PROTECTING CRITICAL RAIL INFRASTRUCTURE

by

Gregory S. Capra

The Counterproliferation Papers

Future Warfare Series No. 38

USAF Counterproliferation Center

Air University

Maxwell Air Force Base, Alabama

Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **DEC 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE **Protecting Critical Rail Infrastructure**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,USAF Counterproliferation Center,Maxwell AFB,AL,36112-6427**	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Terrorist attacks and accidents involving rail systems have resulted in death and destruction. The attacks in Madrid and London are good indications of the potential effects of a terrorist attack on the United States rail systems. Three years after the Madrid bombings, the United States has made little progress in securing its rail systems. This paper advocates that the United States develop a long-range comprehensive, integrated National Transportation Strategy to address security of the systems and the demand to move more people and cargo. A background on foreign terrorist attacks in the United States and an overview of rail systems are included, as well as an examination of ? terrorist threats to the United States and its rail systems ? vulnerabilities and critical elements of freight railroads and passenger rail systems ? Department of Defense?s role in protecting critical rail infrastructure; and ? specific recommendations on what to protect first and how to protect it. Priorities for protecting rail systems are: (1) transit rail stations in the biggest, most densely populated cities with a history of terrorist attacks (2) railroad shipment of hazardous materials through large metropolitan areas; and (3) passenger trains and other rail stations. Actions required to protect these assets are: (1) accelerated development of high-volume, walk-through chemical, biological, and radiation sensors to screen passengers and bags at transit stations; (2) rerouting hazardous cargo railroad shipments around cities with high densities of population; and (3) developing an integrated National Transportation Strategy.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**62**	

Protecting Critical Rail Infrastructure

Gregory S. Capra

December 2006

Counterproliferation Paper No. 38

USAF Counterproliferation Center

Air University

Maxwell Air Force Base, Alabama 36112-6427

The Internet address for the USAF Counterproliferation Center is:

http://cpc.au.af.mil/

Contents

Disclaimer

The views expressed in this publication are those of the author and do not reflect the official policy or position of the U.S. Government, Department of Defense, or the USAF Counterproliferation Center.

The Author

Gregory S. Capra serves as the Chief of the Program Management Office, Air Force Center for Environmental Excellence, Andrews AFB, Maryland. He earned a bachelor's degree in Civil Engineering from the University of Colorado and a master's degree in Strategic Studies from the Air War College at Maxwell AFB, Alabama. He is licensed as a Professional Engineer in the Commonwealth of Virginia. Since entering Federal Civilian Service in 1987, he has supported the men and women of the United States Army and Air Force by serving in various positions at the installation, major command, and headquarters. Prior to attending Air War College in 2006, he served as a Base Closure and Realignment Analyst for the Office of the Air Force Civil Engineer, Headquarters Air Force, Washington, DC.

Acknowledgments

Abstract

Terrorist attacks and accidents involving rail systems have resulted in death and destruction. The attacks in Madrid and London are good indications of the potential effects of a terrorist attack on the United States rail systems. Three years after the Madrid bombings, the United States has made little progress in securing its rail systems.

This paper advocates that the United States develop a long-range, comprehensive, integrated National Transportation Strategy to address security of the systems and the demand to move more people and cargo. A background on foreign terrorist attacks in the United States and an overview of rail systems are included, as well as an examination of:

- terrorist threats to the United States and its rail systems;

- vulnerabilities and critical elements of freight railroads and passenger rail systems;

- Department of Defense's role in protecting critical rail infrastructure; and

- specific recommendations on what to protect first and how to protect it.

Priorities for protecting rail systems are: (1) transit rail stations in the biggest, most densely populated cities with a history of terrorist attacks; (2) railroad shipment of hazardous materials through large metropolitan areas; and (3) passenger trains and other rail stations.

Actions required to protect these assets are: (1) accelerated development of high-volume, walk-through chemical, biological, and radiation sensors to screen passengers and bags at transit stations; (2) rerouting hazardous cargo railroad shipments around cities with high densities of population; and (3) developing an integrated National Transportation Strategy.

Protecting Critical Rail Infrastructure

Gregory S. Capra

I. Introduction

Terrorist attacks on public transportation are nothing new. Since the early 1990s, those concerned with the security of public surface transportation have been increasingly worried that trains and buses were becoming highly attractive targets for terrorists bent upon body counts… For those [terrorists] determined to kill in quantity and willing to kill indiscriminately, trains, subways and buses are ideal targets. They offer terrorists easy access and escape. Congregations of strangers guarantee anonymity. Crowds in contained environments are especially vulnerable to both conventional explosives and unconventional weapons. Terrorist attacks on public transportation systems also cause great disruption and alarm – the traditional goals of terrorism. The terrorists who target transportation systems are often seeking slaughter. An analysis of nearly 1,000 terrorist attacks on transportation found that the percentage of those involving fatalities – 37 percent – was much higher than the percentage for terrorist attacks in general. Two-thirds of the surface transportation attacks clearly were intended to kill; 74 percent of the fatal attacks involved multiple fatalities; and 28 percent involved 10 or more fatalities.

–Brian Michael Jenkins
Before the Committee on Judiciary United States Senate
April 8, 2004

Terrorist attacks and accidents involving rail systems have resulted in the death of innocent people and millions of dollars of damage. In 2003, terrorists simultaneously exploded 10 bombs killing 191 people and injuring 1,500 people in a coordinated attack of four commuter trains in Madrid. In 2005, another coordinated terrorist bombing of one bus and three underground trains in London killed 56 and injured more than 700 people when terrorists exploded four bombs.

In addition to these documented terrorist attacks, there are rail accidents that give a good indication of what might be the effects of a terrorist attack against U.S. rail systems. In 2005, two trains collided in Graniteville, South Carolina, releasing poisonous chlorine gas. Nine people were killed, 545 were treated at local hospitals, 5,400 were forced to evacuate, and the estimated damages are $30 million to $40 million.[1] In 2005, a commuter train struck a sports utility vehicle parked on railroad tracks by a man attempting to commit suicide. The man changed his mind at the last minute and left his vehicle. The commuter train railcars jack-knifed and struck another commuter train and freight train. Eleven people died and more than 100 were treated for injuries.[2] Had terrorists caused these accidents, the damage, deaths, and economic effects would have been potentially much greater.

These terrorist attacks and rail accidents have increased concern for the security of the rail systems in the United States. However, nearly three years since the attack in Madrid, the United States has shown little progress in improving the security of its rail infrastructure, but rather has focused nearly all its attention on securing passenger aviation transportation infrastructure.

The United States Congress Government Accountability Office has advocated for additional federal funding to secure rail infrastructure and recommended allocation of funds based on the highest risk – not a fair share basis.[3] Recently the Government Accountability Office and terrorism experts also recommended the United States government use an integrated approach in securing all transportation systems.

This paper uses a risk management approach to prioritize which rail systems to protect first and how to go about protecting them. This method determines the risk by assessing three factors: the threat, the vulnerabilities, and the criticality or importance.[4]

The first step is to evaluate the threat to the system. Is there a person or organization with the motive and capability to attack this system? The second step is to evaluate if the system is vulnerable to an attack from the identified threat. The last step is to evaluate the critical elements of the system to determine what elements of the system, if attacked, could cause the most loss of life, adverse economic impact, and operational disruptions. This paper advocates that the United States develop a long-range, comprehensive, integrated National Transportation Strategy to simultaneously address security of the systems and the demand to move more people and cargo.

A background on foreign terrorist attacks in the United States and an overview of rail systems are included, as well as an examination of the:

- terrorist threats to the United States and its rail systems;

- vulnerabilities and critical elements of freight railroads and passenger rail systems;

- Department of Defense's (DoD) role in protecting critical rail infrastructure; and

- specific recommendations on what to protect first and how to protect it.

Overview

The September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon have taught another generation of American citizens that the United States is vulnerable to attack by a foreign enemy. Using a weapon as simple as a $7 box cutter, terrorists simultaneously hijacked four commercial jetliners carrying private citizens and thousands of gallons of jet fuel and used them as weapons of mass effect to terrorize America. The terrorists' plans were effective in destroying the two skyscrapers; significantly damaging the Pentagon, the symbol of the U.S. military strength; destroying four aircraft; and killing more than three thousand innocent citizens, the functional equivalent of using cruise missiles. By turning components of the public transportation system into weapons of mass effect in the 9/11 attacks, the terrorists revealed one of the vulnerabilities in the government's ability to protect the homeland, the

U.S. intelligence agencies inabilities to share full information with the Federal Bureau of Investigation and one another, and the airline industry's inability to provide security for its passengers.

The events of 9/11 raised many questions. How could such a catastrophic event happen in two major metropolitan cities of the most powerful nation in the world? What went wrong and why did the government fail to protect the homeland and its citizens? Who could be responsible for such a horrific attack? What type of person purposely seeks to kill thousands of citizens? Are our public transportation systems safe?

To answer many of these questions the President and Congress established the 9/11 Commission. Based on their findings, the Commission made far-reaching recommendations to help prevent another catastrophic terrorist attack from happening in the United States. To date, some of the recommendations have been implemented, but due to the overwhelming scope of the problems, limited progress has been made in many areas dealing with protection of the critical infrastructures. For example, in the *Report on the Status of 9/11 Commission Recommendations* reviewers gave an unsatisfactory rating to United States efforts to date in eliminating vulnerabilities of the national critical infrastructure, as required by Public Law 108-458.[5]

One critical infrastructure is the U.S. transportation system.[6] The focus of this paper will be on the security issues surrounding only the rail portion of transportation. The national objectives for protecting critical infrastructure are: (1) to identify and assure the protection of those assets, systems, and functions that we deem most "critical" in nature, particularly in a national or major regional context; (2) to assure the protection of infrastructures and assets that face a specific, imminent threat; and (3) to pursue collaborative measures and initiatives to assure the protection of other potential targets that may become attractive over time.[7]

Rail Background

Rail systems are classified into two categories. The first is the freight rail system which includes the DoD Strategic Rail Network. Freight systems are privately owned. Seven major railroads own 80 percent of the rail lines and the remaining 20 percent is owned by more than 500 short-

line railroads. The amount of Class I rail lines has steadily decreased since the height of railroad use in the early 1900s. There are approximately 100,000 miles of Class I rail lines crossing the country.[8] Of this amount, DoD classifies 30,000 miles of Class I rail lines as critical to mobility for national defense. The freight railroads are the workhorse for moving large quantities of raw materials long distances. Freight railroads carry 42 percent of intercity freight, including 65 percent of coal shipments, 70 percent of automobile shipments, and 30 percent of grain shipments when compared on a ton/mile basis.[9] The freight network has some redundancy, providing resiliency against critical failure.

