

# **IMPROVING PUBLIC SURFACE TRANSPORTATION SECURITY: WHAT DO WE DO NOW?**

Brian Michael Jenkins

Like almost everything recently written on security, this essay takes September 11, 2001 as its starting point. On that date, the most lethal terrorist attack in history profoundly affected how Americans view security. However, the essay draws upon research that began much earlier. That research addressed the protection of surface transportation systems against terrorist attacks. It focused particularly on identifying the best security practices and by September 11 had already produced several reports. These were quickly summarized after the attacks on the World Trade Center and the Pentagon and were disseminated through various government-sponsored and industry association forums.<sup>1</sup>

While the essay specifically deals with surface transportation security, it also touches upon the broader issues of homeland security and national transportation strategy. It begins with a review of the threat and then discusses some of the broader aspects of implementing homeland security. Next, it reviews the progress made in improving surface transportation security and discusses remaining problems. It then examines ways to approach the problem (and ways not to). A final section summarizes the conclusions.

## **The Threat**

The terrorist threat to surface transportation is real: contemporary terrorists have made it a major theater of operations. Initially, the primary terrorist targets were commercial airliners, which were widely available symbols of nations and policies despised by the terrorists, and also portable containers of victims or hostages, as well as sometimes being a means of escape. But as aviation security improved, the total number of attacks on commercial aircraft declined, and terrorists increasingly turned to attacks on surface transportation: bombing trains, stations, depots and buses. A softer target than aviation, surface transportation offers terrorists easy access and little security to penetrate. In addition, the large crowds of strangers at surface transportation facilities guarantee anonymity for the attackers and facilitate their escape.

Transportation systems are the nervous systems of large cities. Attacking them produces profound psychological effects and economic disruption. Concentrations of people in contained environments also enhance the effects of explosives and chemical weapons and offer venues for the spread of biological agents – all attractions to terrorists who are determined to kill in quantity and willing to do so indiscriminately.

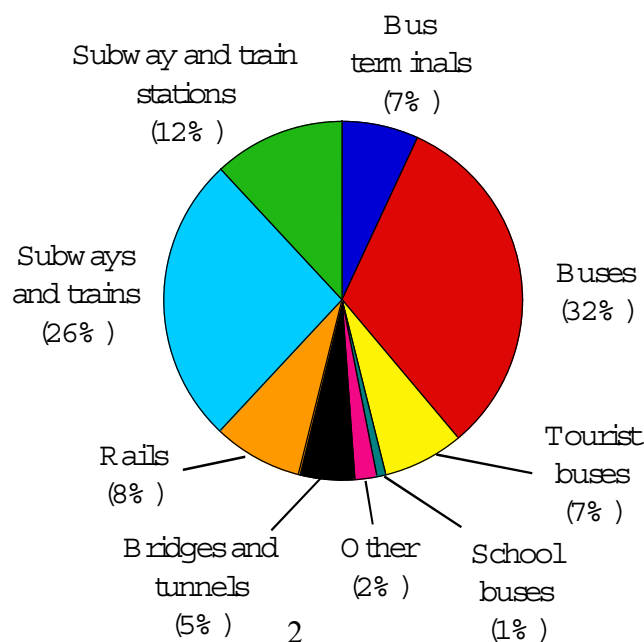
Clearly, killing is the objective of many terrorists who attack surface transportation targets. Such attacks have been almost twice as lethal as terrorist attacks overall. An analysis of nearly 1,000 attacks on surface transportation revealed that two-thirds were intended to kill and 37 percent resulted in fatalities. The goal was often slaughter: 74 percent of the fatal attacks involved multiple fatalities and 23 percent involved ten or more deaths.<sup>2</sup> To be sure, many of these attacks occurred in the midst of ongoing civil wars, but a third of them took place outside of identified conflict zones.

Although many of the attacks are isolated incidents, major terrorist campaigns have targeted surface transportation. The Irish Republican Army (IRA) waged a 25-year terrorist campaign against London's Underground and British railroads. Between 1991 and 1999, IRA terrorists planted 81 explosive devices; during the same period, British transportation authorities had to deal with more than 6,000 bomb threats and had to inspect more than 9,000 suspicious objects.<sup>3</sup> From 1995 to 1996, terrorists in France carried out a bombing campaign aimed at the Paris Metro, local commuter trains, high-speed intercity trains, and other surface transportation targets. For the past two years, suicide bombers in Israel have frequently targeted buses. Terrorists connected with Al Qaeda planned to carry out attacks on Singapore's metro.

