

RAIL SECURITY

Keeping terror off

*Kim E. Petersen,
President of RailSecure
LLC, looks at what steps
are being taken to reduce
the risk of terrorist attacks
on rail networks*

The man with the backpack blended seamlessly into the crowd of commuters – office workers and schoolchildren mostly – as he pressed his way onto the train bound for Madrid. Like his colleagues on the other three trains setting off from the Alcala de Henares station that morning, there was nothing about his appearance that would betray anything suspicious, let alone the fact that the rucksacks each was carrying contained 10 kilogrammes (kg) of high explosives.

Shouldering past the others boarding the train, the man and his terrorist brethren placed a total of 13 radio-controlled bombs onto luggage racks in nine tightly packed commuter carriages on four separate trains. Leaving their mass murder devices behind, they disembarked from their respective trains well before their arrival in Madrid.

At 06:39 local time on 11 March 2003, the first train came to a halt in Madrid's Atocha station. At that precise time a call was placed to the cell phone detonator attached to each device, exploding bombs in three separate carriages killing the first 34 people. Within seconds, four more bombs detonated on a second train that was just entering the station. Two minutes later, bombs in two other trains ripped through a total of three more carriages. In all, 191 people were killed and over 1,800 injured in the largest terror attack in Spain's history. Shortly following the attacks, the Abu Hafs al-Masri Brigade, claiming to act on behalf of Al Qaeda, took responsibility for the Madrid attack. Their communiqué to the press triumphantly stated: 'The Brigade's death squads are at your doors and will hit with an iron hand at an appropriate time and in an appropriate place. Praise be to God who granted us the victory of Madrid and destroyed one of the pillars of the evil Crusader axis.'

Evidence collected by western intelligence services indicates that subsequent to their horrific success with the 3/11 bombings in Madrid, Al Qaeda has expended significant resources to assess the vulnerabilities of rail operations around the world. The **US Department of Homeland Security (DHS)** has since issued threat bulletins regarding potential terrorist plots targeting US subways, trains, and buses in major cities.

Considering that world-wide, on an annual basis, passengers travel over two trillion miles and billions of metric tonnes (mt) of cargo are transported by rail, how vulnerable are the railroads, how serious is the terrorist threat, and what steps are being taken to reduce the risk of future attacks?

Railroad vulnerabilities

Railroad operations cannot be protected in the same fashion as aviation. 'You cannot run a train station or a commuter rail station like you run an airport. We're not surrounded by boundaries like an airport,' said Lieutenant Detective Mark Gillespie, commander of the Boston transit police department's investigative services. In the US alone, there are over 140,000 miles of rail network. In addition to immense quantities of freight, there are over 13 million passengers travelling daily on railroads, many times the number flying on commercial airliners. Consider that the US now employs some 60,000 screeners at airports to check just two million passengers daily. Experts agree that airport style screening of all rail travellers would be virtually impossible.

The success of any rail system relies in large measure on its accessibility to population and industrial centres. And it is this ubiquity and the essential role trains play in transporting people and goods that makes them such an attractive target for terrorists. Rail-directed terror is enticing precisely because of the approachable nature of railroad operations. The design and layout of terminals and stations, for example, promise concentrations of victims along with reliable corridors for escape. The terrorist's choice of vectors for attack are manifold, including: mechanical derailment; release of hazmat by way of explosives or stand-off attack (using firearms or rocket propelled grenades); explosives placed within commuter train cars; sabotage of trestles, bridges, or tunnels; explosives or firearms attack on train stations; the release of a biological or chemical agent into the atmosphere within a train or terminal; and, cyber attack, including interference with traffic control systems. Terrorists have used simple hand tools to conduct sabotage against railroad tracks and switches. Unbolting joint bars, misaligning switches, or even positioning

Kim E. Petersen is the President of RailSecure LLC. A multi-disciplinary company, RailSecure provides risk consulting, risk management solutions, training, and specialised-guard services. Kim E. Petersen has held senior staff positions with former US Secretaries of State Henry A. Kissinger and Alexander M. Haig, and in both the US Senate and US Defense Department in the areas of national security and intelligence.

the tracks

a vehicle across the tracks of an oncoming train can wreak catastrophe.

