation operators are obliged to take extraordinary measures that would be difficult to justify outside of the conflict zones.

Leaving out countries with ongoing armed conflicts would eliminate about two-thirds of the incidents and would provide a different picture of the threat. Bomb threats, acts of sabotage, extortion, individual assaults, and isolated crimes would predominate. There would be fewer fatalities. Individuals with personal motives and mentally deranged perpetrators would figure more prominently. The threat in these circumstances becomes less predictable, which, in turn, creates dilemmas for security planners.

Absent an ongoing armed conflict and without reliably precise and timely warnings from intelligence efforts, how do transportation providers and security planners protect against terrorism? How much security is enough? Is the answer to these questions the same everywhere? Should San Francisco's BART or a medium-sized bus company in rural America adopt the same measures as those used by London Transport?

Location does make a difference. This does not mean that a terrorist event cannot occur in a small or medium-sized city seemingly distant from national symbols, the political centers of power, and the more complicated social geography of our major cities—witness the Oklahoma City bombing—but it does mean that attacks in such areas are less likely. Historically, the United

States, although a comparatively violent country, has not suffered high levels of terrorist violence. Within the United States, six major metropolitan areas (New York, Miami, Washington, D.C., Chicago, San Francisco, and Los Angeles) account for a majority of the terrorist incidents, although owing to the magnitude of the event in Oklahoma City, not a majority of casualties.

SECURITY AGAINST TERRORISM

Threat assessment cannot be based solely upon perceived vulnerabilities, which are infinite, or hypothetical foes. At the same time, the absence of a specific threat cannot be an excuse for doing nothing at all. Security planners, therefore, should not consider the list of best practices in Appendix A as formulaic. It is a catalog from which planners can choose the best options for the location and nature of their specific transportation systems.

Cost is a legitimate criterion in designing security measures, and security budgets are limited. However, many of the security measures identified as best practices in the case studies have been found to contribute also to the efficiency of transport operations (vehicle locating systems, multimode communications), to passenger safety (design and materials used in station and coach construction), to making systems more convenient and attractive to passengers (good lighting, clean and well-kept interiors, up-to-the-minute information on system status, visible presence of staff), and to reducing ordinary crime (closed-circuit television [CCTV], high-profile and undercover patrolling). Those anti-terrorist security measures that have an obvious deterrent effect on criminal activity should be favored.

Many measures involve only modest expenditure. Improving liaison with local police and other emergency responders, establishing crisis management plans, conducting exercises, and putting in place procedures for handling bomb threats and left or suspicious objects are not costly undertakings. Technology that further reduces security operating costs also should be favored.

As mentioned previously, *physical security by itself does not prevent terrorism, but good security can displace the risk,* pushing terrorists toward still vulnerable but less lucrative targets where their actions are likely to cause fewer casualties. Terrorists will always find a vulnerable place to attack. They can attack anything, anywhere, anytime. We cannot protect everything, everywhere, all the time, which means that security often will necessarily be reactive. Security is increased after an attack to plug any gaps that the attack has made obvious, in anticipation of further possible similar attacks, and to

reassure an apprehensive public that something is being done. The added security measures may be suspended when the threat is reduced, although these measures are more easily increased than reduced—once in place, security measures have a tendency to become a permanent feature of the landscape. This, in turn, suggests that security measures should be flexible, capable of being increased or reduced in accordance with the perceived threat.

The following basic principles dictate the overall strategic approach to security for public surface transportation:

- Security has two major objectives: Preventing casualties is the paramount goal; reducing disruption in the form of unnecessary shutdowns is the secondary goal.
- Security cannot prevent terrorist attacks, but it can persuade terrorists (except those for whom escape or even their own survival does not matter) to choose less lucrative targets.
- Potential casualties can be reduced both through the design of stations and vehicles and through effective and rapid response.
- Disruptions can be minimized with technologies and procedures that permit prompt assessment, accurate diagnosis, and rapid, well-rehearsed responses.

Effective security, therefore, includes not only deterrent and preventive measures but all efforts to mitigate casualties, damage, and disruption. Since deterrence and prevention are difficult to achieve given the nature of terrorism and the inherent vulnerabilities of public transportation, great emphasis is placed upon the mitigation of casualties through design of facilities and upon effective, rapid response that ensures safety while minimizing disruption. Crisis management planning is essential. Constant training, including tabletop simulations and field exercises involving operating entities and local authorities, is essential to rapid response and successful crisis management.

The security topics listed here fall into two broad categories: (1) pre-incident preparedness, including threat assessment, security in station and vehicle design, security personnel, security technology, and communications; and (2) response and recovery, including crisis management planning, procedures for dealing with bomb threats and suspicious objects, emergency response teams, frequent exercises, dealing with victims and their families, and reassuring apprehensive passengers.

Pre-Incident Preparedness: A Comprehensive Security Plan

Most transport operators have plans for dealing with service interruptions caused by natural disasters, bad weather, accidents, or other incidents, including serious crimes or acts of terrorism. These plans usually emphasize minimizing disruption and maintaining service. Security issues often are scattered among these plans or are addressed in separate documents that deal with specific issues such as bomb threat response procedures. Operators may or may not have a separate formal crisis management plan.

All transport operators should have an overall security plan or manual that addresses organization and responsibilities, facilities and procedures, preparation and response. This plan should be prepared in cooperation with local authorities (that is, police and emergency responders), consistent with best practices, approved by management, used as the basis for testing and exercises, and regularly reviewed and updated.