The second is the passenger rail system that includes intercity passenger rail (Amtrak) and transit rail which includes commuter rail, heavy-rail (metro, subway, rapid transit, or rapid rail) and light-rail (streetcar, tramway, or trolley).[10] According to *The National Strategy for The Physical Protection of Critical Infrastructure and Key Assets,* about 20 million intercity passengers ride trains annually that travel on the surface and 45 million passengers ride subways each year.[11]

Amtrak operates intercity passenger service on 22,000 miles of rail track but only owns 650 miles of rail track in the profitable northeast commuter corridor.[12] "Amtrak serves over 500 train stations, the majority of which are owned by cities, states, and freight railroads. However, about 135 stations are owned by Amtrak, including Penn Station in New York, which is used by 400,000 [local] commuters and intercity rail customers daily. Amtrak also owns and operates the Northeast Corridor, the most heavily traveled passenger rail corridor in the country, [running] over 1,200 trains per day, including over 1,000 trains operated by commuter authorities."[13] Transit rail systems have 6,800 miles of commuter rail, 1,600 miles of heavy-rail and 1,000 miles of light-rail.[14] Each year public transit serves 9.5 billion passengers (including buses), approximately one-third of these passengers use transit rail systems. On a daily basis, this is greater than the total number of passengers served by air or intercity rail.[15]

II. Threat Assessment

> Defeating terrorism will remain our top objective as widely dispersed terrorist networks present real danger to U.S. national security interest at home and abroad. Our reporting indicates Al Qaeda is intent on finding ways to circumvent U.S. security enhancements to strike Americans and the homeland… Our reporting that Al Qaeda or another group wants to use chemical, biological, radiological, and/or nuclear weapons cannot be ignored.
>
> –Porter J. Goss
> Director of Central Intelligence
> March 17, 2005

Terrorist Threat to the United States

Is there a significant terrorist threat in the United States? In the *National Security Strategy of the United States of America*, the President describes the global war on terrorism as the greatest threat.[16] *The National Defense Strategy of the United States of America* states: "Increasingly sophisticated irregular methods—e.g., terrorism and insurgency—challenge U.S. security interests."[17] The *National Military Strategy of the United States of America* refers to terrorists more than 15 times.

DoD's *Strategy for Homeland Defense and Civil Support* states: "We now confront an enemy who will attempt to engage us not only far from U.S. shores, but also at home. Terrorists will seek to employ asymmetric means to penetrate our defenses and exploit the openness of our society to their advantage. By attacking our citizens, our economic institutions, our physical infrastructure, and our social fabric, they seek to destroy American democracy. We dare not underestimate the devastation that terrorists seek to bring to Americans at home."[18]

The *Homeland Security Presidential Directive-7* says: "Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass

casualties, weaken our economy, and damage public morale and confidence."[19]

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets states: "The September 11, 2001, attacks demonstrated the extent of our vulnerability to the terrorist threat. In the aftermath of these tragic events, we, as a nation, have demonstrated firm resolve in protecting our critical infrastructures and key assets from further terrorist exploitation. In this effort, government at all levels, the private sector, and concerned citizens across the country have begun an important partnership and commitment to action."[20]

In his testimony before the Senate, The Director of the Defense Intelligence Agency stated the threat to the United States.

> The primary threat for the foreseeable future is a network of Islamic extremists hostile to the United States and our interests. The network is transnational and has a broad range of capabilities, to include mass-casualty attacks. The most dangerous and immediate threat is Sunni Islamic terrorists that form the "Al Qaeda associated movement."… We judge [that] terrorist groups, particularly Al Qaeda, remain interested in Chemical, Biological, Radiological and Nuclear (CBRN) weapons. Al Qaeda's stated intention to conduct an attack exceeding the destruction of 9/11 raises the possibility that planned attacks may involve unconventional weapons. There is little doubt it has contemplated using radiological or nuclear material.[21]

The *9/11 Commission Report* portrays the new type of Al Qaeda terrorist by describing Khalid Sheikh Mohammed, the master mind behind the attacks, as intelligent and creative. He had a degree in mechanical engineering from North Carolina Agricultural & Technical State and was equally comfortable in a government office or a terrorist safe-house. He applied his imagination, technical aptitude, and managerial skills and his "wild" ideas for attacks included conventional car bombing, political assassination, aircraft bombing, hijacking, reservoir poisoning, and ultimately, the use of aircrafts as missiles guided by suicide operatives. He began planning an attack that included blowing up 12 U.S. commercial

jumbo jets over the Pacific during a two-day period. This event was stopped by authorities.[22]

According to the *9/11 Commission Report,* Khalid Sheikh Mohammed believed an attack on the U.S. economy would have the best influence on the country's foreign policies. He considered New York and California the financial centers of the United States. His initial 9/11 planning included simultaneous attack of 10 targets with aircraft including the Federal Bureau of Investigation and Central Intelligence Agency headquarters, nuclear power plants, and the tallest buildings in California and Washington State.[23] The report assesses that the final 9/11 targets were selected as follows: Bin Laden selected the White House and Pentagon, Khalid Sheikh Mohammed selected the World Trade Center, and they collectively selected the Capitol.[24]

Even as the United States continues to make significant impacts on terrorist organizations and networks in the global war on terrorism, Al Qaeda's leader, Osama bin Laden, and his deputy, Aymann Al Zawahiri, remain the highest threats to the U.S. homeland. Why is Al Qaeda the major threat to the United States? In his book, *The Crisis of Islam,* Bernard Lewis states the main goal of the new-style terrorist groups is the slaughter of innocent and uninvolved civilians.[25] Al Qaeda is a new-style terrorist organization and Osama bin Laden declared war on the United States in 1996. In 1998, he issued a fatwa against Americans and their allies, which included killing both civilians and military wherever possible. He states in his fatwa that God, not bin Laden, ordered Muslims to kill all Americans.[26] For Al Qaeda, this is a holy war.

Terrorist Threat to Rail Systems

The terrorist endgame includes a complex mix of political, economic, and psychological objectives. To achieve their objectives, terrorists may choose to target critical infrastructures and key assets as low-risk means to generate mass casualties, shock, and panic.

−The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets

Since the 9/11 terrorist attacks on the World Trade Center and the Pentagon, experts have been specifically warning of the vulnerability of critical rail systems to terrorist attack. The Century Foundation Task Force Report lists the security of rail systems, chemical plants and ports receiving shipping containers among the highest priorities to protect.[27] The Rail Security Act of 2004 Report stated: "A terrorist attack on the nation's rail system could cripple freight and commuter transportation. . . . Even the brief service disruptions following the 2001 terrorist attacks caused emergencies for several cities awaiting rail deliveries of chlorine used to purify their water…"[28] The *9/11 Commission Report* warned that "While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime or surface transportation. . . . Surface transportation systems such as railroads and mass transit remain hard to protect because they are so accessible and extensive."[29] Clearly, there are risks associated with rail systems but the question that remains unanswered is, what will the government do to protect them?

Part of the concern is the U.S. Government's lack of emphasis on and funding for the security of rail systems. Essentially, protection of U.S. rail systems have been given a much lower priority than protection of the U.S. airline industry as a result of the impact of the terrorists' acts on the commercial aviation industry. This is reflected in the funding provided by the U.S. Government for security through the Transportation Security Agency.

During the Secretary of Homeland Security's testimony before the Homeland Security Committee, Representative Bennie Thompson (D-MS) pointed out the fact that the Transportation Security Agency focused too much on aviation and had allocated a mere 7 percent of its budget to inspect and patrol rail lines. Representative Thompson felt this was unacceptable and that, if necessary, the Transportation Security Agency should be reorganized to make rail security a higher priority.[30] In addition, the GAO recently reported that funding for aviation security for fiscal years 2005 and 2006 was 87 percent of the Transportation Security Agency's budget.[31] The president of the American Public Transportation Association testified that since 9/11 the industry identified a $6 billion requirement for security enhancements of all systems, they invested $2 billion,

and only received $250 million from the Transportation Security Agency over three years.[32]

Finally, the Federal Transit Administration assessed transit national critical infrastructure as ". . . designed and operated as an open environment—it is by its very nature a high risk, high consequence target for terrorists. More than 9.5 billion passengers a year ride our transit systems. Some of the largest transit systems report that more than 1,000 people a minute enters their largest intermodal facilities during rush hour. Transit subways travel under key government buildings, business centers, and harbors. Worldwide, transit has been a frequent terrorist target, including bombings in the London and Paris subways [and bus lines], the sarin gas attack in Tokyo, and bus bombings in Israel."[33]

Approximately 3 percent of the total gross domestic product, $319 billion, is attributed to freight for-hire transportation services. Of this, rail systems account for approximately $26 billion.[34] The gross domestic product attributed to transportation-related final demand is over $1.1 trillion, about 10.5 percent.[35] In addition, the annual operation expenses for the transit sector exceed $30 billion annually.[36] With such a high potential to affect the economy, it is possible the next terrorist attack in the United States could be on the rail systems.