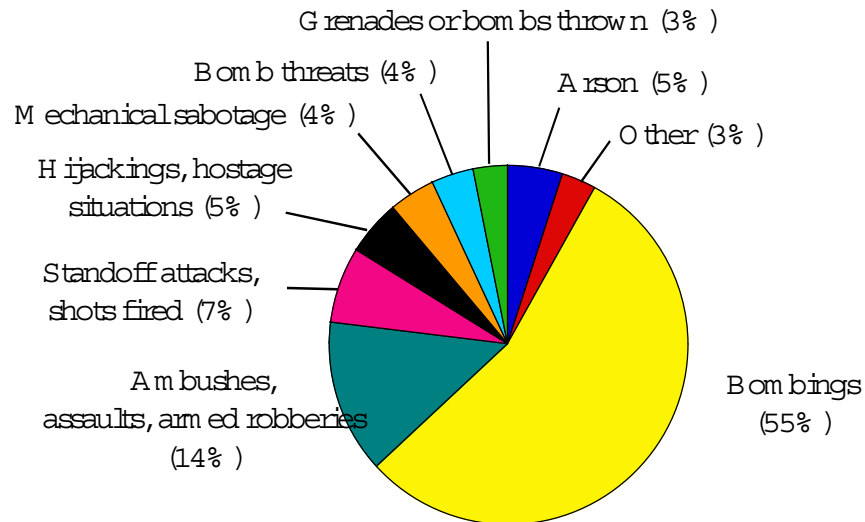
In the United States, the 1993 bombing of New York's World Trade Center blasted the train stations beneath the towers, although the attack was not aimed specifically at the subways. In 1995, a still unidentified saboteur derailed Amtrak's Sunset Limited in Arizona. In 1997, terrorists planned to carry out suicide bombings on New York's subways, but the plot was foiled when one of the groups informed police. The September 11, 2001, attack completely destroyed the New York Transport Authority (NYTA) and Port Authority Trans-Hudson (PATH) train stations at the World Trade Center. After September 11, a mentally disturbed individual attacked the driver of a Greyhound bus, causing it to crash and killing seven persons.

The following two charts, drawn from research conducted by the Mineta Transportation Institute, show that attacks on surface transportation have historically been divided almost evenly between trains and buses, with bombing being the most common tactic (excluding bomb threats). The deadliest incidents have resulted from explosions or deliberately initiated fires in crowded stations, trains or buses and from train derailments.

## Targets of Attacks on Public Surface Transportation Systems (1920—2000)



## Tactics Used Against Public Surface Transportation Systems (July 1997—December 2000)



European authorities today worry about chemical or biological attacks on local subways. Terrorist use of chemical, biological or radiological weapons in surface transportation is a real, not a theoretical, threat. In 1995, members of Japan's Aum Shinrikyo sect released nerve gas on Tokyo's subways, killing 12 persons; 5,500 people sought medical treatment and millions were terrified. Recent arrests in Europe of extremists connected with Al Qaeda who were engaged in manufacturing ricin and the discovery of a container of ricin in a Paris train station renewed fears that terrorists might try to disperse lethal chemicals or release biological agents at transportation facilities. Even a radiological attack is not unprecedented. In 1974, a mentally disturbed individual spread small quantities of radioactive isotopes on train coaches in Austria.

Large-scale attacks involving chemical or biological substances would be very difficult to carry out, but even a small-scale attack could produce widespread panic and, as demonstrated in the anthrax attacks in the United States in 2001, it could deny use of transportation facilities for a lengthy period and result in costly cleanups.

As the Tokyo subway experience shows, rapid diagnosis of an attack can be key to limiting casualties and contamination and can assist in discerning hoaxes, thereby reducing unnecessary shutdowns and disruptions. Bio-detectors can alert public health authorities to the dissemination of dangerous pathogens that otherwise might not become apparent for days, i.e. until symptoms developed and medical diagnosis was confirmed. Development of effective monitoring systems and portable devices is an area of intensive research, particularly in government-sponsored laboratories. Chemical and biological detectors were recently installed in the Washington, D.C., Metro on an experimental

basis. These detectors are, of course, useful for dealing with natural outbreaks of disease as well as terrorist attacks.