Threat Assessment and Analysis

Almost all the information that transport operators receive about terrorism comes from government authorities. In the United States, the federal government will continue to be the principal source of information about terrorist threats, although larger local police departments with intelligence units may have additional information about threats in their locales. Many large U.S. cities have antiterrorist task forces that facilitate the flow of information and coordination between the FBI and local law enforcement agencies. Unlike the commercial aviation industry, where there is an established national structure for communicating terrorist threat information directly, surface transportation operators may be at the end of a long line to receive such information. The United Kingdom's system of communicating terrorist threat levels to the commercial sector is enviable. *To ensure their awareness of current terrorist threats, transportation operators should establish and maintain good formal and informal relations with both local police and federal officials.*

At the same time, transportation operators should not ignore their own sources of knowledge. Specialized chronologies like those in Volumes II and III and accounts of highly publicized attacks elsewhere in the world, which may inspire local copycats, should be examined. In addition to having external sources, operators are aware of local crime patterns that affect their systems and should have detailed knowledge of how ordinary criminals, thieves, and

vandals approach their facilities. British authorities discovered that IRA terrorists followed the same paths used by vandals and graffiti taggers to surreptitiously trespass on transportation property. Threat reviews should be conducted at regular intervals.

Uncertainty, however, is the reality of dealing with terrorism, and serious crimes like the mass shooting on the Long Island Railway by a mentally disturbed gunman or extortion against the transit system remain entirely unpredictable.

Every event that occurs must be closely analyzed to identify vulnerabilities and establish the adversaries' mode of attack. Identified gaps must be plugged, and responses must be improved. A single event may be the beginning of a campaign.

Station and Vehicle Design

When new stations are built or old ones remodeled, security should be a factor in the design. In the United Kingdom, architectural liaison officers—specially qualified police personnel with knowledge of blast effects on structure, cladding, glazing, fixtures, and street furniture, and an understanding of the principles of emergency evacuation routes and bomb security areas—advise local companies on security issues in design and construction. In France, the removal from rail stations of metal-framed wall signs and other extraneous items, along with combustible materials, reduced potential casualties from shrapnel, fire, and smoke inhalation.

Good station design includes emphasis on open space, including broad fields of vision, the absence of dark corners and other spaces where criminals might hide or terrorists could place bombs, good lighting, the effective deployment of CCTV, installation of fire doors and blinds, ventilation shafts with reversible fans to provide rapid smoke evacuation, emergency evacuation routes, and bomb security areas.

Fencing and Other Physical Barriers. Public surface transportation must have easy access, which limits the use of physical barriers. However, fences should be built around bus yards, around public parking areas adjacent to stations, and along surface tracks. Public parking areas also can be controlled by gates, CCTV cameras aimed at the drivers of vehicles, and cameras covering the entire parking area. Employee and visitor parking in bus yards should be controlled by permit. Power facilities and buildings or rooms

containing ventilation systems, electrical power connections and controls, communications systems, switching controls, computers, and other vital systems must remain locked, with access to them controlled and visually monitored.

Access Control and Alarm Systems. Access control and intrusion detection are areas of continuing rapid technological advance. Used in conjunction with physical barriers and CCTV, access control systems enable security personnel to monitor and protect vital systems (power facilities, control centers, computers, communications, air conditioning systems, etc.). We have not attempted to summarize this area in detail, as it is a major security topic with its own extensive literature.

Closed-Circuit Television (CCTV). Faced with serious terrorist threats, both French and British systems have made extensive use of CCTV to protect public transport. As of 1996, the Paris Metro and RER (commuter rail system) had installed 4,000 cameras to monitor entrances and stations, to enable drivers to check passengers, and to perform other security tasks, and more cameras were being installed. The French video system employs sophisticated hardware that combines the televised image with other types of data input and enables operators to instantly summon the image from any camera (see Volume II).

By the late 1990s, British authorities had installed 3,500 cameras to keep watch on the London Underground and rail transport; this number was being increased to 5,000. All station cameras can be called up on demand and are directly accessible by the police (see Volume III).

CCTV can be used to monitor activity, detect suspicious action, recognize individuals, and identify suspects beyond a reasonable doubt. Each of these tasks requires a progressively tighter focus and better image. Technology has advanced rapidly in this area, producing cameras with increasingly better resolution.

The mere presence of cameras probably contributes to deterrence, although CCTV surveillance in Tokyo's subway stations did not stop Japanese cult members, one of whom was caught on a station camera, from disseminating nerve gas. "Dummy" cameras are not recommended.

In locating cameras, transport operators should identify areas where passengers are most vulnerable and not immediately visible to staff; they should situate cameras so that they cannot easily be avoided, damaged, or obscured, and can

be moved or added to later; and they should consider eventually extending coverage to the surrounding areas. All passenger call boxes and help points should be covered by cameras.

Police should record the locations of the cameras in advance so that images from those cameras can be used to identify suspects and aid prosecutions.

Although CCTV has proved enormously effective in reducing crime and contributing to the deterrence of terrorism, authorities have found that a combination of CCTV coverage plus security patrols and prompt police response makes the greatest contribution to security.