Background and threats

The Madrid train bombings were a wake-up call analogous to the Al Qaeda maritime attacks against the *USS Cole* and the *Limburg*. These events finally spurred action by government and industry, even though terrorists have been successfully attacking rail and maritime assets for decades. For example, only a few weeks before the Madrid attacks, terrorists placed a bomb on Moscow's Metro killing 39 and injuring more than 100.

According to the **RAND Corporation's** database of terrorist incidents, and excluding the Madrid bombings, there were a total of 181 terrorist attacks world-wide on trains and rail-related targets, such as rail yards and stations, between 1998 and 2003 – an average of 30 a year. These attacks resulted in the deaths of 431 people.

The **US State Department** reported that over the past ten years, indigenous groups, and not transnational groups as one might expect, committed most of the terrorist attacks against rail systems. Some notable incidents are attributed to age-old antipathies directed at former colonial powers – the proverbial chickens coming home to roost. For instance, Algerian extremists have carried out multiple improvised explosive device (IED) attacks against rail systems in France. None of these Algerian attacks have been on the scale or the sophistication of the Madrid bombings, but the vulnerability of the railway infrastructure is nevertheless manifest.

A sampling of terrorist attacks on trains and subways over the last quarter of a century include:

- *France, 2004-2005*: A group calling itself AZF sent letters demanding \$6 million to president Jacques Chirac and interior minister Nicolas Sarkozy, warning that it would set off explosives on French rail lines if its demands were not met. Police were given the location of a bomb planted near Limoges. Investigators detonated the device, which police described as 'surprisingly sophisticated'.
- *Israel, 24 April 2003*: One Israeli died

'Rail-directed terror is enticing precisely because of the accessibility of railroad operations, coupled with their fundamental vulnerabilities'

and 13 were wounded in a suicide bombing outside the Kfar Saba train station. Groups related to the Fatah Al Aksa Martyrs Brigade and the Popular Front for the Liberation of Palestine claimed responsibility for the attack.

- *India, 13 March 2003*: At least ten commuters were killed and 70 injured when a bomb detonated in the first class compartment of a local train in Mumbai.
- *Angola, 11 August 2001*: An explosive device derailed a train carrying refugees between Luanda and Dodo. The attackers, identified as members of the terrorist organisation UNITA, then used small arms to kill 91 people and wound another 165 attempting to escape from the wreckage.
- *Pakistan, 7 June 1998*: Officials blamed India's Research and Analysis Wing of the Indian intelligence service for involvement in a train bomb explosion that killed 22 people and injured another 36.
- *France 25 July 1995*: Officials identified an Algerian terrorist network as being responsible for an attack on a subway train at the St. Michel metro station in Paris on 25 July, killing ten and injuring many more. The attack was part of a wave of bombings in 1995.
- *Japan, 20 March 1995*: Tokyo subways suffered a poison-gas attack when terrorists from the religious cult Aum Shin Rikyo put containers of highly toxic Sarin nerve gas in three trains at rush hour. Although the Tokyo Emergency

Control Centre staff received alarms within fifteen minutes, the lethal gas spread quickly at fifteen subway stations (carried there by the trains). Twelve people died, and over 5,000 became ill, with numerous victims suffering permanent brain damage.

Despite this grim history and the daunting task of preventing future acts of rail terrorism, much is being done to effectively mitigate security vulnerabilities and risks.