## **Implementing Homeland Security**

Security against terrorism has improved greatly since September 11. With allied help, the United States has launched a global campaign against terrorism, and at home, Americans have embraced the concept of "homeland security" – providing for the common defense – as a national mission. The government has created a new Department of Homeland Security to coordinate the federal response and a new military command has been created to coordinate the Defense Department's supporting role. Security has been significantly increased nationwide, largely by using local resources such as the National Guard, police and private security. Specific new measures have also been implemented to enhance the security of commercial air travel and the shipment of containerized cargo.

The vaccination of soldiers and health workers against smallpox has begun and sufficient vaccine is being stockpiled to inoculate the entire nation. New vaccines and antidotes to deal with other biological weapons are rapidly being developed, but thus far have failed to reverse the decline in U.S. public health and emergency medical treatment capabilities. Because of constrained local budgets, public health capabilities are, in fact, being reduced and emergency treatment centers closing.

Intelligence collection efforts have increased and federal agencies are getting better at sharing information. A system has been developed to consolidate all available intelligence and communicate judgments about threat levels. In addition, the federal government is about to create a combined intelligence analysis center. However, the government still has difficulty communicating threat information to the public in a way that does not lend itself to provoking panic or derision. And it has failed to effectively exploit the vast intelligence capabilities of the local police. With additional training and support, both technological and financial, local police departments could become part of a national terrorism intelligence network to supplement the current "hub and spoke" system in which intelligence is passed to the federal government and then fed back to local agencies.

Despite a great deal of rhetoric and some exchange of information, the federal government and the private sector have yet to achieve a true operating partnership. Problems lie on both sides. The government is understandably reluctant to share sensitive threat information (what little it has) or to offer specific advice. Corporations have increased their security, but they are reluctant to share proprietary information and they have not launched business-sector initiatives outlining workable security solutions. The surface transportation industry is a significant exception.

Clearly, many problems remain. The approach to homeland security, especially in the transportation sector, is regulatory and rule-based, implemented by enforcement – a “gates and guards” approach. This approach may be necessary to prod industries that are reluctant to divert precious resources to security, but regulatory approaches are seldom imaginative and with their emphasis on prevention rather than resiliency they are dangerously predictable and rarely efficient.

Paradoxically, a society that incorporates into its national myth the minuteman, the self-reliant pioneer and the armed citizen, has failed to effectively engage the public in homeland security. Ordinary people are warned what to expect, but they are not instructed as to what they can do.

### **Progress in Transportation Security**

The September 11 attacks prompted a profound review of transportation security. Understandably, the initial focus was on commercial aviation. The Transportation Security Agency (TSA) was established by the Aviation Security Act of 2001 to take over airline security, but it soon began addressing security for other transportation modes. Subsequently the TSA was moved from the Department of Transportation to the newly created Department of Homeland Security.

A review of events on and immediately after September 11 showed that local surface transportation systems were profoundly affected by the attack, but also that they played a vital role in evacuation, rescue, communications and recovery. Prompt action by stationmasters saved lives by preventing the unloading of passengers at the New York subway and PATH train stations under the World Trade Center. Additional commuter trains were mobilized to help evacuate New York City, and Washington's Metro and bus system similarly assisted in the evacuation around areas of the capital. At the same time, the Metropolitan Transportation Authority (MTA) in New York played a major role in getting emergency personnel into the city and to ground zero. The MTA's own emergency personnel and heavy equipment provided major support to the rescue effort, while its communication system was used to augment New York's damaged and overloaded emergency communications systems. The MTA also used its own website and staff to communicate directly with the public.

Following September 11, the Department of Transportation's Federal Transit Administration reviewed security measures and discussed improvements with industry associations and state governments. Systems operators and local police implemented the easy measures first. They increased the presence of uniformed and plainclothes security staff and conducted more frequent patrols. The public was asked to remain vigilant for suspicious activity and abandoned packages. Doors leading to vital systems were locked and stations were tidied to reduce hiding spaces. Crisis plans were reviewed and responses exercised.