The emplacement of cameras on vehicles is a recent development brought about by technological improvements. However, its effectiveness is limited by the availability of bandwidth for broadcasting images from a large number of vehicles. One solution would be to equip all vehicles with cameras (both visible and hidden) that are brought on air by a distress signal from the driver or an external command from the operations center. Another option would be to equip buses or train coaches on high-crime routes with hidden surveillance cameras temporarily.

Bomb Shelter Areas. In cases where time or specific circumstances do not permit evacuation out and away from the facility, people can be routed to a bomb shelter area. Bomb shelter areas are predetermined areas within a building or other facility that have been examined by a structural engineer and determined to provide protection against blast effects. These locations typically are surrounded by full-height masonry or concrete walls (but are not located in stairways or areas with access to elevator shafts that open to the ground level); are away from windows, external doors, and walls (flying glass is a major source of casualties in bomb blasts); and are away from the "perimeter structural bay." Bomb shelter areas also need access to communications to keep occupants updated.

Limiting Availability of Trash Containers as Receptacles for Explosive Devices. Because bombs are often left in trash containers, a great deal of attention has been devoted to this issue. *Removing trash cans entirely or sealing permanent receptacles, sometimes an emergency response following a bombing, are not useful long-term solutions* as they could lead to piles of rubbish, which, in turn, could provide suitable places for concealing explosive devices and make bomb searches even more difficult.

All trash containers should be monitored for use to identify and remove those that are not absolutely necessary. Those remaining should be located in prominent, well-lit areas within view of CCTV systems and away from sources of secondary fragmentation such as windows, mirrors, or overhead glass. Trash containers should not be located adjacent to obvious terrorist targets such as police stations, post offices, or banks.

A number of blast-resistant trash containers now are commercially available. Transparent trash-can liners provide a clear view of their contents.

Emergency Evacuation Routes. *Emergency evacuation routes should be preplanned to provide the safest means of egress in a variety of emergency situations.* For new facilities, this issue should be addressed in the design phase. Evacuation routes should take people away from the point of danger (for example, a suspicious object, a source of mysterious fumes) to a safe location at a distance from the facility. The location of the safe area will depend on the nature of the threat. For example, passengers evacuating from subways in response to chemical or biological threats or attacks should not be allowed to loiter on sidewalk ventilation grates above the stations and tunnels. Evacuation routes should not clog the access routes of emergency responders trying to get to the scene (these access routes should be designated in advance). Alternate routes to bomb shelter areas, to be used when exit is not possible, should be included in the evacuation plan.

Underground stations and subways in tunnels are the most difficult environments to evacuate. The routes should be broad enough to accommodate a surge of people (for example, no narrow staircases) and should contain no obvious choke points (for example, elevators) where impatience and alarm may lead to panic and casualties. Evacuation routes should be able to accommodate stretchers and should be designated clearly by signage as well as easily discerned identifiers, such as lighted colored arrows that can be switched on in an emergency.

Design of Coaches and Buses. Safety reinforces security in new vehicles, which are designed to withstand collisions and are constructed with materials that will not easily burn or will not produce toxic fumes if they do burn. Specific antiterrorist measures include the reduction of shrapnel-producing interior fixtures, sealing areas below the seats to prevent easy concealment of explosive or chemical dispersal devices, and the installation of both covert and visible but protected CCTV cameras.

The Security Force

Most large public transportation systems have their own dedicated security force. This may be a proprietary private security force or a regular police department dedicated to the transit authority, such as the Metropolitan Transportation Authority (MTA) Police Department or Port Authority Police in New York. Some larger urban police departments may have a dedicated transit police division. Operators of smaller transport entities are more dependent on regular local police, who may or may not have specific responsibilities and training for responding to incidents involving transportation systems. Proprietary security forces and dedicated police forces generally deal with routine patrolling and ordinary street crime. Major security challenges, such as the Olympics or a continuing terrorist campaign, require cooperation and augmentation from several police departments. While self-reliance is a desirable goal, reality often dictates that additional external resources are required. Jurisdictions also vary depending on the location and nature of the crime. Complexity is guaranteed. Coordination is required, and it is not easy.

Rail systems, especially underground rail systems, are special environments for which security personnel require special training. To work in these unfamiliar environments, regular police must be given detailed training and guidance or be accompanied by dedicated personnel (page 65 of Volume I). The United Kingdom, although it fields a transport police force of 2,000, has tried to improve overall awareness, training, and response capabilities at the local level by designated Counter Terrorist Crime Prevention Officers (CTCPOs) in each police department. CTCPOs receive special training and provide guidance to their private sector "clients." Absent a CTCPO equivalent, the same approach can be taken through less formal but still structured liaison arrangements created at the initiative of the transport operator.

There is no right number for the size of the security force. It will depend on the size and nature of the system, the organizational structure in place, and the level of threat.

Security requires the active participation of the transit entity's security personnel and civilian staff, special transit police in cities where they exist, local police, and the general public. Intercity transport may involve a number of local police jurisdictions. Procedures should be standardized as much as possible. This requires the dissemination of detailed guidance to all involved parties. In the United Kingdom, the National Terrorist Crime Prevention Unit (NTCPU) performs this task by analyzing terrorist and criminal threats and

providing police and transport operators with lessons learned, best practices, and detailed guidance on everything from trash bins to the proper emplacement of CCTV to dealing with bomb threats. No such entity exists in the United States, although a similar role could be assumed by the Department of Transportation working through one of its research institutes.

