

April 15, 2004

Madrid train bombing highlights deadly threat

19th century security measures jeopardize 21st century rail systems

Images of the train bombing in Madrid, Spain, on March 11, 2004, immediately triggered vivid recollections of the hijacked planes that crashed into New York's World Trade Center; the Pentagon in Washington, D.C., and a Pennsylvania field on September 11, 2001. The al Qaeda network responsible for the September 11 attacks in the United States has also been linked to the terrorists who carried out the bombings in Madrid. Authorities in Spain have arrested 20 suspects in connection with the attack, which killed 191 people and wounded more than 1,800.

Dubbed by some U.S. media outlets as "Spain's 9/11," the bombing once again directed the world's attention to the new breed of terrorism. Rather than targeting military or government representatives, the perpetrators of this horrific attack killed businesspeople and school-children and struck at the heart of the city's economy. While the terrorists chose to use trains rather than airplanes to carry out murder and mayhem on this occasion, the goal was the same as on September 11: to destroy the way of life in the Western world.

While the Madrid bombing reminded the United States that destruction of the World Trade Center was not an isolated incident, the National Commission on Terrorist Attacks Upon the United States continues to investigate what should have been done prior to September 11 to reduce the risk of terrorism in this country. Administration officials have testified before the panel on "who knew what and when," but the business community needs to focus on acting now to protect against future attacks.

'Spain's 9/11'

On March 11, during the morning rush hour in Madrid, 10 bombs concealed in backpacks tore apart four crowded commuter trains. The terrorists, believed to have detonated the bombs using cell phones, reportedly have links to al Qaeda. In the weeks after the bombing, Spanish authorities have continued to make arrests, with most of the individuals charged and jailed.

Three days after the attacks, many Spaniards—blaming the incident on Prime Minister Jose Maria Aznar's support of the U.S.-led war in Iraq—voiced their outrage during their national election, ousting Aznar and electing Jose Luis Rodriguez Zapatero in a surprise upset. Zapatero quickly pledged to with-

draw the estimated 1,300 Spanish troops now in Iraq unless the United Nations assumes control over coalition forces there. A suspected al Qaeda affiliate viewed this pledge as a sign of victory, sending a statement to an Arabic newspaper. "Because of this decision, the leadership has decided to stop all operations within the Spanish territories until we know the intentions of the new government that has promised to withdraw Spanish troops from Iraq." The Federal Bureau of Investigation has since warned that terrorists might seek to influence upcoming U.S. elections in the same way.

The nation's worst terrorist attack, and the highest death toll from a single act of terrorism in a Western country since September 11, 2001, the bombing ignited concern for the potential execution of similar incidents in other European capitals. Less than two weeks later, a French railroad worker discovered an explosive device buried along a railway line from Paris to Switzerland. Then on April 2, police discovered more than 20 pounds of explosives under a track along the high-speed rail line between Madrid and Seville, again heightening the focus on the terrorists' new modus operandi.

The Madrid tragedy stirred empathy among U.S. residents, but the attack also renewed fears of existing vulnerabilities in the United States and revived questions about what progress the country has made on the security front during the past two years.

Slow progress

Protecting the U.S. transportation system remains a daunting task despite increased funding and the creation of the Department of Homeland Security. Each year in the United States, 730 million people travel via commercial airliners, carrying more than 700 million pieces of luggage that are screened for explosives. Ground transportation includes 11.2 million trucks and 2.2 million rail cars entering the United States annually, and 7,500 foreign ships make 51,000 calls in U.S. ports each year.

In the weeks following the attack in Madrid, U.S. Homeland Security Secretary Tom Ridge

(continued on next page)

Madrid train bombing highlights deadly threat

19th century security measures jeopardize 21st century rail systems

(continued from preceding page)

announced new U.S. rail security programs, calling the Madrid bombing “a solemn reminder that terrorists continue to expose or exploit our vulnerabilities.” In addition to developing a program of “best practices” shared between railroad, aviation and local transit authorities, Ridge proposed a rapid-deployment K-9 program to respond to special explosive threat situations. Citing the need to balance security with flexibility and convenience, Ridge announced a pilot program to test the feasibility of screening luggage aboard trains similar to the procedures used by airlines.