In 2002, the National Academies created a Committee on Science and Technology for Countering Terrorism. Actually, this was a committee of committees; one panel, jointly sponsored by the National Academies and the Transportation Research Board, addressed the specific issue of transportation. The panel recognized that responsibility for the security of surface transportation rests with state and local law enforcement authorities and the public and private entities that own and operate the transportation infrastructure and assets. However, it noted that the creation of the TSA represents an opportunity to build security into the nation's transportation sector in a more systematic way. The TSA could be more than a mere regulatory and enforcement arm, although to fulfill a strategic role it would need to establish a strategic research and planning office. The panel also

recommended that the TSA establish an in-house capability to support its operations and evaluate new technologies for systems operators.

In late 2002, the General Accounting Office (GAO) conducted a survey of transit agencies to determine their security needs and to identify ways the federal government could best assist them. The GAO took note of the difficulties in securing public surface transportation: inherent vulnerabilities and high ridership make surface transportation systems both attractive targets and difficult to protect. Much progress had been made since September 11, but most of the improvements have addressed the easy things. Further significant improvements would cost billions. "Insufficient funding," the GAO reported, "is the most significant challenge in making transit systems as safe and secure as possible."<sup>4</sup>

In their constrained local budget environments, transit systems operators have looked to the federal government for help, but at the federal level, they would have to engage in fierce competition for finite dollars. Moreover, federal expenditures would have to be prioritized. The GAO concluded that a comprehensive risk-management approach would be the most effective way to improve surface transportation security.

The same themes were echoed in a broader GAO report issued in April 2003,<sup>5</sup> which repeated the need to develop a comprehensive risk-management approach and went on to recommend ensuring that transportation security funding needs be identified and prioritized, establishing effective coordination among the public and private entities responsible for transportation security, ensuring adequate work force competence and implementing security standards for transportation facilities. It is this final recommendation that merits close attention. The GAO believes that setting and enforcing security standards "will ensure that operators improve their security practices in modes where lax security could make surface transportation facilities attractive targets to terrorists." (This specific comment was made in the context of pipelines, but it would also apply to other transportation modes.) The GAO would require the Department of Transportation to prescribe standards for security and then approve or disapprove the operators' programs on the basis of adherence to these standards.

Operators, of course, would prefer a nonregulatory approach that gives them flexibility in designing security programs for specific facilities. The GAO itself recognized that there is little precedent for enforcement of standards in entities as large, complex and diverse as surface transportation systems. Moreover, setting standards presupposes that we know how much security is enough when, in fact, this is extremely difficult to determine. Finally, while goals and some performance measures are necessary, words such as *standards*, *prescribe*, and *enforce* have a decidedly regulatory ring. It is necessary to find a balance between exhortation and rule making, and we have to remain realistic about risk.

## **What do we do now?**

We tend to review transportation security mode by mode: commercial aviation, ports and container shipping, transport of hazardous cargo, public surface transportation, pipelines, bridges and tunnels. Each mode has its own requirements, but in treating each separately we may miss some broader strategic issues. Security must be assessed across the entire spectrum of transportation systems. Such an across-the-board look could lead to new and innovative security solutions.

Historically, security considerations in times of war have been major factors in the development of America's transportation system. George Washington's early unsuccessful military expeditions over Indian trails that did not allow the passage of cannons and wagons provided impetus for the new federal government to build the national road from Cumberland to Wheeling, West Virginia. While commerce was the main reason for improving the internal road network, British blockades in the War of 1812 further underscored the need. The great difficulty in moving troops and munitions to western New York provided an additional strategic reason for digging the Erie Canal. Railroads were built to open up the west, but it was the Civil War that demonstrated their strategic importance. In return for land grants, railroads were obliged to transport troops at half fare.

Poor roads plagued Pershing's expedition into Mexico. In World War I, shipping sufficient numbers of horses to Europe and enough fodder to feed them on the way obliged the American Expeditionary Force to switch to motorized transport, for which existing U.S. roads were inadequate; the vehicles could not be driven to embarkation ports and had to be ferried by rail. American security required good highways, an imperative renewed in World War II, ultimately leading to the federally subsidized interstate highway system. In the post-September 11-security environment, it is appropriate to contemplate a national transportation security strategy.

At present, there is no such strategy. Creating one would require identifying and ranking overall objectives: preventing the loss of life; minimizing long-term risks to health; and limiting social upheaval, environmental catastrophe and economic disruption. Because these concerns transcend the specific topic of transportation, the next step would be to determine the unique vulnerabilities of transportation systems and their potential consequences.