High Profile and Plainclothes Patrols. Many public transportation systems use a combination of highly visible and plainclothes patrols. Visible patrols provide an obvious deterrent and reassure passengers, while plainclothes patrols, their presence occasionally publicized through arrests, greatly increase uncertainty on the part of would-be adversaries. Plainclothes patrols are especially useful in high-crime areas or during outbreaks of crime; they will not stop a determined suicide bomber, but they will give pause to the adversary who wants to carry out his mission and escape.

The Role of Civilian Staff. All transport system staff members contribute to security, whether or not that is their primary responsibility. Just their visible presence adds to deterrence, and some transport operators have deliberately deployed civilian staff to make them more visible, which also reassures passengers. Employees are effective monitors of what is going on. They are often the first to notice left or suspicious objects. They will be best positioned to recognize and diagnose trouble. They are truly the first responders to any incident, and they are the most reliable communicators in the first moments of an incident. They are the shepherds who will lead passengers to safety and who will guide emergency responders to the problem, and they are the people who stand by to restore operations.

Because these roles are not explicit, civilian employees often are overlooked when it comes to training and equipment that would assist them in performing these vital tasks. Providing training does not mean altering the primary responsibilities of civilian staff members, but recognizing that a security role automatically comes with their presence on the scene. It also recognizes that they are often among the first casualties. When station personnel in Tokyo removed by hand the deadly sarin-leaking bags from the subway coaches, they were unaware that they were exposing themselves to illness and death in the process. Training in awareness, surveillance, response procedures, and self-protection is owed the civilian staff.

Training. Training programs vary depending on the configuration of the security force. Where security is provided by local police, officers undergo regular police academy training. They may or may not receive additional

special training to familiarize themselves with unique public transportation issues. Ideally, they will. Where security is provided by a transit police division or a separate transportation police department, regular police training is supplemented by special training.

Proprietary private security forces and contract security personnel rarely receive police training, and the quality of the security training they do receive varies greatly. Although civilian staff are relied on as a "first line of defense" and expected to apply psychological profiles and recognize and exercise judgment regarding suspicious packages, they rarely receive adequate formal training to do so. In addition to providing formal training, the British make extensive use of laminated cards containing basic instructions for operators and nonspecialist police officers who are confronted with bomb threats, suspicious objects, and other contingencies.

Management-level personnel who will be involved in on-scene response and crisis management should meet minimum training requirements through attending disaster management courses, in-house training, and regular exercises. Command team members should be fully educated on available local, state, and federal disaster response services and should know how to request them (pages 50-51 of Volume I).

Covert Testing. Faced with a continuing terrorist threat, British transport security authorities emphasize covert testing of security and response procedures to ensure that security personnel and civilian staff remain alert and are familiar with procedures. The U.S. Federal Aviation Administration also conducts increasingly realistic covert testing to ensure high standards of security at the nation's airports. *Covert testing followed by critiques should be an integral part of the security plan.*

Public Involvement in Security. There are pros and cons to encouraging public involvement in security. The fact that passengers are constantly being advised to be on the lookout for suspicious behavior increases the risks perceived by would-be attackers who imagine themselves to be under constant surveillance. Vigilant passengers often are the first to notify authorities of left items or suspicious objects. Repeated public warnings, however, may also frighten passengers, inspire hoaxes, and lead to numerous false alarms. Where the terrorist threat is remote, the potential adverse consequences may outweigh the benefits. However, where terrorist attacks have occurred and the threat level remains high, the risk of hoax threats and false alarms is already high. Israel, France, the United Kingdom, and other countries that have experienced

terrorist campaigns have sought public participation through signs and repeated public announcements reminding travelers to keep personal packages under their direct control, remain vigilant for left parcels, and immediately report suspicious activity or articles to staff. In the United Kingdom, police are confident that any such parcels will be discovered within a few minutes, far less time than terrorist bombers normally allow when they set their timers to permit them to escape. The objective is to move the bombers toward less-frequented areas where, if a bomb did explode, it would likely cause fewer casualties. Public announcements also warn people not to touch suspicious objects. *Public vigilance plus rapid response can reduce the risk of casualties and disruption.* Involving passengers in their own security also has the psychological effect of reducing anxiety by transforming passengers from seeing themselves exclusively as helpless victims to seeing themselves as contributing to their own security.

Security Technology

Computerized System Layout. New York Transit has developed a computerized database capable of depicting the rail track network, with corresponding street grid, emergency exits, access points, and ventilation fans in selected sectors of the system. This enables the operations center to readily envision all options in a crisis situation. An emergency mobile command center equipped with a duplicate of the computerized layout can be dispatched to the scene.

Security System Integration. The installation of access control systems—alarmed doorways backed by thousands of cameras—increases the requirement for personnel to monitor them and presents a challenge for security systems integration. Advances are being made in automated problem recognition; for example, a breach of a secure zone automatically brings a camera to focus on the site of the breach and alerts a security official at the operations center. Fortunately, technology is moving fast in this area, offering cost-effective solutions.

Systems to Detect Chemical and Biological Agents. Government research on systems to detect and identify dangerous chemicals or harmful pathogens in the air is ongoing. While significant advances have been made and some devices currently are being used by the military, by hazardous materials teams, and by technical personnel in special circumstances, there is as yet no commercially viable technology that would allow reliable continuous monitoring of the air in large semi-enclosed areas such as train stations or

subway systems. Moreover, where potential victims cannot promptly don protective clothing and breathing apparatuses, the utility of warnings is diminished. Fire department hazardous material teams are able to deploy detectors when a chemical dispersal is suspected, however, and further development is anticipated in this area.