While securing 22,000 miles of passenger track “just isn’t feasible” according to some in the industry, one rail line has added bomb-sniffing dogs to its security program and budgeted \$1 billion to improve safety at six New York train tunnels. Further action must be taken to protect the more than five million people who use the U.S. rail system on an average weekday. Unfortunately, this transportation system continues to rely on the 19th century security initiatives developed to protect passengers from such perils as attacks by train robbers or Native Americans.

Despite the railroad security upgrades outlined by Ridge and efforts to enhance port security and border patrols, 97 percent of the Transportation Security Administration’s budget is earmarked for aviation security. Proponents argue that attacks on a train, subway, truck or ship could not produce the catastrophic results of an assault involving an airplane, and that the expansive nature of the railway, road and coastal systems prevents effective risk containment. Critics argue that a successful attack involving the country’s rail, trucking or shipping lines could create a crisis of confidence in the U.S. transportation system, shutting operations down during an investigation and bringing the economy to its knees—a primary goal of the enemy.

Unresolved problems

Despite progress, vulnerabilities still jeopardize the nation’s critical infrastructure, such as the

utilities, food, finance and transportation industries. While airline passenger baggage undergoes screening for explosives and other potential weapons, airfreight does not receive the same scrutiny. New initiatives have improved scrutiny of shipping containers, in excess of 15 million en route or awaiting delivery around the world daily, but the U.S. General Accounting Office (GAO) reports that the volume of imports makes it impossible to physically inspect all oceangoing containers without disrupting the flow of commerce.

Separate GAO reports reveal that the agriculture and chemical industries still lack comprehensive security measures to ensure protection against food contamination or a “dirty bomb,” which uses traditional explosives to disseminate radioactive particles. The devastating disconnect in communications among emergency responders, manifested in the deaths of firefighters in the collapse of the World Trade Center, has yet to be rectified. Incompatible equipment often prevents responders from neighboring communities or cooperative organizations from sharing information during times of crisis. The Terrorist Screening Database, a single source for names of suspected terrorists, finally went online March 12, 2004, but it remains a “work in progress.”

Plans to address many of these weaknesses remain under development, such as new technology for countermeasures to intercept suicide bombers and truck bombs. But the list of existing vulnerabilities still offers a lengthy menu of options for terrorist groups. The number of unresolved security issues, however, requires immediate action and cooperation between the public and private sectors.

“The business community needs to find a means of arriving at uniformly enforced standards,” says Dr. Stephen E. Flynn, Jeane J. Kirkpatrick Senior Fellow for National Security Studies with the Council on Foreign Relations. “This will require the private sector to help establish and implement the procedures, but it will also require government to mandate and enforce them. It has

become obvious that we cannot achieve adequate security within these critical infrastructures by voluntary efforts alone. The public and private sectors must work together to identify vulnerabilities, establish standards, and enforce policies so that everyone shares the cost and responsibility of the effort and no market advantage exists to leaving security problems exposed.”

The assaults on September 11 served as a catalyst to improving airline security; the nation cannot wait for a future attack to direct the focus on another vulnerability. To garner the necessary public and corporate support, the blueprint for security must strike a balance to ensure protection without compromising either the flexibility and convenience of the transportation system or the civil liberties demanded by Americans. In the transportation arena, for example, security is viewed as an inhibitor that raises costs and undermines efficiency and reliability. Yet similar arguments decades ago against the use of airport magnetometers in response to hijackings—and more recently against the implementation of extensive passenger and baggage screening after September 11—waned after realization that the measures greatly improved security with minimal disruption.

Role of the private sector

As more time has elapsed without an attack on U.S. soil, many people have been lulled into a sense of complacency, convincing themselves that the aggressive military response to September 11 deterred al Qaeda. Madrid changed that attitude, demonstrating that al Qaeda cells have metastasized and are capable of wielding a sophisticated attack in a major European city, likely without any direct oversight from their senior leadership.