Airliners hijacked by suicidal pilots clearly represent the biggest terrorist threat to national security, since they can produce an order of magnitude more casualties than the bloodiest incidents of airline sabotage or truck bombs, and they can result in orders of magnitude more economic disruption. It could be argued that the security of commercial aviation therefore merits a larger share of the national resources devoted to security, whether paid for out of general tax revenues or special taxes on air travel. Clandestinely delivered weapons of mass destruction, the principal concern in container security, could also produce large-scale casualties and destruction, making this another priority area. Attacks on other transportation modes would have local effects, although the psychological effects could be felt nationally.

After September 11, many travelers switched from commuter flights to passenger trains, where available, or to private automobiles. Airlines understandably lamented the loss of revenue, but was this truly a negative development? Putting aside other factors, such as the efficient use of energy and environmental impact, one could argue that the shift actually favored security. Trains run on rails; unlike hijacked airliners, they cannot be turned into piloted missiles. Theoretically, fewer flights would represent a security gain. Such considerations should be factored into a national transportation security strategy.

Protecting one set of targets against terrorist attacks that can just as easily be carried out anywhere else may still be desirable for occupants and owners, but it represents no gain in overall national security – it merely displaces the risk. Some transportation targets may offer terrorists unique opportunities – for example, major train stations through which millions of passengers pass daily may present unique opportunities for chemical or biological threats. Tunnels also may have unique vulnerabilities.

Vulnerable bridges can be upgraded and protected at a cost, or, if they are near obsolescence, they can be replaced with new physically stronger structures. The system could also be augmented with additional bridges to make it less vulnerable overall. Rather than merely becoming a continuing operational expense, security could be the basis for the reconstruction of the U.S. national transportation infrastructure.

### **Surface Transportation Requires Its Own Security Model**

The commercial aviation model of security cannot be applied to surface transportation. There are differences in the threat, the consequences of attacks, the ability to provide security and the economics of the two modes. The terrorist threat to both is high: commercial aviation has remained a preferred terrorist target since the late 1960s, although improved security measures and international treaty agreements to extradite or prosecute hijackers have reduced the number of attacks. And according to government sources, approximately one-third of all terrorist attacks are directed against surface transportation.

The risk to individual passengers in either aviation or surface transportation is very low. A total of 246 passengers died in the four aircraft hijacked on September 11. Since there are more than 700 million passenger boardings annually in the United States, the risk to an individual on any flight in 2001 was approximately one in several million. Considering a longer time span – say, 10 years – would change the odds of perishing on an aircraft hijacked or sabotaged by terrorists to one in tens of millions. Every year, nine billion passengers use public surface transportation in the United States, so the odds of becoming a victim of terrorism in this venue are infinitesimal – one in tens of millions, or close to one in a hundred million if a longer-term horizon is used for an actuarial chart.

The consequences of attacks, however, do differ. A hijacked airliner with a suicide pilot at the controls can bring death to thousands, potentially tens of thousands. Damage can run to the tens of billions of dollars, with economic disruption in the hundreds of billions. It can be argued that with the new aviation security measures in place, especially locked

reinforced cockpit doors, this is no longer a viable tactic, unless the pilot in place is suborned. And even before the new doors were in place, the tactic had already failed: On September 11, realizing what was happening, passengers on United Airlines flight 92 took action against the hijackers and became part of the security system. Facing certain death if they do not take action, determined passengers are likely to behave the same way again; or when an aircraft is known to have been hijacked, Air Force planes might be ordered to bring it down. At least terrorist planners can no longer count on a permissive environment inside or outside the plane.

The situation is different with surface transportation. Trains and buses cannot be flown into skyscrapers, so the casualties that occur in a surface transportation attack are likely to be confined to the passengers themselves. And whereas the deadliest terrorist attacks on passenger aircraft have killed several hundred (325 in the 1985 sabotage of an Air India flight, 270 in the sabotage of PanAm 103 and 189 in the sabotage of a 1989 UTA French airline flight), the five deadliest train derailments each killed between 25 and 95 people, the ten deadliest bombings on trains or in stations each killed between 20 and 80 persons, and the deadliest attacks on buses each killed fewer than 40 persons. But while approximately 10,000 flights take off every day – perhaps fewer now as a consequence of recent cutbacks – the number of potential targets in the surface transportation system is probably in the hundreds of thousands.