Protecting Signal Systems. Vandalism is a common problem in rail transportation. Authorities report more than 10,000 incidents a year nationwide. In 1994, there were approximately 3,000 incidents of signal vandalism, 154 of which resulted in derailments, although none involved passenger trains. Ensuring the integrity of signal systems requires both physical and electronic measures.

Track Monitoring. One of the most dangerous types of incidents is the deliberate derailing of a speeding passenger train, although the one recent derailing incident in the United States fortunately resulted in only one fatality. In most urban rail systems, the frequency of trains itself acts as a security measure. Where trains run with less frequency, opportunities for sabotage increase. Track security is maintained by using the track itself as a low-voltage electric circuit, with the rails as its conductor. When the current is interrupted or compromised, the system displays a red signal to the engineer. In the 1995 Amtrak derailment, however, the saboteur spliced a shunt wire around the dislocated rail section, thus bridging and preserving the circuit and allowing the signal to display green. This, of course, takes knowledge and time. Additional security for remote rail systems can be provided by regular patrols and frequent track inspection.

GPS Tracking of Vehicles. Most modern rail systems provide real-time information about the precise location of trains. GPS tracking technology has improved and has become cheaper, enabling operators to identify the exact location of specific buses or trains that may be experiencing a security problem. GPS may be used in conjunction with duress switches for drivers and on-board CCTV cameras that can be turned on remotely to provide authorities with a picture of what is taking place on board.

Individual Location Devices. Personnel on foot in tunnels can be equipped with locating devices that use the existing radio infrastructure. These devices can be integrated with a vehicle-locating system to provide a graphic display of the position of all security and response elements connected with the system. Such technology is currently employed in Paris by the Metro and RATP (Régie Autonome des Transports Parisiens) (see Volume II).

Passenger Screening. The passenger screening procedures in place at commercial airports are not feasible for public surface transportation. The number of surface transportation passengers is too great, there are too many points of access, and advance ticket purchase is not required. Attempting to have all passengers pass through metal detectors before entering train or subway stations or X-raying their parcels would create significant delays and impose huge costs. Public surface transportation would cease to be convenient. For buses, such measures would not work at all. However, this does not preclude deploying some X-ray or other bomb detection technology to conduct random security checks in extreme threat situations.

Communications

Multimodal communications are essential. Case studies show that communication breakdowns resulting from technical failures or inadequate procedures are a common problem. Explosions destroy hard lines. Radios do not work well in tunnels. Backups are required. In an ideal situation, all drivers and security staff have radios, although frequencies used by emergency responders differ from those used by transport operators. A common-frequency radio communications system should be set up in each local community, permitting transportation staff and emergency response organizations to share information and coordinate operators (page 53, Volume I). Inadequate procedures compound technical problems, and information received by one component (for example, bomb threats) may not be quickly relayed to response agencies.

Communications with passengers should include several modes. Electronic signs that routinely provide information about the time to arrival of the next train can be used to provide instructions during emergencies, supplementing public address systems. *Larger urban systems must also recognize the need for public announcements to be made in more than one language.*

Passengers should be able to communicate with operators through clearly indicated and readily accessible alarms, emergency telephones, and help points on trains and in stations that will immediately connect the caller with a security person or other staff member. Emergency call boxes should be under visible CCTV surveillance (a camera focused at the caller) both to help security officials assess the communicator and diagnose the situation and to discourage hoax reports.

Response and Recovery

Crisis Management Plans

Deterrence and prevention are difficult to achieve given the nature of terrorism and the inherent vulnerability of public surface transportation; in most cases, authorities will be responding to events that have occurred. The ability to respond rapidly and effectively, mitigate casualties and damage, reduce unnecessary disruption, deal with victims and their families and friends, and reassure a nervous public is critical. *Crisis management planning must be regarded as an essential component of the overall security plan.* Crisis management plans must include procedures for notification and activation of the crisis management team(s) and must indicate the roles and responsibilities of all those involved. The plans must address evacuation and shutdown procedures; dealing with victims, families, and relatives; liaison with local emergency responders; ensuring safety and security of passengers after the incident; restoring service or creating alternatives; issuing public information; and reassuring anxious passengers.

Alert Levels with Predetermined Security Measures

To ensure the consistency of security responses in heightened threat conditions, it is useful to identify in advance alert levels with predetermined security measures. This enables authorities to warn operators of threat situations without providing confidential details, and it allows operators to quickly adjust security measures to the perceived level of threat.

U.S. airports currently operate under such a system, with the Federal Aviation Administration informing airports and carriers of threat levels that then mandate corresponding security measures. British authorities have developed a similar system to assist rail operators and commercial centers to adjust their security according to four levels of threat.

Security Augmentation. A major terrorist incident or publicized threat will require that security be increased visibly to fill any obvious gaps, deter future attacks, and reassure the public. Mutual aid agreements should be negotiated in advance. After the first bomb attacks on its commuter rail and Metro systems, France reinforced security on the RER, Metros, and other potential targets with an additional 5,000 soldiers and gendarmes, a level beyond the capacity of most departments but a demonstration of how huge the workforce burden can become. Deployments of this magnitude in the United States would require

mobilization of the National Guard at the state level or federal assistance, actions that normally are seen only in large-scale civil disturbances but that are increasingly being considered in response to catastrophic terrorist incidents. Such augmentations would necessarily be of short duration. Their contribution to actual security is debatable. Additional security personnel contribute to deterrence, and nervous terrorists will move their attacks further out, away from the heavy security. Nevertheless, additional security cannot prevent determined attackers.