III. Rail Infrastructure Assessments

> What was demonstrated on September 11 is that transportation systems and assets can be misused by terrorists in ways that can be difficult to anticipate and overlooked in day-to-day efforts to ensure transportation security. . . . Given the size, scope, and ubiquity of the transportation sector, coupled with its myriad owners, operators, and users, many opportunities exist for terrorists to exploit components of transportation systems in novel ways unanticipated by those traditionally responsible for transportation security. . . . Yet terrorists are actively seeking to exploit new threat vectors that lie beyond such conventional perceptions of order.[37]
>
> –Panel on Transportation, Committee on Science
> and Technology for Countering Terrorism, 2002

When considering the vulnerabilities of critical rail systems, the United States must imagine the unthinkable. Terrorists will look for unconventional ways to exploit rail system vulnerabilities similar to the way they exploited the airline industry in the 9/11 attacks. It is important to understand and remember the mind set of Al Qaeda and jihadist supporters. They are willing to sacrifice their lives in the acts to achieve "martyrdom" for their cause. They do not differentiate between military and civilian targets, or between men, women, and children when killing Americans. According to Bin Ladin's fatwas, the more Americans they can kill, the greater their perceived glory.

All rail systems share many of the same vulnerabilities: they are open to hijackings, and there are myriad unsecured rail cars, rail corridors, tunnels, bridges, switch gear, maintenance and storage yards, buildings, parking areas, and power, communication and surveillance systems. Freight systems can operate in a closed network where the railroads have control over the cargo as opposed to passenger systems that rely on an open system. A closed system, similar to the screening process of the airport security, is easier to protect. Once freight is screened by rail security, it remains protected by the railroads until it reaches its destination. Decisions on how

much protection to provide to freight rail should be a reflection of the type and quantity of hazardous materials (HAZMAT) involved. HAZMAT loads should get priority protection. Passenger trains are harder to protect because they require an open system to allow a large number of passengers' quick entry and exit from trains and stations.

All rail systems are vulnerable to failures of other critical infrastructures like the electrical, communications, and water systems. For example, during the August 2003 blackout across the northeast, New York City's 413 subway trains lost power and communication and stranded over 400,000 passengers.[38] It took nearly three hours to evacuate all passengers.[39] In addition, loss of power to over 10,000 traffic signals resulted in instant gridlock on the streets of Manhattan.[40] The resulting pedestrian and vehicular traffic jam in Figure 1 shows the disruption caused by loss of rail service in a major city. On 9/11, a broken water main flooded two major transit tunnels. The pump system used to drain the tunnels was not operational due to the loss of electricity. Loss of power was also an issue for the railroads after hurricane Katrina struck. The railroad workers had to bring in generators to provide power for the signals and switches before they could restart operations.

Figure 1. 59th Street Bridge Crowded with Pedestrians and Vehicles[41]

Freight Rail Vulnerability Assessment

> I understand the complexity of these issues [transportation of hazardous materials], and I know there have been numerous studies on many of these issues. Yet the larger context has changed dramatically. We now face a different security threat not only in transportation, but in all aspects of American life. We have to be willing to meet that changed threat with additional counter-measures, and still find ways to keep our transportation systems the efficient and vital circulation system of our economy. We must therefore judge our security options in a different light than we might have judged them in the past.

> –Norman Y. Mineta
> Secretary of Transportation

Freight rail has three targets that terrorists are most likely to attack. These targets are: (1) the hazardous materials being shipped though densely populated cities, (2) choke points like bridges and tunnels, and (3) the Strategic Rail Network. Freight rail does not offer terrorists large crowds located in close spaces. Typically, a freight train will only have two people on board, the engineer and conductor. Since trains run on fixed rail tracks, they can be easily controlled, if hijacked, to prevent them from being crashed into a building or structure.

Terrorists could attack a freight train hazardous material shipment to release poisonous gas in a populated area to achieve an effect comparable to the use of a chemical weapon. There are numerous ways for a terrorist to attack or derail a freight train carrying hazardous materials to include any of the following methods:

- an improvised explosion device (placed on-board or on tracks);

- shoulder-fired missiles;

- a motorcycle or other vehicle pulling along side to place backpacks containing explosive materials on board;

- a truck bomb at a road crossing or bridge;

- parking a vehicle at the intersection of the rail tracks; or

- running the train at excessive speed during a hijacking.

It has been suggested that a 0.50 caliber assault rifle could penetrate railcar HAZMAT storage tanks releasing poisonous gases.[42] Even with the tightest surveillance and security, it would be difficult to deter or defend against terrorists in these types of attacks.

The American Association of Railroads received high praise for their quick action to address security of freight rail after the 9/11 attacks. They immediately contracted with a private security firm and worked with federal agencies to develop a security plan that includes four threat levels, with corresponding protective actions. They provided employee awareness training and conducted vulnerability assessments.[43] These assessments identified the need for assistance from the National Guard to secure critical assets during heightened states of alert.[44]

In 2003, the Government Accountability Office visited five rail facilities to observe security measures. They found "large facilities had security video cameras, lights, observation towers staffed by railroad personnel that can be used as security lookouts, and fencing along some parts of the facility. . . . all of the facilities we visited could be readily accessed because they are not fenced or fences did not completely separate the facilities from adjacent areas. . ."[45] Both small and large rail facilities had "No Trespassing" signs posted and railroad personnel were on duty part or all day. GAO observed the following:

- there was heavy reliance on the vigilance of employees;

- employees were not required to display identification but provided photo identifications upon request;

- the presence of security guards varied; and

- at intermodal facilities, procedures were in place to check for tampering with the valves of tank cars transporting hazardous materials.[46]

Freight Rail Critical Infrastructure Assessment

Major cities across the United States have significant traffic congestion on rail systems and highways. In a study by the America

Association of State and Highway Transportation Officials, five major rail corridors which were evaluated support commercial freight. These corridors were selected due to the high volumes of freight moved by rail and associated highways. The study showed the systems could not support the projected increased freight over the next 20 years without investment for new infrastructure. The five corridors are described below.

- The first corridor is the I-5 corridor running from California to Washington. It is constrained by the single mountain rail pass east of Bakersfield and the passenger rail traffic between Los Angles and San Diego.[47]

- The second corridor is the east-west connection from Southern California through Chicago to New York which handles most of the intermodal rail traffic between Asia and the Northeast. There has been significant investment to enhance service in this corridor by increasing the number of lines and quality of the terminals but terminals still appears to be the constraint.[48]

- The third corridor is the I-95 eastern corridor from Maine to Florida which runs through the densely developed Mid-Atlantic corridor between New York City and Washington, D.C. The CSX route passes through congestion in northern New Jersey and constricted tunnels under Baltimore, and shares trackage with Amtrak and commuter services (most significantly between Baltimore, Maryland, and Fredericksburg, Virginia).[49]

- The fourth corridor is the single largest rail market in the country, the Powder River Basin corridor, from the low-sulfur coal fields of northeastern Wyoming to power plants throughout the Midwest and South. Traffic is expected to grow as more power plants east of the Mississippi switch to the lower sulfur coal. There are no significant rail capacity constraints.[50]

- The last corridor is the Detroit to Mexico corridor known for connecting the automobile manufacturing facilities and the Texas/Mexico border. Constraints are: limited border crossing points in the Houston, Texas, terminal and the interchanges between the Eastern and Western carriers.[51]

Key nodes to attack can be found in each of the corridors described above, but the northeast corridor appears to the most lucrative target that a terrorist might consider. An attack here would impact the: (1) financial center, New York, (2) federal government, Washington, D.C., and (3) highest concentration of people and U.S. manufacturing. Figure 2 shows the web of Class I rail lines in the United States.

To demonstrate how terrorists could launch a catastrophic attack in the northeast corridor, note a recent accident in Baltimore. In June 2001, a 60-car CSX freight train carrying hazardous materials derailed in the Howard Street Tunnel running through the center of Baltimore. The tunnel is the only freight through-route from the southern states through Washington, D.C., Baltimore, and New York. One end of the tunnel is located near Camden Yards where the Baltimore Orioles play baseball.[52] The derailment, which was an accident but which, in the future, could be duplicated by a terrorist attack, ignited a fire in the tunnel that lasted five days and released hazardous materials (see Figure 3).[53] While no one was harmed, it could have been deadly if the cargo had been chlorine gas.
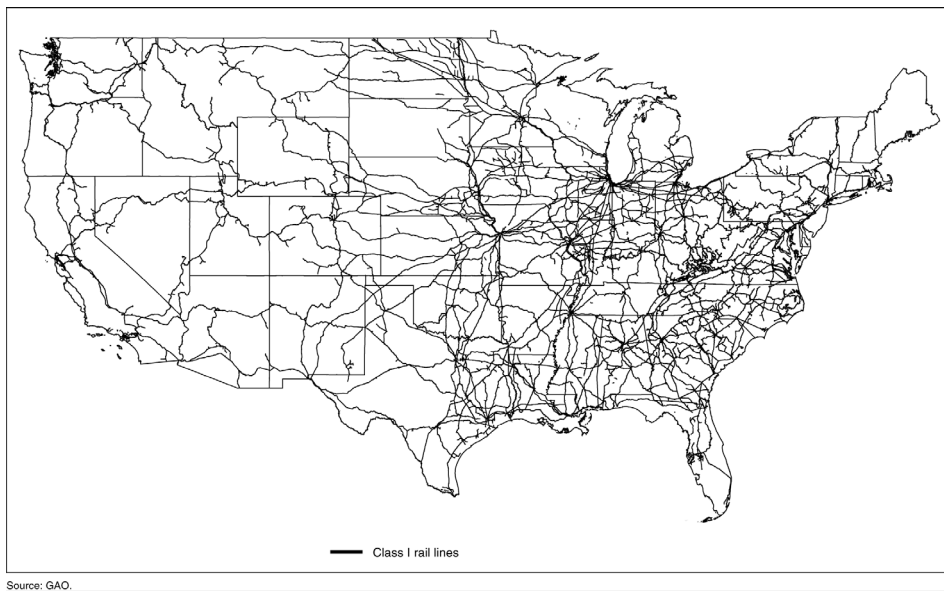
Source: GAO.