“Al Qaeda cells in our first-world societies are demonstrating their ability to identify and exploit vulnerabilities,” said Flynn. “We need a much greater sense of urgency in both the public and private sectors to enforce safeguards. There has really been very little improvement in trans-

portation security since September 11, 2001, and because the system is primarily in the hands of the private sector, it will take action by the private sector to implement incentives for investing in security initiatives.”

Adopting a single security solution, such as an access control system, however, will not solve the problem. Eliminating one method of attack will only prompt terrorists or criminals to seek another method. Layers of security must be employed to improve effectiveness. The following steps can provide valuable assistance to the security efforts of the nation, as well as individual corporations:

Prepare for the unexpected. Company executives and security personnel should engage in an exercise to identify all potential threat scenarios that the facility could encounter. This process should include pinpointing details such as likely targets and methods of attack. All possible threats listed in the exercise should then be ranked according to their likelihood of occurrence and their ramifications to business continuity. This creative-thinking process can help identify the most pressing security concerns faced by the organization by incorporating insight from both business leaders and security experts.

Assess the vulnerability of industries and facilities. Industry leaders should examine the vulnerabilities they face and develop cooperative response plans. For example, the origin and shipping methods of raw materials could create a potential risk for sabotage. Procedures must be in place to effectively monitor shipments and their contents at each point along the delivery route, such as checking for signs of tampering and matching serial numbers with invoices. In addition, each facility should be evaluated by an outside professional with experience in identifying potential risks and recommending security solutions. Access control procedures and heating, ventilation and air conditioning (HVAC) systems represent two key areas requiring attention.

(continued on next page)

Madrid train bombing highlights deadly threat

19th century security measures jeopardize 21st century rail systems

(continued from preceding page)

Organizations that produce or store “dual use” materials, such as the radioactive components used by hospitals for cancer detection and treatment, must particularly enhance security of these resources, lest they be stolen and fashioned into “dirty bombs.”

Conduct pre-employment background screenings.

Companies should carefully screen applicants for employment, while complying with U.S. Immigration and Naturalization Service requirements, to help protect against “sleepers,” terrorist agents who establish themselves in society until called to action, as well as criminals seeking easy access to a facility or even unqualified individuals submitting dishonest résumés. Ensure that contractors and vendors whose employees will have access to the facility adhere to similarly high standards of employment.

Develop cooperative relationships. Effective security requires a shared effort among suppliers, transporters, manufacturers, sellers and users to develop and implement cohesive measures. Companies should also establish relationships with local police, firefighters and other emergency responders to develop sound crisis response plans. In addition, educational campaigns by government agencies, local authorities and businesses can help the general public understand the risks still faced by the nation and the importance of supporting security efforts.

Practice crisis response plans. Preparedness requires more than just a written outline of procedures. Tabletop exercises give those on the response team an opportunity to test the plan and correct any weakness before it must be put to the test. To be effective, plans must be practiced at the industry and facility level, and must be performed regularly and adjusted in response to developing vulnerabilities and evolving security needs.

Establish a shared focus on security. Like-minded industries should work together to

establish best practices for their specific security needs, incorporating insight from government agencies and outside security professionals. In addition, employees must understand the need for compliance with established security procedures, as well as know to whom they can report suspicious individuals or activity.

Even the most carefully crafted and rigorously implemented security program cannot protect against all forms of attack. Terrorists willing to give their lives to promote a cause or even the uncontrollable forces of nature can at times overcome the best laid security plans. But having an effective security program is like an insurance policy—its value is often only appreciated when faced with a crisis.

Gaping vulnerabilities still exist within the U.S. transportation systems. These security threats require a serious focus on implementing effective solutions, including Cabinet-level meetings and marshaling of agencies' resources and expertise. The problems require enlightened, 21st century thinking for a 19th century system. During the early years of rail travel, for example, the expense of lighting railway stations prevented the installation of a basic security measure that remains inadequate today. Those who oversee and operate the railroad system must adopt a proactive approach to its protection. In addition, private enterprise and individuals cannot rely on the government to be the nation's sole protector. Each corporation and citizen must contribute to the ongoing security effort by fortifying the protection of business facilities and demanding prompt response to the glaring vulnerabilities that still exist within the United States—before terrorists exploit them once again.



The Lipman Report Editors