Industry response post-9/11

In the aftermath of 9/11, the rail industry and the DHS struck a partnership to safeguard the 142,000 miles of rail network, 500 million annual passenger trips, and several thousand train stations across the country. The proactive leadership of the **Association of American Railroads (AAR)** created a freight rail industry security plan immediately following 9/11 without prompting from the government. The AAR's *Terrorism Risk Analysis and Security Management Plan*, orchestrated by former Executive Vice President Chuck Dettmann – believed by many to be the US's leading expert in rail security – was comprehensive and based upon national security intelligence at the Top Secret level. Few in the government were similarly capable of comprehending both the magnitude and the appropriate technical approach required to assess the vulnerability of the massive US rail system.

Detailing proactive measures and protocols that have since become standard operating procedures for railroads throughout the nation, the plan was predicated on a comprehensive risk analysis that covered the entire industry including train operations, communications and cyber-security, identification and protection of critical assets, transportation of hazmat, and liaison with military, intelligence, and law enforcement agencies. The report considered non-rail operators throughout the supply chain, including seaports and other surface transportation entities.

The AAR's risk analysis identified more than 1,300 critical assets resulting in a priority-based blueprint of actions; the creation of more than 50 permanent changes to

RAIL SECURITY

procedures and operations, including: restricted access to facilities; increased tracking of high-risk shipments; enhanced employee security training; and, improvements in information and cyber-security. The AAR then adopted a progressive four-level security alert system, each with a set of countermeasures to be activated when specific threat indicators are triggered.

Integrating industry and government

Rail industry priorities included establishing a threat intelligence system for appropriate industry operators to ensure rapid and proportional countermeasures. This was accomplished in three ways:

- provisioning a rail police administrator to the **Federal Bureau of Investigation's (FBI)** National Joint Terrorism Task Force, along with a rail security analyst at two DHS intelligence offices, to provide critical expert analyses of raw intelligence up to the Top Secret level.

- creating a **Department of Defense (DOD)**-certified Operations Centre, operating 24/7. Working with classified intelligence, the Ops Centre evaluates threat data and communicates with railroads through the Railway Alert Network (RAN).

- creating an intelligence fusion centre under the provisions of Presidential Decision Directive 63, which encouraged the establishment of an industry-led Information Sharing and Analysis Centre (ISAC). Also operating at the Top Secret level, the AAR's Surface Transportation ISAC (ST-ISAC) collects information from government, industry, and open sources, and using rail security experts with operational experience, analyses and relays security intelligence to railway officials.

Recognising that employees are the eyes and ears of the industry, railroads ramped up security training that is now part of every employee's duty preparation. Now, employees receive daily security briefings as well as lectures, emails, brochures, newsletters and posters. Some railroads have also instituted a rewards programme for tips and suggestions on enhancing security. Expert organisations such as **RailSecure** are providing broad-based security training and certification programmes for railroad

employees and management, as well as law enforcement personnel.

Hazmat transportation is a recognized target for terrorists, and industry is responding to the threat.

Hazmat tank cars must comply with stringent **Department of Transportation (DOT)** construction specifications and field-testing. The AAR is heavily involved in tank car safety and research at its own testing facilities, and rail crews are given special hazmat training pursuant to federal regulation.

Given the magnitude of the industry's response to 9/11, it is not surprising that many in government have praised its efforts. Allan Rutter, former Administrator of the **Federal Railroad Administration (FRA)**, said in an interview: 'I can say how impressed I am by the scope of the analysis, the sophistication of the analytical framework, and the manner in which rail carriers have devoted substantial resources – both funding and senior leadership – to the completion of this important task (of enhancing security). Railroads have done remarkable work.'

Government response post-9/11

The responsibility for regulating the security of US rail and mass transit systems is primarily shared between the DHS and the DOT, though other federal agencies have taken steps to address rail security in partnership with the public and private entities that own and operate rail systems. Proposed initiatives target three specific areas: threat response capability, public awareness and participation, and technological development. Several key rail security programmes are being discussed by these government agencies:

- **Mass Transit K-9 programme**

DHS hopes to develop a rapid deployment Mass Transit K-9 programme by using existing explosives-detecting K-9 resources. Building upon the **Transportation Security Administration's (TSA)** work in aviation, the DHS will also provide training and assistance for local K-9 teams. The mobile programme would predominantly be used in special threat environments, providing additional federal resources to augment state and local transit and rail authorities' organic security capabilities.