Figure 2. Map of Class I Rail Lines[54]

Figure 3. Smoke Billows from Howard Street Tunnel's South Portal, with the Baltimore City Skyline in the Background[55]

Secondary effects included the break of a 40-inch water main running above the tunnel that flooded the local area; loss of the critical fiber optic cable that provided Internet connectivity for the Mid-Atlantic area; road closings shown in Figure 4; closure of light rail commuter systems running along Howard Street above the tunnel; and two cancelled major league baseball games.[56] The 1.7-mile tunnel, built in the 1880s and lacking the most basic fire protection requirements, is an example of obsolete but key infrastructure that badly needs to be replaced.

The Radioactive Waste Management Associates used the Howard Street Tunnel scenario to demonstrate a hypothetical accident involving the shipment of nuclear waste being transported to the national repository at Yucca Mountain, Nevada. They obtained the proposed routes for each state from the Environmental Impact Study on the Yucca Mountain website and used a computer model from the Department of Energy to determine the impact of a severe high-level radioactive waste transport accident. This scenario assumed the protective container failed in the fire. The estimated release of radiation in Baltimore would cost over $10 billion to clean up and cause 115 latent cancer fatalities.[57] However, several

government studies determined the nuclear waste transportation container would not have failed in the fire. The debate over shipping spent nuclear materials through densely populated areas continues. It needs to be readdressed due to the terrorist threat that now exists.
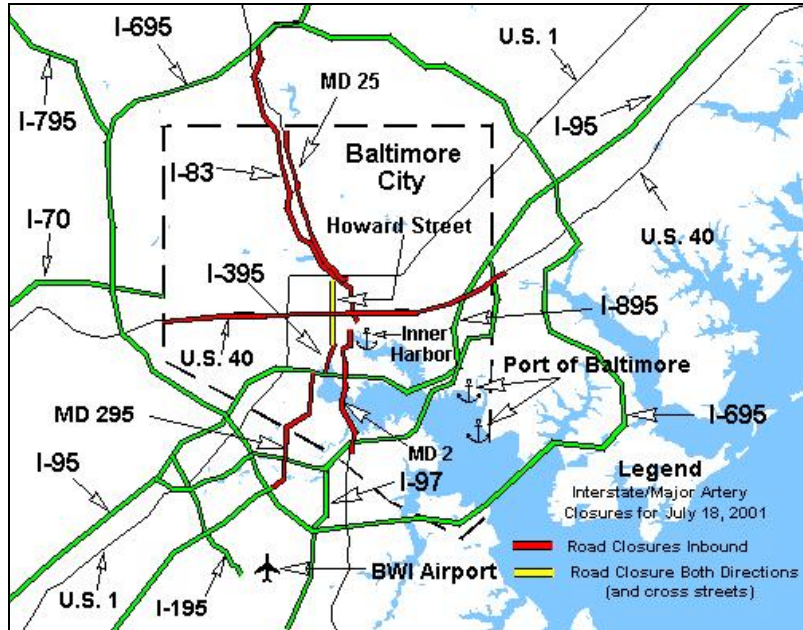
Figure 4. Road Closures into Baltimore City[58]

There are several positions on the criticality of freight rail, the capacity of the system, and its ability to survive a major terrorist attack. In his Senate testimony, Mr. Jack Riley of the RAND Corporation points out both sides of the argument. On one hand, he states concerns about the resilience and robust nature of the freight rail, capacity, the danger of sharing freight lines with passenger trains, and the lack of alternative routes.[59] On the other hand, he states some are more confident that the national transportation infrastructure is resilient against a system-wide attack as compared to a point attack.[60]

A major attack on the freight system would have local and regional impacts but would be unlikely to have a significant economic impact on a national level. The resiliency of the freight rail system was best shown after the 1993 Midwest flood and 2005 Hurricane Katrina. These catastrophic events covered several states but the railroads were able to reroute shipments through other nodes.

According to the Association of American Railroads, "Katrina's damage to rail infrastructure affected six of the seven major railroads and Amtrak. The railroads diverted freight to other routes, going through a number of other gateways, including Memphis, Nashville, Montgomery, St. Louis and Chicago."[61] The worst damage was along the 100-mile line between Pascagoula, Mississippi, and New Orleans, Louisiana.[62] Michael Ward, chairman, president and chief executive officer of CSXT said, "The physical impact to our rail infrastructure, while significant, is confined to a relatively small segment of our 22,000 mile network."[63] Another example is the Howard Street Tunnel derailment in the center of Baltimore. The derailment blocked CSX's only direct route from Florida to New York. The company placed low priority shipments on hold and worked with Norfolk Southern to reroute time sensitive shipments through Harrisburg, Pennsylvania. However, this added up to an extra 36 hours per shipment.

The freight rail systems also support the Railroads for National Defense Program which ensures DoD has strategic rail mobility when it is needed. DoD classifies more than 30,000 miles of commercial rail lines, called the Strategic Rail Network, as critical for strategic mobility and shipments of munitions. The Military Surface Deployment and Distribution Command Transportation Engineering Agency manages the Railroads for National Defense Program and the Strategic Rail Network. They worked with the Federal Railroad Administration, state rail planners, installations, and commercial railroads in developing and coordinating the Strategic Rail Network and Strategic Rail Network connector lines.[64]

In the event of a national emergency, the railroads can give the military first priority to the Strategic Rail Network by restricting shipment of lower priority commercial customers. While Figure 5 shows potential choke points in the system, it also shows the redundancy of the network. If a node or corridor is disrupted, shipments can be rerouted through a different node.
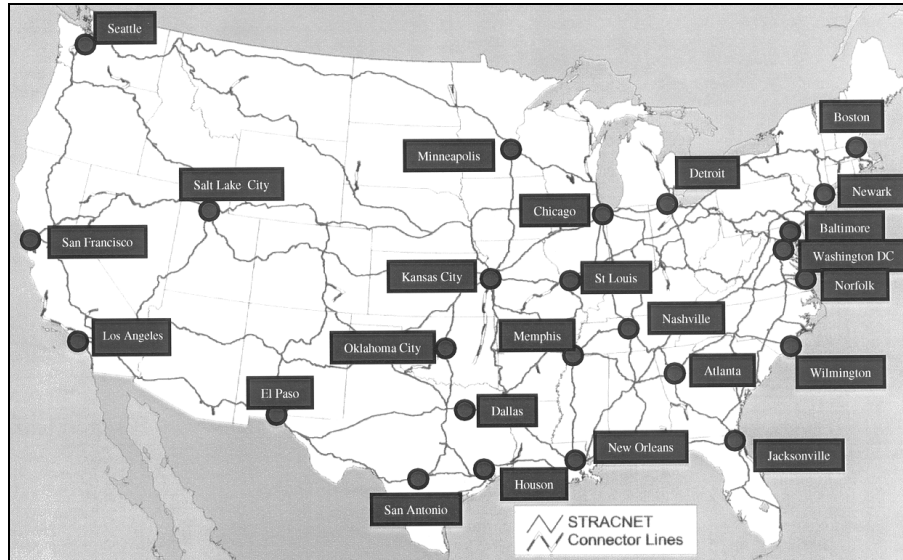
Figure 5. Choke Points in Freight Rail Corridors[65]

An area of concern is the maintenance of the low-density lines that make up one-third of the Strategic Rail Network. The Military Surface Deployment and Distribution Command Transportation Engineering Agency has advocated federal loan legislation to provide funding for the maintenance of these lines.[66]

Passenger Rail Vulnerability Assessment

> We learned about an enemy who is sophisticated, patient, disciplined, and lethal. The enemy rallies broad support in the Arab and Muslim world by demanding redress of political grievances, but its hostility toward us and our values is limitless. Its purpose is to rid the world of religious and political pluralism, the plebiscite, and equal rights for women. It makes no distinction between military and civilian targets. *Collateral damage* is not in its lexicon.
>
> –The 9/11 Commission Report

Of the two rail systems, passenger rail has the highest risk and must be given the highest priority for funding to implement corrective actions. It has the highest threat based on the history of terrorist attacks, the highest vulnerability due to the required open nature of the system, and it is the most critical to the economy since over 50 percent of its passengers are commuting to and from work each day. Its major vulnerabilities are the 3,000 stations, the trains, supporting utilities, location to important business zones and key government buildings, and its workforce. In addition, approximately 20 percent of the transit rail track is elevated or in tunnels which offers an adversary additional targets.[67]

Passenger rail has two categories. Intercity service is the first and is provided by Amtrak. Since nearly the entire rail network Amtrak uses is owned by the freight railroads, Amtrak would receive the benefits of freight rail security enhancements. The only exception is where Amtrak owns the rail infrastructure in the profitable northeast corridor from Washington, D.C., to New York where the U.S. Government has heavily subsidized the ownership costs. Of the 64,000 Amtrak passengers per day, approximately two-thirds use the northeast corridor.[68] Due to the lack of security checks at Amtrak stations, they can provide terrorists entering at the Baltimore-Washington International airport station with luggage easy access to other rail networks in the northeast corridor. However, using Amtrak in a coordinated attack of a train station would be risky due to their historically poor on-time record.[69]

The second category of passenger rail is transit. The American Public Transportation Association estimated that public transportation use increased by 22 percent from 1995 to 2003, an increase in use over highway or air travel.[70] More than 14 million people use public transportation in the United States and take more than 31 million trips each weekday, of which 11 million trips are by rail.[71] According to American Public Transportation Association data, the reasons passengers use transit systems are: work (54 percent), schools (15 percent), shopping and social visits (9 percent each), and medical appointments (5 percent).[72] Based on these usage numbers, loss of public transportation would significantly affect the local economy and possibly the nation if the largest systems were simultaneous attacked.