Responding to Bomb Threats. Bomb threats are by far the most common method used by terrorists and others seeking to cause alarm and disruption. Generally, terrorists do not begin a campaign with bomb threats, because they have no established credibility. However, the disruptive effects of actual terrorist bombings may be amplified subsequently with bomb threats, an IRA technique. Bombings also inspire hoax threats. Therefore, transport operators must have well-established protocols for dealing with bomb threats.

First, it is essential that the threat be relayed to the responsible persons, whether it initially is telephoned to the police, transportation company headquarters, switchboard operators, stationmasters, toll-free help lines, reservation centers, or any other number. Everyone should be trained to obtain as much information as possible from the caller and promptly forward it to the appropriate authorities. A bomb threat checklist can be found in Appendix C of Volume I. Some operators (for example, Amtrak) have instant recording devices at all locations where bomb threats may come in. This allows all calls to be captured and transmitted to the police. Second, a protocol for evaluating the threat is needed. Actions can range from watchful waiting to local searches to shutdowns and immediate evacuations. Evacuations will be rare. Authors of bomb threats are rarely bombers. Even during the height of the IRA's bombing campaign, fewer than 2 percent of the threats were considered serious, and evacuations or partial evacuations were ordered in response to fewer than 0.66 percent of the threats. Still, even when threats appear to be hoaxes, as almost all are, they cannot be ignored. A reasonable assessment must be made and appropriate action taken. The desire to avoid needless disruptions must be balanced against the threat to public safety. Guidelines based upon actual experience (and defensible in a court of law if things go wrong) are helpful in taking the pressure off local decision makers.

Handling of Unattended Items. Public transportation systems deal with thousands of items left unattended or left in stations and on trains and buses each year. These impose a tremendous burden on security. Although

unattended parcels are rarely linked to explosive devices, they all represent a potential threat, and during periods of high alert, they need to be examined systematically. To deal with the IRA's terrorist campaign, British authorities developed a standardized reporting form that records where the item was found, its contents, whether the parcel was X-rayed, and whether the bomb squad had been called. All left items are photographed.

The Tokyo and London case studies in Volume III underscore the importance of diagnosis in dealing with terrorist attacks. In the Tokyo case, the mysterious and unprecedented nature of the chemical attack prevented the prompt shutdown of the affected trains and immediate evacuation; contaminated coaches continued on their runs, causing more casualties. In the British case, close analysis of the patterns of the terrorists allowed security authorities to design more effective countermeasures.

Emergency Response Teams

Several of the public transportation operators examined in the case studies have some form of mobile response team that can respond rapidly to serious incidents that cause system disruption. These teams may comprise management personnel who remain at operations headquarters or deploy to the scene of a major incident and trained specialists who have specific responsibilities, specialized training, and equipment for responding to derailments, explosions, chemical incidents, etc. These operational personnel can get to the scene of the incident within minutes. Some operators also have teams with mobile tool sheds and rolling-stock-lifting teams, but their function is related to restoration of service. Having a mobile command center with proper communications equipment is a good idea. Despite the rapid reaction capability of operators' teams, they may be delayed by police and fire units that arrive on the scene first and put in place strict security cordons. This underscores the need for close coordination, recognizable badging, and joint exercises.

Emergency Services

The capabilities of the local emergency services—fire, rescue, hazardous materials, and medical services—are beyond the control of the transport operator whose own resources are likely to be extremely limited. Transport operators should be aware of the capabilities of the local services. Joint exercises should be conducted regularly to identify and remove any unnecessary obstacles to prompt, effective response. The World Trade Center

and Oklahoma City bombings, along with heightened concerns about the possibility of terrorist attacks involving chemical or biological substances, have prompted the U.S. federal government to devote increasing resources to improving the training and equipment of first responders.

Exercises

There are two ways to determine whether crisis response plans work. One is to wait for a real-life incident and hope for success, since the learning curve is very steep and mistakes can be fatal. The other is to conduct regular exercises, both tabletop crisis response games and field exercises, aimed at specific objectives, including testing response procedures, communication, and coordination. Problem areas can be identified and remedies applied without loss. The costs generally are modest, mainly consisting of time. A number of large operations, including New York's Metropolitan Transportation Authority (MTA), conduct such exercises regularly. Most plans, however, are never tested until actual episodes occur.

Assistance for Victims and Their Families

A terrorist attack is, above all, a human tragedy. People are injured, perhaps killed. The precise casualty count and the identities of the casualties and the dazed survivors may remain unclear for hours, or even days, creating agonizing uncertainty for relatives and friends. The problem is compounded in the case of surface transportation by the absence of passenger manifests. While rescue efforts focus on saving lives, investigators try to figure out what happened and gather evidence to determine who was responsible. Operators focus on clearing the wreckage and restoring operations.The task of dealing with victims and their families, as well as those who fear that a relative or a friend might be among those harmed, may be ignored or handled cavalierly. This lack of assistance is one of the biggest sources of complaint and criticism in air and surface transportation disasters.