Thus, the approach to security must be different for surface transportation. In commercial aviation security, the emphasis is on deterrence and prevention. If the layers of security have been breached, there is seldom much that can be done other than to use blast-resistant cargo containers to provide some protection against bombs smuggled inside checked bags or to implement schemes that override cockpit controls and remotely bring hijacked aircraft to safe landings. Mitigation is not much of an option – an airline crash allows few opportunities for lives to be saved, even with rapid response.

Public surface transportation offers easier access and higher volumes of passengers than aviation. Some deterrence of terrorist attacks may be possible, but prevention is extremely difficult in the absence of screening measures that, given the volume of users, the vast number of access points, the absence of advance ticket purchases and the low cost of fares, are unrealistic. Nearly 60,000 federal employees are needed to screen 700 million passengers a year at airports and waits at check points can be as long as an hour. How many security personnel would be needed to conduct even a rudimentary screening of nine billion surface transport users? And what kind of delays would screening introduce? It is significant that when faced with long-term terrorist threats to surface transportation, neither the United Kingdom nor Israel has adopted airport-style passenger-screening procedures (except at Israeli central bus depots).

Neither do the finances support the application of commercial aviation security to surface transport. Airline passengers now pay a security tax of \$2.50 per trip segment to offset total security costs. This represents a small percentage of a several hundred-dollar airline ticket. A similar percentage of surface transportation fares – which are typically a dollar or two – would not provide anywhere near the funds needed to support airport-style screening.

Security emphasis therefore must shift to mitigation through station and vehicle design, quick diagnosis of threats, prompt intervention and rapid response. In other words, surface transportation security has to be more reactive than proactive.

Commercial aviation is a network, whereas surface transportation is a mosaic. A terrorist bent upon attacking commercial aviation must penetrate security at one of 430 commercial airports in the United States. Once inside the security, however, the terrorist's target range is national. Surface transportation offers almost unlimited access points, but once a terrorist is on board his target range is local.

Because it is a single system, commercial aviation may be viewed as a single target, with the same security measures in effect at all airports. Surface transportation, in contrast, comprises diverse modes -- subways, elevated trains, light rail and buses -- and as a result, standardized procedures are harder to sustain or to justify.

Finally, the federal government's role in aviation is different from its role in surface transportation. In commercial aviation, the government has a broad mandate to dictate security measures. After September 11, Congress, in no mood to listen to industry opposition, created the TSA and instructed it to take direct charge of airport security. There is still concern that the federal government, driven by political considerations, may impose additional requirements that are disruptive, costly and that contribute only marginally to overall security. Given the airline industry's traditional reluctance to implement security measures that affect operations or the bottom line, an adversarial relationship has developed between government and the industry.

The federal government has far less authority in dealing with surface transportation, and we do not envision the creation of a national transport police like the force in the United Kingdom. Instead, we are likely to see an altogether different but still significant federal role, which we will discuss later.

### **A "Best Practices" Approach Rather Than Uniform Rules**

A surface transportation security strategy must reflect the diversity of the transportation networks. These complex networks range from long-distance rail and bus systems to commuter and city transit systems. They include trains, light rail, elevated trains, subways, stations, buses, terminals, thousands of miles of rail line itself, bridges and tunnels. (For the purpose of this discussion, we are excluding freight and pipelines.) Operations range in size from multi-modal urban systems to rural bus lines.

Transportation security has two objectives: preventing casualties and minimizing disruption. Therefore, a broader definition of "security" is required. Effective security must consist of more than deterrent and preventive measures; it must encompass all efforts to mitigate casualties, damage and disruption, and to facilitate rapid restoration of operations. Attributes of effective surface transportation security include flexibility, the ability to increase and decrease efforts according to threat conditions, an emphasis on

technology rather than personnel, and, given limited prevention possibilities, a focus on crisis planning and response training.