The recent terrorist bombings of rail systems in Madrid and London have increased the concern of a similar attack in the United States. Could

such an attack happen here? An attempt was made in 1997; police stopped Islamic extremists who were planning to bomb New York City's subways.[73]

For rail systems, the primary terrorist targets are where the greatest casualties could occur and such rail attacks have been nearly twice as lethal as terrorist attacks overall.[74] The vulnerability of transit stations is due to the large number of passengers that congregate there, the lack of screening of packages for weapons, and the easy access of such sites for terrorists. Rail stations are most vulnerable at rush hour when trains are packed full of riders. The most vulnerable stations are where the largest number of rail lines intersects. Historically 50 percent of the attacks on transit systems have been on rail, and 50 percent of these attacks have been by exploding conventional bombs.[75] "Terrorists tend to carry out their attacks in nearby, familiar surroundings, . . . within an hour's drive of the terrorist's home, . . . [and] 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 Angles."[76] For example, Penn Station in New York and Union Station and Metro Center in Washington, D.C. would be considered especially vulnerable high-value targets due to their high passenger movement.

New York City has the largest transit system in the United States and with its reputation for being the U.S. financial capital, should be considered at the top of the list for a terrorist attack on a passenger rail system. The Washington, D.C., metropolitan area, with the largest concentration of U.S. Government buildings and as the home of the White House, Capitol, and Pentagon, should also be considered a top target on the list for a terrorist attack. The *9/11 Commission Report* concluded that Al Qaeda's leadership believes these two cities are the highest priority targets for these reasons. It also concluded that terrorists are persistent since they waited eight years for a second attack on the World Trade Center but had not given up on that target. Since terrorists have previously attacked these cities, it may be only a matter of time before they try again. Defense of other U.S. cities should be prioritized based on population density, passenger loads, direct access to rail from commercial airports, and the previous history of such terrorist attacks.

Passenger Rail Critical Infrastructure Assessment

Intercity passenger service provided by Amtrak should be considered a lower priority due to its small market share of passengers across most of the country. Only five routes in the northeast have a market share greater then 30 percent. The Amtrak network is less robust than the freight system and has fewer alternatives for rerouting train service in the event of a failure at a critical node (see Figure 6). The Amtrak network appears to have two critical choke points or nodes in their east-west network at Chicago and New Orleans. However, it is doubtful that a simultaneous attack on these nodes would negatively affect Amtrak's operating revenue since their highest revenue routes are in the northeast corridor.
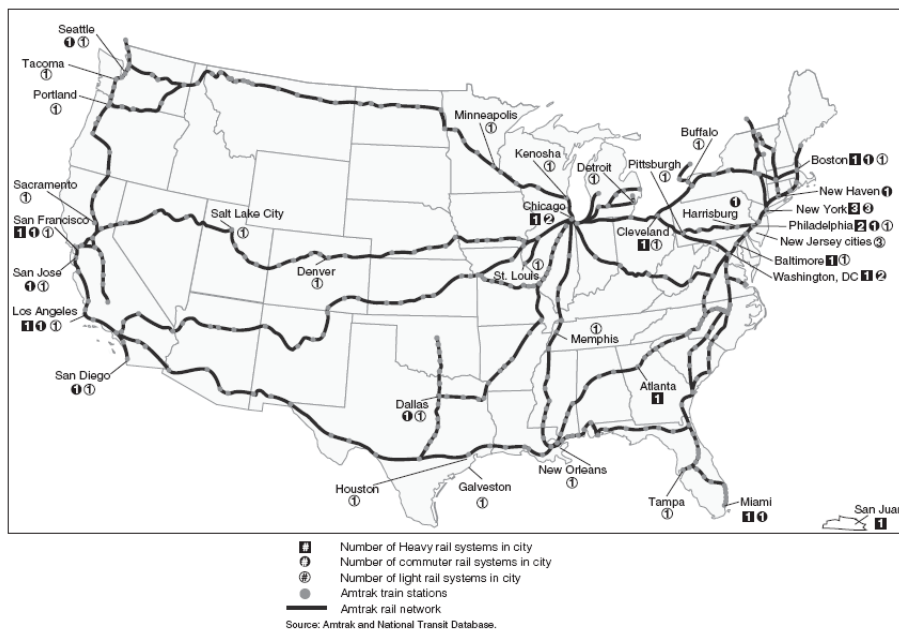

Figure 6. Geographic Distribution of Amtrak and Rail Transit Systems[77]

Transit systems have proven to be critical assets in responding to and recovering from a major terrorist attack. Rod Diridon Sr., the Executive Director of Mineta Transportation Institute, best described the transit

system in their review of the 9/11 attacks. "What emerged from this investigation was a clear sense that public transit agencies were the unsung heroes of the 9/11 attacks. From their role in saving passengers' lives and evacuating Lower Manhattan to delivering rescue workers and heavy equipment to Ground Zero and providing communications capacity, the transit agencies played a vital role in rescue and recovery work. Heroic efforts resulted in system repairs and the establishment of new service in fractions of the usual required time, greatly assisting New York's economic recovery."[78]

For transit rail, the simultaneous bombing of several critical transit stations would disrupt, if not eliminate, service and would have a high potential for mass casualties. A good example is in the Washington, D.C., metropolitan area where there is limited redundancy in the rail systems. There are four stations in Washington, D.C., where three rail lines intersect and these would be considered the most critical targets. The next critical are the seven stations where two lines intersect. The subway network in Washington, D.C., is made of the Blue, Red, Yellow, Green, and Orange lines. The Virginia Railway Express commuter train operates the Manassas and Fredericksburg lines. The key target for the Virginia Railway Express trains is Union Station where its two lines meet Amtrak lines, MARC lines, and Metro's Red line.

Also, a simultaneous attack on five en-route commuter stations could have promise for a high body count and would have the most potential to disrupt commuters. These stations are:

- Pentagon City, which is always a busy station due to the adjacent shopping mall, where the Blue and Yellow lines share a station;

- Rosslyn, where the Blue and Orange lines share a station;

- Fort Totten, where the Green and Red lines share a station;

- Stadium-Armory, where the Blue and Orange lines share a station; and

- Virginia Railway Express Crystal City station where the Fredericksburg and Manassas lines share a station.

The Metro's Yellow and Blue lines stop at Reagan International Airport station in Virginia and Amtrak stops at Baltimore-Washington

International Airport station in Baltimore. A group of terrorists could get on the subway and Amtrak at these stops with medium sized pull-behind luggage without drawing any attention. A simultaneous attack, with multiple bombers and larger quantities of explosives hauled in luggage, would be more devastating than the coordinated attacks in Madrid. By using medium size luggage to conceal their explosives, they could easily do much more damage per bomb than the London bombings where backpacks where used to conceal weapons. This type of attack could temporarily paralyze Washington's rail services.

IV. DoD's Role in Protecting Critical Rail Infrastructure

DoD's involvement in Homeland Security is identified through the:

- National Security Strategy;

- National Strategy for Homeland Security;

- National Defense Strategy;

- National Military Strategy;

- Strategy for Homeland Defense and Civil Support;

- The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets; and

- Joint Publication, 3-26, Homeland Security.

DoD's role in protecting rail systems is part of their overall mission to protect defense critical infrastructure and national critical infrastructure.

The purpose of the Defense Critical Infrastructure Program is to ensure availability of critical defense assets through risk management. DoD agencies have two roles in Defense Critical Infrastructure Program. The first is to conduct risk management assessments of the rail infrastructure on the installation and to identify, remediate, or mitigate the risks. This program complements other programs that protect the installation assets like the antiterrorism, force protection, continuity assessment, and installation preparedness programs.[79] Risk management evaluates and prioritizes assets based on the potential threats, vulnerabilities and critical value. To remediate or mitigate the risks, DoD can change the operation of the systems, change physical security, or both.

The Department of Defense's second role is to identify and communicate defense mobility requirements to the appropriate federal, state, and local agencies and the local railroad providers. The Military Surface Deployment and Distribution Command Transportation Engineering Agency is responsible for the Railroads for National Defense Program and serves as DoD's liaison for civil rail carriers and state rail authorities.[80] They communicate the requirements for the Defense Critical

Infrastructure Program for rail systems through the Railroads for National Defense Program on behalf of the Commander of the U.S. Transportation Command to the Federal Railroad Administration. The local installation is responsible for working with the state and local governments and the railroads. They typically do this with a memorandum of agreement for mutual support during a crisis.

DoD's role in protecting national critical rail infrastructure is limited since the primary responsibility belongs to other federal, state, and local agencies and private rail companies. However, the Association of American Railroads testified before the U.S. Senate that the National Guard would be needed to secure critical assets during heightened states of alert.[81] The Posse Comitatus Act prohibits the National Guard in Title 10 status under the control of the President from performing law enforcement duties.[82] Therefore, this support would be best provided by the National Guard in Title 32 status under the control of state governors so they can perform law enforcement duties.

The Department of Defense also has the role of providing civil support to other federal agencies and private sectors when directed by the President of the United States or Secretary of Defense. The *Strategy for Homeland Defense and Civil Support* describes DoD's roles and responsibilities in protecting critical infrastructure:

- U.S. Northern Command (NORTHCOM) and U.S. Pacific Command (PACOM) are designated the lead DoD agencies for protecting defense critical infrastructure and national critical infrastructure in the continental U.S. and Hawaii respectively.

- Installation commanders are responsible for protecting the defense critical infrastructure on military installations.

- Joint Force Headquarters - National Capital Region has a key role in the National Capital Region. Their role is to work with the state, local governments, and the owners of the private rail systems to prevent and prepare an attack.

- Joint Task Force - Civil Support will provide integrated DoD support to the designated lead federal agencies for domestic Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) consequence management. When required, the Secretary

of Defense directs deployment of the Joint Task Force - Civil Support to CBRNE incident sites through NORTHCOM's commander. The Joint Task Force - Civil Support role is to establish command and control for DoD forces and provide civilian support.