Crisis management plans and exercises should address this issue directly. The biggest challenges are seeing to the immediate nonmedical needs of the survivors (assistance in communications, clothing, housing, counseling, etc.) and providing accurate and timely information about casualty numbers and identities. The National Transportation Safety Board (NTSB) has been given these responsibilities, but transportation operators must be prepared to participate actively. Crisis plans, therefore, should designate a manager who will be responsible for these tasks.

Working with the NTSB, transportation officials may establish an information center near the location of a disaster (but not where it could hamper rescue and investigative efforts) at which worried family members can seek assistance. Information also can be disseminated through toll-free numbers established for this purpose and through the news media.

The immediate needs of survivors should be promptly identified, and reasonable assistance should be offered. In large-scale disasters, transport staff may have to seek information aggressively from local hospitals regarding emergency admissions; NTSB support will help there. Providing prompt assistance to survivors and victim identification and location information to relatives will not save lives, but it will spare the operating entity some of the ugly criticisms that have come with inept handling of these tasks.

ACRONYMS AND ABBREVIATIONS

CAD	computer-aided design
CCTV	closed-circuit television
CTCPO	Counter Terrorist Crime Prevention Officer
FTA	Federal Transportation Agency
GPS	Global Positioning System
HVAC	heating, ventilation, air conditioning
IRA	Irish Republican Army
MTA	Metropolitan Transportation Authority
MTI	Mineta Transportation Institute
NTCPU	National Terrorist Crime Prevention Unit
NTSB	National Transportation Safety Board
RATP	Régie Autonome des Transports Parisiens
RER	Réseau Express Régional

APPENDIX A: BEST PRACTICES CHECKLIST

PLANS

- Comprehensive security plan
- Alert levels with predetermined security measures
- Emergency response plan
- Coordinated with local authorities
- Periodic review

INTELLIGENCE AND THREAT ANALYSIS

- Periodic meetings with local, state, and federal authorities
- Analysis of local crime patterns

STATION AND TERMINAL DESIGN

- Target hardening
- No highly combustible materials or sources of toxic fumes or shrapnel
- Reversible fans
- Open spaces
- Good visibility
- No hiding or hidden spaces
- Adequate emergency exits
- Designated evacuation routes
- Bomb-secure areas with communications
- Good lighting
- Effective CCTV coverage
- Easy to maintain and well-maintained
- Bomb-resistant, well-placed trash containers

VEHICLE DESIGN

- Crumple impact zones
- No highly combustible materials or sources of toxic fumes or shrapnel
- Modification of car seats to eliminate concealment space
- Visible or hidden CCTV coverage

PHYSICAL BARRIERS

- Fencing for perimeters of parking lots and structures
- Fencing for bus yards, maintenance depots, etc.
- Fencing for vital facilities (power, fuel, etc.)
- Fencing along track
- Locked doors at signal boxes, electric controls, etc.

ACCESS CONTROL AND INTRUSION DETECTON

- Headquarters and operations centers
- Power stations and fuel depots
- HVAC facilities
- Bus yards and depots
- Train yards and maintenance facilities
- Other vital facilities
- Integrated with CCTV

CCTV COVERAGE AND CAPABILITIES

- Stations
- Passenger call boxes and information points
- Entrances
- Parking lots and structures
- Surrounding areas
- Access-controlled doors

- On board vehicles
- Pan, tilt, zoom where appropriate
- Good quality image
- Record full-time or on command
- Date, time synchronized
- Integrated with access control and intrusion detection
- Can be transmitted directly to the police

TRACK AND SIGNAL MONITORING

- Automatic systems (electric current, validation)
- Patrols

CHEMICAL AND BIOLOGICAL DEFENSE

- Detectors in place
- Protective gear for security staff
- Breathing apparatuses available to station staff and drivers

COMMAND CENTERS

- Designated crisis management center and alternate
- Operations center
- Mobile command center

CAD LAYOUTS AND GPS LOCATORS

- CAD layout of system
- GPS on buses
- GPS on trains
- GPS for individual security staff (displaying position at operations center)

SECURITY ORGANIZATION

- Proprietary security
- Contracted security
- Dedicated police department
- Local police
- Police departments along routes
- Liaison with state and federal authorities
- Involvement of civilian staff
- Public involvement

AUGMENTED SECURITY

- Arrangements in place with local police
- K-9 units available

COMMUNICATIONS EQUIPMENT AND PROCEDURES

- Multimodal communications
- Dedicated landlines at track intervals
- Dedicated landlines at stations
- Direct lines to emergency services
- All security personnel have two-way radios
- All drivers have two-way radios
- Common frequency for communications with emergency services
- Cellular phone backup
- Plan talk to eliminate misleading jargon

PUBLIC COMMUNICATIONS

- Emergency phones for passengers indicating caller location
- Public address system
- Multilingual public announcements

TRAINING

- Propriety security
- Dedicated police department
- Local police
- Additional police jurisdictions along routes
- Managers and members of crisis management teams
- Civilian staff

ADDITIONAL GUIDANCE

- Laminated cards
- Liaison with designated officer in each jurisdiction

CRISIS MANAGEMENT

- Crisis management plan
- Designated crisis management team
- Designated emergency response team
- Crisis management manual indicating roles and responsibilities
- Public spokespersons designated and trained
- Regular exercises
- Lessons learned

EXERCISES

- Tabletop crisis management exercises
- Joint field exercises to test emergency response
- Covert testing of security