- **Transit Inspection Pilot**

The DHS plans to implement a pilot programme testing the feasibility of screening targeted luggage and carry-on bags for explosives at rail stations and aboard trains. The initial programme will be implemented at one station with commuter rail service in conjunction with **Amtrak** and the FRA. The pilot programme would provide the DHS with a venue to test new technologies and screening concepts. The lessons learned could allow transit operators to deploy targeted screening in high threat areas or in response to specific intelligence.

- **Education and awareness**

The rail industry and the **Federal Transit Administration (FTA)** have co-developed several employee and public awareness campaigns. The DHS intends to work with state and local rail and transit authorities along with the DOT to incorporate previously existing passenger and rail education and awareness programmes.

- **Countermeasures**

The DHS's Science and Technology division focuses on developing security technologies for deployment in mass transit environments, including countermeasures applicable to chemical and biological events. President George W. Bush's FY 2005 budget request includes \$407 million for the DHS to continue developing biological countermeasures (including an integrated threat agent warning and characterisation system) and \$63 million for chemical and high explosives countermeasures, with both efforts applicable to rail systems.

Most of these programmes are in the planning stages, with funding less than certain as the US Congress pares back spending in all segments of government.

Recommendations

At a recent conference of rail executives, John Hart, CEO of RailSecure, said: 'In an industry that prides itself on its passenger and employee safety record, significant work is now underway to address emerging threats from terrorism and crime.'

Speaking to an international audience of executives and operators, including many from the developing world, he made

RAIL SECURITY

recommendations designed to mitigate security risks.

Among his suggestions were that railroad operators:

- repair or replace dilapidated fencing around rail facilities
- install security-grade lighting around facilities and critical infrastructure
- replace garbage cans at passenger rails stations with blast-resistant, transparent trash containers to prevent their being used for concealing IEDs
- design passenger terminals for ease in evacuation and to facilitate the arrival of emergency first-responders
- install closed-circuit television systems to monitor facilities, tunnels, and bridges
- use intelligent video surveillance systems to increase efficiency and reduce manpower costs

- affix signage in stations and on carriages to increase awareness about unattended packages, evacuation procedures, and restricted areas

- increase the training of all railroad staff
- conduct frequent drills and exercises, particularly regarding emergency response actions
- increase security patrols around facilities and along track corridors
- conceal the contents of hazmat tank cars so as to make it difficult for terrorists to visually identify worthwhile targets, but work with law enforcement and first-responder organisations to ensure that they can readily determine such contents in the event of an incident
- redesign passenger cars to reduce hiding places for IEDs
- educate passengers on the need for their

vigilance in spotting and reporting suspicious persons or items that could represent a threat to public safety.

Terrorists have already demonstrated a preparedness to attack commuter, passenger, and freight rail operations making it essential that industry and government, in partnership, complete the process of forging a terrorist-resistant security infrastructure. At the same time, governments must do a better job of allocating counterterrorism resources to the rail industry.

Contact:

Kim E. Petersen
 RailSecure LLC
 Mobius Security Group
 Tel: +1 954 567 4700
 Fax: +1 954 567 2511
 Web: www.railsecure.com

Cargo Security International

A unique source of intelligence on intermodal cargo security

Cargo Security International is read by thousands of transport, cargo and security professionals, and by governments, legislators and military experts in more than 40 countries. Why? Because it is the **ONLY** magazine that covers all modes of transportation – air, rail, road and maritime – with such a sharp focus on security.

The magazine is fully supported by the highly active 24/7 Internet news and archive service, www.cargosecurityinternational.com, a wholly reliable source of information on all new security-related commercial and governmental initiatives around the world.

Subscribe today and find out more by visiting www.cargosecurityinternational.com

Be aware, be prepared, be involved

SUBSCRIBE NOW!