- The National Guard Weapons of Mass Destruction - Civil Support Teams operating under state status will likely be the first military responder to a chemical, biological, radiological, nuclear, or high-yield explosives (CBRNE) incident site.[83]

The Military Surface Deployment and Distribution Command Transportation Engineering Agency developed and manages a key rail information asset for DoD, the Intelligent Road/Railroad Information Server web-based tool. According to the Intelligent Road/Railroad Information Server White Paper, Intelligent Road/Railroad Information Server (IRRIS) "technology integrates transportation logistics, real-time tracking, and infrastructure data into a single, secure application [computer program] accessible through the Internet. With real-time and relevant information about road conditions, construction [sites], incidents [accidents, attack or system failure], and weather [conditions] from more than 150 worldwide data sets, IRRIS technology enables SDDCTEA [Military Surface Deployment and Distribution Command Transportation Engineering Agency] to visualize assets and perform spatial queries and analysis, such as plume modeling to depict the effects of hazardous materials and/or explosives on any geographic area. . . . It uses the latest Web[-based] geographic information systems (GIS), intelligent transportation systems, location-based services, wireless technologies, and global positioning systems to provide support for effective logistics, emergency response, and management."[84]

Figure 7. Intelligent Road/Railroad Information Server Plume Modeling[85]

Figure 7 shows an example of the Intelligent Road/Railroad Information Server plume modeling. For example, Military Surface Deployment and Distribution Command Transportation Engineering Agency used the Intelligent Road/Railroad Information Server to assist the U.S. Department of Transportation, U.S. Northern Command, and Federal Emergency Management Agency during the Hurricane Ivan evacuation in 2004.[86]

V. Recommendations

Protect the Transit Rail Stations in Metropolitan Areas

Based on the analysis above, the assets at highest risk in the rail transportation system are the transit stations in major metropolitan areas. This is based on the history of terrorist attacks on rail systems, the vulnerability of the stations due to their open nature, the large crowds that gather at them offering the potential for mass casualties, and the criticality of the rail system to the U.S. economy. In addition, passenger railroad trains with access to an airport present an opportunity for a terrorist to use a large bomb, since it is common for riders to carry their luggage to and from the airlines and the nearby rail systems. High capacity sensors for detection of conventional explosives, chemicals, and biological agents are needed to protect these systems.

Protect Hazardous Material Carriers

The second highest risk target in the rail system is when hazardous materials are transported by freight railroads through densely populated areas. This assessment is based on the understanding that an attack on trains carrying hazardous materials in the middle of a city could inflict a significant loss of life, and create significant economic disruption. This is also a major risk due to the vulnerability of the unsecured maintenance and transfer yards, the vulnerability of trains to attack when approaching choke points like tunnels and bridges, and the criticality of the bridges and tunnels in the network. The railroad executives very much need to continue to work to secure the perimeter of maintenance and transfer yards, bridges, and tunnels in order to reduce this risk.

Protect Passenger Trains/Stations

The next highest risk is to the passenger intercity rail system. Like intra-city transit systems, intercity rail requires an open system to allow easy movement of a high volume of passengers onto and out of the trains. In addition, it provides an easy access point for terrorists wishing to attack

stations shared with transit rail. Probably no significant investments in security upgrades should be made until the United States develops a long-range integrated strategy for protecting intercity passenger rail service but this should be done as soon as possible. However, before the government invests in security upgrades for Amtrak, the bigger question that must be answered is "What is the future for Amtrak and intercity passenger service? And, how does it dovetail with all air-ground-sea transportation plans and needs?" This question is outside the scope of this paper; however, it is important and warrants attention.

Required Actions to Protect High Risk Rail Infrastructure

First, the U.S. Government must invest in automated security technology to ensure a 24/7 security blanket is in place at transit stations. Technology such as surveillance cameras and sensors can reduce the financial burden of personnel costs during times of elevated security across the country. Under the current system, every time there is a threat of a possible terrorist attack, increased surveillance costs millions of dollars in personnel overtime. The U.S. Government must take the lead to accelerate development, testing, and implementation of high capacity scanners for conventional explosives, chemical agents, and biological agents. Much research and development work and acquisition funding will be required before a practical security system is feasible.

Second, the U.S. Government needs to address the transportation of hazardous materials through densely populated areas. State and local governments do not have the authority to restrict passage since this involves interstate transportation of goods. Therefore, the U.S. Government needs to provide funding or incentives for the freight railroads to relocate rail lines carrying hazardous materials away from densely populated areas with critical choke points like the Howard Street Tunnel in Baltimore. In addition, shipment of hazardous materials either should never be routed through major population centers or should at least be restricted in densely populated areas or through critical nodes during high threat levels. As a minimum, the U.S. Government needs to require freight railroads to notify local governments when transporting hazardous materials to allow these communities the opportunity to provide additional security.

Third, federal and state governments need to develop and publish standards for prioritizing what is defended and then should oversee the vulnerability assessments of critical assets to ensure consistency. Lack of sufficient funding is the number one issue preventing transit organizations from implementing security enhancements and they are looking to the federal government for that funding.[87] Before the federal government invests tax dollars or provides tax incentives to make security improvements, standards for risk assessments and levels of security need to be established. Several standard and risk assessment models exist that can be used to ensure comparable results. For example, the Federal Highway Administration's *Recommendations for Bridge and Tunnel Security* provides an assessment guide that could be applied across all transportation systems.[88] The Federal Transit Agency's *Transit Security Design Considerations* provides guidance on incorporating security measures into transit projects.[89]

The GAO recommends systematic planning to optimize resources. For example, they found that the Transportation Security Agency acted promptly to meet the Congressional mandate to screen 100 percent of the luggage on commercial airlines for explosives, but they did not always use a risk assessment process to determine priorities and requirements. This led to 7,000 explosive scanners being installed in airport lobbies rather than being incorporated into the airport baggage conveyor system. Since these systems were not engineered into the screening process, the net result was an operational inefficiency and a requirement for additional screeners. The Transportation Security Agency is now working with nine airports to correct the oversight. Once implemented, this initiative will reduce the number of screeners and supervisors by 78 percent and save the government $1.3 billion over 7 years.[90] Procedures need to be developed for screening passengers and luggage boarding trains and similar approaches to this would avoid many future problems if things are done systematically. The rail industry should learn from the airline industry's experiences with security screening and avoid making the same costly mistakes.

Fourth, the top priority for freight railroads is the physical security of transfer and maintenance yards. This can be accomplished by securing the perimeter and controlling entry. The U.S. military uses a layered approach in force protection, which could easily be followed by the freight

railroads. The ultimate goal is to minimize mass casualties. Securing the perimeter of the installation defends against threats like car and truck bombs. Controlling the access at a limited number of manned gates could help ensure that authorized personnel and visitors are allowed in terminals and trains. The second layer of protection inside the perimeter is to ensure a proper standoff distance is maintained by not allowing vehicles to park within 25 meters of a rail facility or train. The freight railroads and Association of American Railroads, like U.S. military installations, set the standard for taking decisive action to secure their sector after the attacks of 9/11. However, a GAO visit to several stations showed that the rail companies need to secure the perimeter of the rail and in-route storage yards and control access to them. It is the same for railroad companies as for U.S. military installations; they need to be vigilant and provide security to their critical assets.

Finally, United States Congress needs to establish and approve a long-range strategy addressing all modes of transportation. At a strategic level, it is easy to argue rail systems should be viewed as national assets in the same manner as the airports, airport security, and federal highways. The federal and state governments need to develop a near-term transportation plan for 2007 and a long-range National Transportation Strategy to provide a vision for the year 2030. This strategy needs to address transportation security issues; protection of intercity passenger rail service; defending freight transportation; providing security of air, rail, and highway systems; and increasing railroad capacity to handle the projected 57 percent increase in freight by 2020.[91]   There are two supporting reasons why a National Transportation Strategy is needed:

- The first reason is discussed in Mr. Jenkins paper, *Improving Public Surface Transportation Security: What Do We Do Now?* He recommends the government develop a transportation system security strategy that focuses on: "preventing the loss of life; minimizing long-term risks to heath; and limiting social upheaval, . . . environmental catastrophe and economic disruption."[92] He suggests: "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."[93]

- The second reason is the amount of money the federal government has spent to keep Amtrak in business that could have been used to fund transportation security. The federal government has spent $21.3 billion for Amtrak from fiscal years 1976 to 2003.[94] GAO recently reported that it has cost the federal government $1 billion annually over the last five years to keep Amtrak operating. Plus, Amtrak says it will need $2 billion annually for operations and deferred maintenance, plus an estimated $70 billion over the next 20 years to expand the high speed passenger rail network.[95] GAO recommended Congress consider developing a system-wide approach to transportation, as opposed to a focusing on one mode or type of travel. This type of approach may significantly change funding for Amtrak.

VI. Summary

This paper has provided a background on foreign terrorist attacks in the United States and an overview of rail systems. Then, it examined the:

- terrorist threats to the United States and its rail systems;

- vulnerabilities and critical elements of freight railroads and passenger rail systems;

- The Department of Defense role in protecting critical rail infrastructure; and

- specific recommendations on what to protect first and how to protect it.

This paper used risk management to prioritize what rail systems to protect first and how to go about protecting them. The first step evaluated the threat to the system. The second step evaluated if the system is vulnerable to an attack from the identified threat. The last step evaluated the critical elements of the system.

Critical Rail Infrastructure Assessment

The first question answered is why the United States needs to augment protection of rail systems. Key reasons for protecting rail systems are:

- Passenger rail systems provide terrorists easy access to 45 million passengers riding subways and 20 million passengers riding trains annually. The recent terrorists' bombings of trains in Madrid and London killed 247 and injured 2,200.

- Railroads provide terrorists easy access to disrupt 42 percent of all intercity freight, including 65 percent of coal shipments, 70 percent of automobiles, and 30 percent of all grain on a ton-mile basis.