BOMB THREATS

- Staff trained
- Bomb threat checklists in place

- Ability to record calls
- Established protocol for threat assessment
- Search procedures
- Laminated cards

LEFT ITEMS AND SUSPICIOUS OBJECTS

- Public awareness
- Staff trained
- Established procedure
- Each item examined and recorded
- X-ray capability

CARING FOR VICTIMS AND FAMILIES

- Familiar with NTSB procedures
- Designated member of crisis team to cover assistance to victims and information for relatives
- Protocol to establish contact center at the scene of the incident

OTHER POST-INCIDENT ISSUES

- Public information plan to restore confidence
- Counseling for staff involved in disaster
- Review of lessons learned

APPENDIX B: FIGURES 1 AND 2

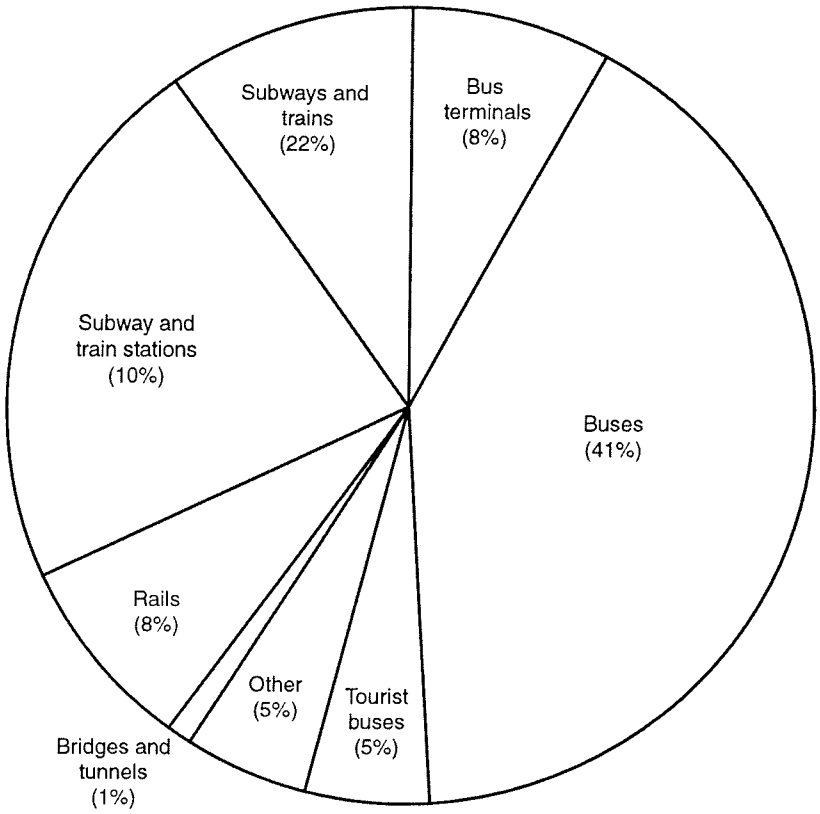

Figure 1. Targets of Attacks on Public Surface Transportation Systems (July 1997–December 2000)

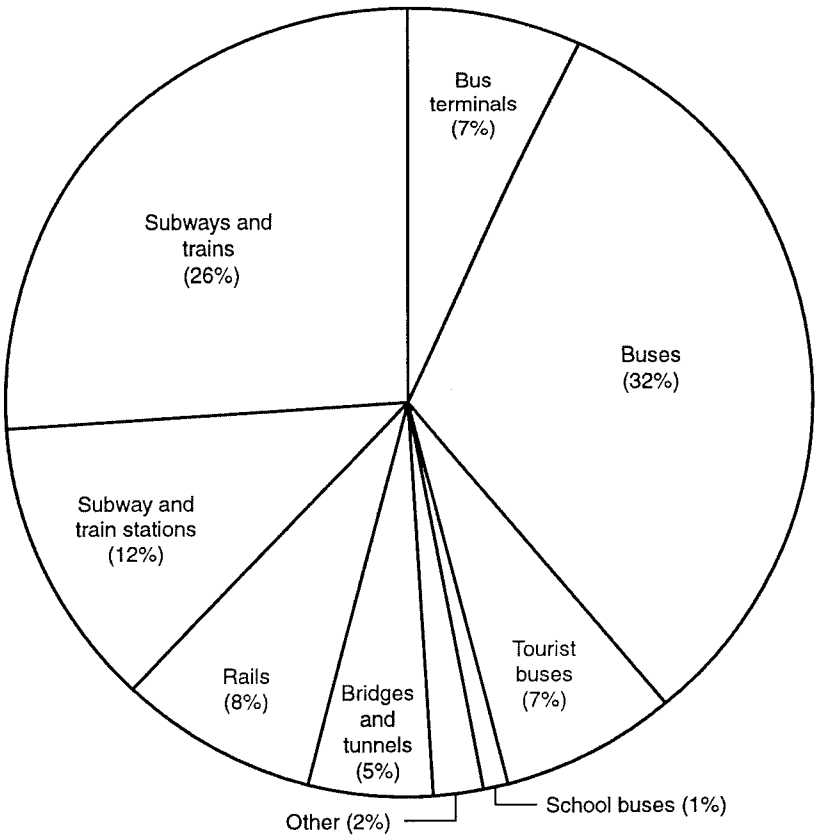

Figure 2. Targets of Attacks on Public Surface Transportation Systems (1920–2000)