The terrorist threat must be viewed in national terms. Terrorists can attack anything, anywhere, anytime. It is not inconceivable that domestic terrorists or terrorists who are sent or inspired from abroad could carry out an attack in any surface transportation venue anywhere in the country. At the same time, the threat is not the same everywhere in the country. In fact, terrorists tend to carry out their attacks in nearby, familiar surroundings; most terrorist bombings occur within an hour's drive of the terrorist's home. Historically, the vast majority of terrorist attacks in the United States have occurred in six major metropolitan areas: New York, Washington, Miami, Chicago, San Francisco, and Los Angeles. The threat is not the same for Duluth as it is for the District of Columbia. Nor is it the same for a small rural bus line as it is for a major urban transportation network. National threat alerts imply a uniformity of threat, which simply does not exist, although no one can argue that "it won't happen here."

There is also considerable diversity in the way security is provided. Some large urban systems, such as the New York City MTA, have their own police forces. A few of the larger police departments have special transit divisions to deal with crime on trains and buses. In many systems, security is provided by a private security force, proprietary or contracted, which may operate under the auspices of a small proprietary police unit or a director of security. In some cases, local police provide security for the systems within their jurisdiction. Combinations of these are common, especially where transportation systems cross two or more police jurisdictions.

Given the diversity of the systems, the differences in the threat and the ways in which security is provided, transportation security cannot easily be mandated according to uniform standards and rules. A best-practices approach may be a more effective alternative. In such an approach terrorist events are constantly reviewed for lessons learned – what worked, what didn't work – to identify best practices, and supporting security technologies are evaluated. The findings are then passed on through reports and industry symposia.

Without compromising sensitive intelligence sources and methods, government agencies attempt to pass the best available information about possible threats, as well as general information about terrorist tactics and targeting, to local jurisdictions and operators. But getting this intelligence to local police and transport operators remains a challenge, one not yet met satisfactorily. The system could work better if local police departments throughout the nation were enlisted in terrorist intelligence collection and given the resources, training, technology and connectivity to become part of a national network.

In a best-practices approach, system operators and local jurisdictions armed with good terrorist intelligence can decide on the investment and procedures that best fit local conditions. There are no universally applied standards. Security for surface transportation becomes goal-oriented rather than rule-based.

Without minimum standards, there will inevitably be different levels of security. However, best practices, when published, have a way of becoming minimum standards. Certainly, no operator wants to operate at less than best practices; if an incident were to occur, the operator would be vulnerable to charges of incompetence or negligence and could be subject to liability litigation. But best practices remain a menu, not a prescribed diet.

### **The Division of Responsibilities**

A best-practices approach does require coordination among the stakeholders – federal, state and local, public sector and private sector. The operating entity has direct responsibility for security, for immediate response to threats, for crisis planning, and for restoration of operations. Local authorities, i.e., the police, share responsibility for providing overall security, passing intelligence along, conducting investigations, providing immediate response to threats, and participating in crisis planning.

In a best-practices approach, the federal government does not dictate security measures but supports ongoing research to conduct case studies that identify the best practices. The federal government funds research and development on new security technologies such as chemical-biological detection systems. It could provide a further valuable service by evaluating new security technologies coming onto the market. In some cases, the federal government could fund the deployment of experimental technology, and it could augment efforts by industry associations and state transportation agencies to disseminate best practices.

In addition to passing threat information to the local police, the federal government sometimes participates in the investigation of terrorist-related crimes. It supports emergency response and, depending on the circumstances, may provide specialized expertise and equipment (for example, in dealing with chemical, biological, or radiological threats). This role is consistent with the recommendations of the Transportation Research Board panel that was convened in 2002.<sup>6</sup>

The federal government also contributes to the ongoing security costs incurred by state and local governments, although this remains a problem area. The increased security costs incurred since September 11, 2001 have imposed an enormous burden on already strapped local governments. In extraordinary circumstances, the federal government could directly augment security at transportation facilities, as both the British and French did on occasion during terrorist campaigns in their countries. To date, this function has been carried out in the United States by the National Guard.

### **Conclusions**

The terrorist threat to surface transportation is real, and it will increase as terrorists seek ways to kill large numbers of people. However, the threat is difficult to quantify and it is therefore difficult to determine the right level of security.

Increased security measures implemented since September 11 have made surface transportation safer – somewhat. Operators and local authorities have done the things they could easily do. Much more remains to be done, but significant gains in security will require significant funding. It is not clear where the money will come from. Riders cannot provide significant funds for security without dramatic fare increases, which would affect use. Local and state governments now subsidize public transportation, but many of these governments are in dire financial straits and are looking for ways to cut budgets. The federal government can assist through research and development (R&D) funding, direct subsidies and tax incentives, but there is fierce competition for finite federal dollars. In the end, Americans may be obliged to accept some risk.