- A thoughtful study, *The Century Foundation Task Force Report,* says rail systems are highly vulnerable and should be one of the

highest priorities for funding to reduce those vulnerabilities and improve security.[96]

- The *9/11 Commission Report* says terrorists could follow trends around the world to target U.S. surface transportation and the opportunities to do harm are as great, or greater, for rail systems than aviation.

Threat Assessment. Terrorists' threats are real, as evidenced by the number of terrorist attacks around the world. Michael Jenkins says terrorist attacks of rail systems are nothing new and that trains, subways and buses are ideal targets for terrorists willing to kill in quantity indiscriminately. The top threats are:

- A terrorist chemical, biological, radiological, or nuclear attack. These are potentially the most dangerous threats, but a conventional bomb is historically the weapon of choice.

- Al Qaeda and its associated jihadist groups. They are willing to kill innocent American citizens, and are very capable of executing a major attack as demonstrated by 9/11. Their operatives are smart and have demonstrated a "wild" imagination for developing unthinkable types of attack. They are persistent and patient, careful in the protection and willing to wait years to attack a key target a second time.

Vulnerability Assessment. Railroads took immediate action to secure freight rail after 9/11 but deficiencies in basic items like fencing and access control were observed at sites visited by GAO in 2003. Those managing intercity and transit passenger rail lines have not achieved the same success in securing their assets as have those directing freight railroads or commercial aviation and security improvements are required.

- The vulnerability of transit stations is due to the large number of passengers that congregate there, the lack of screening of packages for weapons, and the easy access of such sites for terrorists.

- Freight rail has three targets terrorists are most likely to attack. These targets are: (1) the hazardous materials being shipped though densely populated cities, (2) choke points like bridges and tunnels, and (3) the Strategic Rail Network.

- Rail systems are vulnerable to an attack on supporting utilities like power systems.

Critical Assessment. The 1993 Midwest flood and 2005 Hurricane Katrina showed the resiliency of the U.S. freight rail system. These catastrophic events covered several states but the railroads were able to reroute shipments through other nodes. The importance of passenger rail was demonstrated by their involvement in the response to and recovery from the attacks on the World Trade Center.

- For transit rail, the simultaneous bombing of several critical transit stations would disrupt, if not eliminate, service and would have a high potential for mass casualties. The most critical stations are where the largest number of rail lines intersect.

- For freight rail, the northeast corridor appears to the most lucrative target that a terrorist might consider. An attack here would impact the: (1) economic center, New York; (2) federal government, Washington, D.C.; and (3) highest concentration of people and U.S. manufacturing.

- In the event of a national emergency, the railroads can restrict shipments of lower priority commercial customers to ensure that the Strategic Rail Network is available to support critical mobility for national defense.

What Assets to Protect First and How to Protect Them

Passenger rail is most at risk and must be given the highest funding priority to implement corrective actions. To demonstrate that this part of the system is most endangered, one need only look at the recent history of terrorist attacks, note that it has the highest vulnerability due to the required open nature of the system, and understand that it is most critical to the economy since over 50 percent of its passengers are commuting to and from work each day. The priority for protecting critical rail infrastructure is:

1. Transit rail stations in big cities. New York City and Washington, D.C. are on the top of the list since terrorists attacked these cities

on 9/11. Defense of other U.S. cities should be prioritized based on population density, passenger loads, direct access to rail from commercial airports, and the previous history of such terrorist attacks.

2. Hazardous materials shipped by railroad through major cities.

3. Inter-city passenger rail stations and trains.

Five major actions should be taken to protect critical rail systems.

1. The U.S. Government must invest in automated security technology to ensure a 24/7 security blanket is in place at transit stations. They should take the lead to accelerate development, testing, and implementation of high capacity scanners for conventional explosives, chemical agents, and biological agents.

2. The U.S. Government needs to address the transportation of hazardous materials through high population density areas. They need to provide funding or incentives for the freight railroads to relocate rail lines carrying hazardous materials away from densely populated areas with critical choke points.

3. Federal and state governments need to publish standards for prioritizing what rail assets to defend, oversee the vulnerability assessments of these assets to ensure consistency in results, and develop procedures for screening passengers and luggage boarding trains.

4. The top priority for freight railroads is the physical security of transfer (in-transit) and maintenance yards. They can accomplish this by securing the perimeter and controlling entry.

5. The U.S. Congress needs to approve a long-range strategy addressing all modes of transportation. This strategy needs to address transportation security issues; protection of intercity passenger rail service; defending freight transportation; providing security of air, rail, and highway systems; and increasing railroad capacity to handle the projected 57 percent increase in freight predicted by 2020. It should also address whether the federal government would provide intercity passenger rail service or if this service could be provided by commercial companies.

DoD's Role in Protecting Critical Rail Infrastructure

DoD's role in protecting rail systems is limited to primarily ensuring that the vulnerabilities of rail systems owned and controlled by DoD are identified and prioritized for funding based on their value and the degree of risk posed to them. DoD works through the Railroads for National Defense Program with the owners of the off-base portions of the rail systems to ensure: (1) vulnerabilities are identified and prioritized for funding based on risk and (2) contingency plans are developed for high threat levels when issued by the Department of Homeland Security.

The United States has been fortunate it has not suffered a major rail attack but it is most likely only a matter of time before terrorists attempt one. Quick, decisive, protective action is required to prevent attacks like the train bombings in London and Madrid.

Notes

1. Graniteville train disaster, From Wikipedia, the free encyclopedia, On-line, Internet, available from http://en.wikipedia.org/wiki/Graniteville_train_disaster.

2. Glendale train crash, From Wikipedia, the free encyclopedia, On-line, Internet, available from http://en.wikipedia.org/wiki/Glendale_train_crash.

3. Peter F. Guerrero, *Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain, GAO-04-598T*, (Washington, D.C.: Government Accountability Office, 2003), 16, On-line, Internet, available from www.gao.gov/cgi-bin/getrpt?GAO-04-598T.

4. Ibid.

5. Thomas H. Kean, Lee H. Hamilton, Richard Ben-Veniste, Fred F. Fielding, Jamie S. Gorelick, Slade Gorton, Bob Kerrey, John F. Lehman, Timothy J. Roemer, and James R. Thompson "Report on the Status of 9/11 Commission Recommendations, Part I: Homeland Security, Emergency Preparedness and Response," *9/11 Public Disclosure Project.org*, 4, On-line, Internet, 3 December 2005, available from http://www.9-11pdp.org/press/2005-09-14_report.pdf.

6. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, (Washington, D.C.: Government Printing Office, 2005), 6.

7. Ibid., vii.

8. United States Department of Transportation, *National Transportation Statistics, 2005*, (Washington, D.C.: Research and Innovative Technology Administration, Bureau of Transportation Statistics, Summer 2005), Table 1-1, On-line, Internet, available from http://www.bts.gov/publications/national_transportation_statistics/2005.

9. Senate Committee on Commerce, Science, and Transportation, *Rail Security Act of 2004 Report on S. 2273,* 108th Congress, 2d session, Report 108-536, 2004, On-line, Internet, 3 December 2005, available from http://www.globalsecurity.org/security/library/congress/2004_r/srept108-536.htm.

10. Damian Danchenko, *Public Transportation Fact Book March 2005*, (Washington, D.C.: American Public Transportation Association, 2005), 82, On-line, Internet, available from http://www.apta.com/research/stats/factbook/documents/rail.pdf.

11. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* 56.

12. Cathleen Berrick and JayEtta Hecker, *PASSENGER RAIL SECURITY: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts, GAO-05-851* (Washington, D.C.: GAO, 2005), 8, On-line, Internet, available from www.gao.gov/cgi-bin/getrpt?GAO-05-851.

13. Senate Committee on Commerce, Science, and Transportation.

14. United States Department of Transportation, *National Transportation Statistics, 2005,* Table 1-1.

15. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 61.

16. *The National Security Strategy of the United States of America,* (Washington, D.C.: Office of the President, 2002), 2 (letter), On-line, Internet, available from http://www.globalsecurity.org/military/library/policy/national/nss-020920.htm.

17. Department of Defense, *The National Defense Strategy of the United States of America,* (Washington, D.C.: Office of the Under Secretary of Defense Policy, 2005), 3, On-line, Internet, available from http://www.globalsecurity.org/military/library/policy/ DOD/index.html.

18. Department of Defense, *Strategy for Homeland Defense and Civil Support*, (Washington, DC: Office of the Assistant Secretary of Defense for Policy, June 2005), 1, On-line, Internet, available from http://www.globalsecurity.org/security/library/policy/ DOD/d20050630homeland.pdf.

19. *Homeland Security Presidential Directive/Hspd-7, Critical Infrastructure Identification, Prioritization, and Protection,* (Washington, DC: Government Printing Office, 2003), 1, On-line, Internet, available from http://www.au.af.mil/au/awc/awcgate/ whitehouse/20031217-5.htm.

20. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 1 (letter).

21. U.S. Senate Armed Services Committee, *Current and Projected National Security Threats to the United States, Vice Admiral Lowell E. Jacoby, United States Navy, Director, Defense Intelligence Agency, Statement For the Record, 17 March 2005,* On-line, Internet, available from http://www.globalsecurity.org/intell/library/congress/ 2005_hr/050317-jacoby.htm.

22. Thomas H. Kean, Lee H. Hamilton, Richard Ben-Veniste, Fred F. Fielding, Jamie S. Gorelick, Slade Gorton, Bob Kerrey, John F. Lehman, Timothy J. Roemer, and James R. Thompson, *9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States,* (New York: W.W. Norton, 2004), 145-150.

23. Ibid., 145-153.

24. Ibid.

25. Bernard Lewis, *The Crisis of Islam: Holy War and Unholy Terror,* (New York: Random House, 2003), 147.

26. Jerrod M. Post, "Killing In The Name Of God: Osama Bin Laden And Al Qaeda" in *Know They Enemy; Profiles of Adversary Leaders and Their Strategic Cultures,* Edited by Barry R. Schneider and Jerrold M. Post (Maxwell AFB, AL: USAF Counterproliferation Center, July 2003), 24.

27. Richard A. Clarke, et al., *Defeating the Jihadists: A Blueprint for Action,* (New York: The Century Foundation Press, 2003), 7.

28. Senate Committee on Commerce, Science, and Transportation.

29. *9/11 Commission Report*, 391.

30. Bennie G. Thompson, *Testimony of Secretary of Homeland Security, Michael Chertoff Before the House Committee on Homeland Security*, Press Release, 14 July 2005, On-line, Internet, 3 December 2005, available from http://www.dhs.gov/dhspublic/display?theme=45&content=4630.

31. Cathleen A. Berrick, David Alexander, Chan My J Battcher, Seto J. Bagdoyan, J. Michael Bollinger, Lisa Brown, Kevin Copping, Christine Fossett, John Hansen, Adam Hoffman, Christopher M. Jones, Christopher Keisling, Noel Lance, Thomas Lombardi, Lisa Shibata, and Maria Strudwick, *Transportation Security: Systematic Planning Needed to Optimize Resources, GAO05-357T,* (Washington, D.C.: GAO, 2005), 6-7.

32. William W. Millar, *The London Bombings: Protecting Civilian Targets from Terrorists Attacks (House Homeland Security Committee, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity*, (Washington, D.C.: American Public Transportation Association, 2005), On-line, Internet, available from http://www.apta.com/government_affairs/aptatest/.

33. Federal Transit Administration, "Briefing: Update on the Status of FTA Security Initiatives," Transit: Critical National Infrastructure, On-line, Internet, 3 December 2005, available from http://transit-safety.volpe.dot.gov/security/.

34. United States Department of Transportation, *National Transportation Statistics,* 2005, Table 3.1a.

35. Ibid., Table 3.2a.

36. Ibid., Appendix A.

37. William Schneider, Jr., Special Report 270, *Deterrence, Protection, and Preparation The New Transportation Security Imperative,* (Washington, D.C.: Transportation Research Board of the National Academies, 2002), 6-7, On-line, Internet, available from http://Gulliver.Trb.Org/Publications/Sr/Sr270.Pdf.

38. Allan J. DeBlasio, Terrance J. Regan, Margaret E. Zirker, Katherine S. Fichter, Kristin Lovejoy, *Effects of Catastrophic Events on Transportation System Management and Operations August 2003 Northeast Blackout New York City*, (Washington, D.C.: U.S. Department of Transportation, 2004), 7, On-line, Internet, available from http://www.itsdocs.fhwa.dot.gov//JPODOCS/REPTS_TE//14023.html.

39. Ibid.

40. Ibid.

41. Ibid., 11.

42. Public Citizen, "Bush Administration Leaves Chemical and Nuclear Plants, HazMat, Ports and Water Systems Vulnerable to Terrorists," 18 October 2004, On-line, Internet, available from http://www.citizen.org/pressroom/release.cfm?ID=1808.

43. Senate Committee on Commerce, Science, and Transportation.

44. Ibid.

45. Peter F. Guerrero, *Rail Safety and Security Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed, GAO-03-435*, (Washington, D.C.: GAO, 2003), 18-19, On-line, Internet, available from http://www.gao.gov/new.items/ d03435.pdf.

46. Ibid.

47. John Horsley, *Transportation Invest in America, Freight Rail Bottom Line Report*, (Washington, D.C.: American Association of State Highway and Transportation Officials, 2002), 68.

48. Ibid., 69.

49. Ibid., 69-70.

50. Ibid., 70.

51. Ibid., 71.

52. Mark R. Carter, Mark P. Howard, Nicholas Owens, David Register, Jason Kennedy, Kelley Pecheux, and Aaron Newton, *Effects Of Catastrophic Events On Transportation System Management and Operations, Howard Street Tunnel Fire Baltimore City, Maryland July 18, 2001 Findings*, (Washington, D.C.: Intelligent Transportation Systems United States Department of Transportation, 2002), On-line, Internet, 3 December 2005, available from http://www.itsdocs.fhwa.dot.gov/ JPODOCS/REPTS_TE/13754.html.

53. Ibid.

54. Guerrero, *Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain*, 9.

55. Carter, et al., *Effects Of Catastrophic Events On Transportation System Management and Operations*; Photo Source: *Baltimore Sun*

56. Ibid.

57. Ibid.

58. Ibid.

59. Jack Riley, *Terrorism and Rail Security, CT-224, Testimony presented to the Senate Commerce, Science, and Transportation Committee on March 23, 2004*, (Santa Monica, CA: RAND Corporation, 2004), 9-10.

60. Ibid.

61. Association of American Railroads. *Back on Track, Issue 2, September 16, 2005, The Rail Industry's Response to Hurricane Katrina,* 1, On-line, Internet, 19 November 2005, available from http://www.aar.org/pubcommon/documents/ backontrack2.pdf.

62. Ibid., 2.

63. Ibid.

64. Robert S. Korpanty, David P. Dorfman, *Railroads for National Defense Program Pamphlet*, (Newport News, Virginia: Surface Deployment And Distribution Command Transportation Engineering Agency (SDDCTEA), 2004), On-line, Internet, available from https://www.tea.army.mil/pubs/nr/dod/brochures/RND(Jan04).pdf.

65. Robert S. Korpanty, "Preserving Strategic Rail Mobility," *Army Logistician* (Fort Lee, Virginia: Army Logistics Management College, 1999), On-line, Internet, available from http://www.almc.army.mil/alog/issues/NovDecember99/MS455.htm.

66. Korpanty and Dorfman, *Railroads for National Defense Program Pamphlet*.

67. Danchenko*, Public Transportation Fact Book March 2005*, 92, Table 133.

68. JayEtta Z. Hecker, *Intercity Passenger: Issues for Consideration in Developing an Intercity Passenger Rail Policy, GAO-03-712T*, (Washington, D.C.: Government Accountability Office, 2003), 4.

69. Amtrak, *Monthly Performance Report, September 2005*, A-2.1, On-line, Internet, available from http://www.amtrak.com/servlet/ContentServer?pagename=Amtrak/am2Copy/ Title_Image_Copy_Page&c=am2Copy&cid=1081442674477&ssid=322.

70. Danchenko*, Public Transportation Fact Book March 2005,* viii.

71. Ibid.

72. Danchenko*, Public Transportation Fact Book March 2005,* viii and 14.

73. Brian Michael Jenkins, Testimony presented to the Senate Committee on Judiciary on April 8, 2004, *Terrorism and the Security of Public Surface Transportation*, *CT-226*, (Washington, D.C.: RAND Corporation, 2004), 2.

74. Brain Michael Jenkins, *Improving Public Transportation Security: What Do We Do Now?,* 1, On-line, Internet, 28 November 2005, available from http://www.lexingtoninstitute.org/docs/500.pdf.

75. Ibid., 12.

76. Ibid.

77. Berrick, and Hecker, *PASSENGER RAIL SECURITY: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts,* 9.

78. Brian Michael Jenkins, Frances Edwards-Winslow, Ph.D., CEM, with Forward by Rod Diridon Sr., *Saving City Lifelines: Lessons Learned in the 9-11 Terrorist Attacks, MTI REPORT 02-06*, (San Jose CA: Mineta Transportation Institute, 2003), 1, On-line, Internet, available from http://www.transweb.sjsu.edu/publications/Sept11.pdf.

79. Department of Defense Directive 3020.40, *Defense Critical Infrastructure Program (DCIP)*, (Washington, D.C.: Assistant Secretary for Homeland Defense, 2005), 7.

80. Korpanty and Dorfman, *Railroads for National Defense Program Pamphlet*.

81. Senate Committee on Commerce, Science, and Transportation.

82. Wikipedia, The Free Encyclopedia, *Posse Comitatus Act*, On-line, Internet, available from http://en.wikipedia.org/wiki/Posse_Comitatus_Act.

83. Joint Chiefs of Staff, *Joint Publication 3-26, Homeland Security*, (Washington, D.C.: 2005), II-5 – II-12.

84. Paul W. Allred, Marc G. Barthello, *IRRIS 6 Whitepaper*, (Newport News, VA: Military Surface Deployment and Distribution Command Transportation Engineering Agency, 2005), 1-2, On-line, Internet, available from https://www.tea.army.mil/tools/irris.htm.

85. Ibid.

86. Ibid., 2.

87. Peter Guerrero, *Mass Transit: Federal Action Could Help Transit Agencies, GAO 03-263*, (Washington, DC: GAO, 2003), 2, On-line, Internet, available from http://www.gao.gov/cgi-bin/getrpt?GAO-03-263.

88. The Blue Ribbon Panel on Bridge and Tunnel Security, *Recommendations for Bridge and Tunnel Security Recommendations for Bridge and Tunnel Security*, (Washington, D.C.: Federal Highway Administration, 2003), On-line, Internet, available from http://www.fhwa.dot.gov/bridge/security/brptoc.htm.

89. *Transit Security Design Considerations*, (Cambridge, MA: Department of Transportation, Federal Transit Administration (FTA) Office of Research Demonstration and Innovation, FTA Office of Program Management, John A. Volpe National Transportation Systems Center, 2004), On-line, Internet, available from http://transit-safety.volpe.dot.gov/publications/Default.asp#Security.

90. Berrick, et al., *Transportation Security: Systematic Planning Needed to Optimize Resources*, 8-9.

91. Tim Lomax, David Schrank, *The 2005 Urban Mobility Report*, (College Station, TX: Texas Transportation Institute, Texas A&M University System, 2005), 1, On-line, Internet, available from http://mobility.tamu.edu.

92. Jenkins, *Improving Public Transportation Security: What Do We Do Now?,* 9.

93. Ibid.

94. Hecker, *Intercity Passenger: Issues for Consideration in Developing an intercity Passenger Rail Policy*, 6.

95. Ibid., 1-2.

96. Clarke, *Defeating the Jihadists: A Blueprint for Action,* 7.