Effective security for surface transportation consists of more than deterrence and prevention, both of which are difficult, in any case, given the volume of passengers and the ease of accessibility of surface transportation facilities. Effective security must also include mitigation through design and construction and rapid response, both of which can save lives as well as minimize disruption.

Surface transportation is not a single national system. It is a complex quilt of networks that vary in size, mode, and means of providing security. There is no single solution. Immediately after September 11, government agencies and industry associations were able to provide useful security advice quickly, thanks to the availability of research that was conducted prior to September 11. This research examined terrorist tactics, distilled lessons learned from case studies of earlier terrorist attacks and identified best security practices.

Indeed, a best-practices approach may be the most effective model for surface transportation security, since it would allow operators and local authorities to decide what works for them. The aviation security model is definitely not applicable to surface transportation. Threat levels differ, the potential consequences of terrorist attacks are different and the systems themselves differ greatly, as do the means of providing security. There is no national mandate to set and enforce security standards for surface transportation, but given the diversity of the systems, a strict regulatory approach probably would not work anyway.

Crisis management and rapid response are essential ingredients in any security program. Crisis management plans can be improved and tested without a large financial investment, but response remains a problem because of resource constraints at the local level. Further gains in security can also be achieved with the deployment of new technologies. The detection of chemical and biological weapons is a priority area for research.

The federal government should focus on developing an overall strategic approach to transportation security, guiding and supporting research and development, evaluating new technologies and disseminating information to end users. The creation of a Homeland Security Department reaffirms the constitutional duty of the federal government to "provide for the common defense." Its greatest shortcoming thus far has been the failure to provide adequate resources to local authorities who are on the front line.

The transfer of the Transportation Security Agency from the Department of Transportation to the Department of Homeland Security, while reasonable from the standpoint of consolidating security functions, separates transportation security strategy from broader transportation strategy considerations. It could encourage enforcement strategies while failing to consider other ways to mitigate risks and disruptions, e.g., through design of the transportation system. At the very least, the consolidation poses a new challenge for cooperation. Close cooperation between operators and local or state authorities may be easier to achieve than cooperation with federal authorities. It is easy to sort out the respective roles and responsibilities of the operators, the local and state authorities and the federal government, but achieving a truly collaborative effort is far more difficult. There is no obvious answer here.

The terrorist threat is dynamic. Research must continue, not only on the development of new technology, but on monitoring trends in terrorism, anticipating novel means of attack, distilling lessons learned from past incidents and continually updating best practices.

---

<sup>1</sup> See: Mineta, Norman Y. (1996). International Institute for Surface Transportation Policy Studies. *Terrorism in Surface Transportation: A Symposium*, San Jose: Norman Y. Mineta International Institute for Surface Transportation Policy Studies; Jenkins, Brian Michael, et al. (1997). *Protecting Surface Transportation: Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks*, San Jose: Norman Y. Mineta International Institute for Surface Transportation Studies; Jenkins, Brian Michael & Gersten, Larry N. (2001). *Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices*, San Jose: Norman Y. Mineta International Institute for Surface Transportation Studies; and Jenkins, Brian Michael (2001). *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview*, San Jose: The Mineta Transportation Institute.

<sup>2</sup> Jenkins and Gersten, op.cit.

<sup>3</sup> *Ibid.*

<sup>4</sup> General Accounting Office (2002, December 13). *Mass Transit: Federal Action Could Help Transit Agencies*, GAO 03-263. Washington, DC: GAO.

<sup>5</sup> General Accounting Office (2003, April 1). *Transportation Security: Post-September 11<sup>th</sup> Initiatives and Long-Term Challenges*, GAO 03-616T. Washington, DC: GAO.

<sup>6</sup> Transportation Research Board (2002). Special Report 270, *Deterrence, Protection, and Preparation: The New Transportation Security Imperative*. Washington, DC: TRB.

Lexington Institute  
1600 Wilson Boulevard Suite 900  
Arlington, VA 22209  
Main: 703-522-5828  
Fax: 703-522-5837  
www.lexingtoninstitute.org