Executive Summary

Transport vehicles and facilities have been frequent targets of terrorist attacks, hijackings, and sabotage around the world. The characteristics of transportation systems make them especially vulnerable to terrorism: transportation systems carry millions of people daily in enclosed spaces; elements of the infrastructure make them both strategic and symbolic targets; transportation systems have key civilian, as well as military functions; and much of the infrastructure is so distributed and open that effective security measures are difficult to implement. The transportation sector is often not only the target of terrorist attacks, but can serve as a terrorist weapon or delivery mechanism. On Sept. 11, 2001 Al Qaeda hijackers used fuel-laden airplanes as high-impact weapons – trucks or trains carrying hazardous or flammable materials could serve a deadly purpose at any strategic or densely populated location around the country. The 1995 sarin gas attack on the Tokyo subway system raised the stakes of transport terrorism further by introducing weapons of mass destruction (WMD) into the terrorist repertoire.

At the same time, the transportation network allows for the smooth functioning of society and the exchange of goods and services that fuels America’s economy. If this system were shut down due to a terrorist attack, it could hamper mobility and commerce, cause billions of dollars of damage to the U.S. economy, disrupt other infrastructure sectors, and affect the population’s sense of security.

Much has already been done since Sept. 11, 2001 to protect the Nation’s critical transportation infrastructure. Domestic security measures include government restructuring, new legislation, improved coordination and planning, increased funding, and the application of new technologies. As the transportation sector is highly integrated into a global network of travel, tourism, and trade, efforts to protect these systems will fail unless they are pursued abroad as well as at home. This requires strong international cooperation with allies and trading partners on transport and cargo security issues.

Despite the progress already made, the transportation sector remains vulnerable in many ways. In addition, precedent and intelligence information show that terrorists pose a significant threat to the sector. The threat against transportation systems is general and, in some areas, quite specific. Meaningful aviation and maritime security improvements have been attained, but a non-prohibitive, cost efficient security strategy for surface transportation has yet to be developed. To ensure a secure transportation sector, a dual-use security strategy must be developed that protects the U.S. against terrorism while improving passenger safety, service efficiency and convenience, and reducing crime. The success of any security strategy, however, depends heavily on a sustained commitment to the sector’s security, and funding to undertake the necessary initiatives.
Table of Contents

Executive Summary.................................................................................................................................. 1
Table of Contents .................................................................................................................................2
Introduction........................................................................................................................................... 4
Aviation Security.................................................................................................................................... 6
  Aviation Security Measures Since Sept. 11, 2001........................................................................... 6
  Passenger and Baggage Screening.................................................................................................... 6
  Restricting Access to Planes and Airport Facilities.......................................................................... 6
  Air Marshal Program......................................................................................................................... 7
  Strengthening Airplane Security...................................................................................................... 7
  Remaining Aviation Vulnerabilities................................................................................................... 7
  Training and Diligence of Security Personnel.................................................................................. 7
  Ground Security.................................................................................................................................. 7
  Implementing the Air Marshal Program............................................................................................ 8
  Air Cargo Security............................................................................................................................. 8
  Small Airports..................................................................................................................................... 8
  Terrorist Threats Against Aviation Systems...................................................................................... 8
    Hijackings, Planes as Weapons.......................................................................................................... 9
    Missile Attacks Against Planes.........................................................................................................9
  Future Aviation Security Measures.................................................................................................... 9
Maritime Security.................................................................................................................................... 10
  Maritime Security Measures Since Sept. 11, 2001.......................................................................... 10
  Enhanced Physical Security of Port Facilities.................................................................................... 10
  Increased Patrols of Waterways, Coastline, Ports and Coastal Facilities........................................ 10
  Creation of Databases to Track Cargo, Ships and Seamen............................................................... 11
  International Agreements to Improve Vessel and Port Security...................................................... 11
  Container Security and Protection Against WMD.......................................................................... 12
  Remaining Maritime Vulnerabilities.................................................................................................. 13
  Vessel, Port and Coastal Security...................................................................................................... 14
  Cargo Vulnerabilities.......................................................................................................................... 14
  Terrorist Threats Against Maritime Systems..................................................................................... 15
    Attacks Against Vessels.................................................................................................................... 15
    Attacks Using Vessels as Weapons...................................................................................................15
    Attacks Using Containers as Delivery Systems............................................................................ 16
  Future Maritime Security Measures.................................................................................................. 16
    Vulnerability Assessments / Security Standards.......................................................................... 16
    Funding............................................................................................................................................ 17
    Planning and Coordination............................................................................................................. 17
    Port and Coastal Protection............................................................................................................. 18
    New Technologies........................................................................................................................... 18
Surface Transportation Security........................................................................................................... 18
  Surface Transportation Security Measures Since Sept. 11, 2001................................................ 19
    Planning, Coordination and Training............................................................................................... 19
    Physical Security and Access Control............................................................................................. 19
    Additional Security Personnel......................................................................................................... 19
    Staff and Passenger Awareness....................................................................................................... 20
Remaining Surface Transportation Vulnerabilities .................................................. 20
Infrastructure Vulnerabilities ................................................................................ 20
Station and Vehicle Vulnerabilities .................................................................... 21
Terrorist Threats Against Surface Transportation Systems ................................... 21
Conventional Explosives .................................................................................... 22
Weapons of Mass Destruction .......................................................................... 22
Hazardous Materials ........................................................................................ 23
Future Surface Transportation Security Measures ............................................. 24
Planning and Coordination ............................................................................. 24
Funding .............................................................................................................. 24
Safer Stations and Vehicles ............................................................................. 25
Tools and Technologies ................................................................................... 25
Innovative Thinking .......................................................................................... 26
Conclusions ........................................................................................................ 26
Additional Resources ....................................................................................... 27
Reports .......................................................................................................... 27
Media Articles/Press Releases ........................................................................ 28
Websites .......................................................................................................... 30
Legislation ......................................................................................................... 30
Journals/Newsletters ...................................................................................... 30
Introduction

“Virtually every community in America is connected to the global transportation network by the seaports, airports, highways, pipelines, railroads, and waterways that move people and goods into, within, and out of the Nation. We therefore must promote the efficient and reliable flow of people, goods, and services across borders, while preventing terrorists from using transportation conveyances or systems to deliver implements of destruction.” – ‘The National Strategy for Homeland Security’, Office of Homeland Security, June 2002

The paper analyzes the challenges facing transportation security, placing primary emphasis on the aviation, maritime, and surface transportation and mass transit systems. Although pipelines are also considered part of the transportation infrastructure and are at risk of physical and cyber attacks due to their length, location, strategic value, and reliance on vulnerable control systems, pipeline security will not be discussed in detail in this report. Cyber security, which is an important issue that transcends all areas of transportation security, will be dealt with briefly in this introduction.

The transportation network, consisting of myriad interconnected and interdependent highways, mass transit systems, railroads, tunnels, bridges, navigable waterways, ports, and aviation infrastructures, enables the smooth functioning of society and the exchange of goods and services that fuels America’s economic motor. Millions of people use transportation systems every day to get to work or the shops, and vast quantities of freight are transported into and across the U.S. via ship, rail, and road.

The analysis provides a systematic overview of the transportation security initiatives undertaken post-Sept. 11 and evaluates the success of these measures in dealing with the vulnerabilities and threats faced by the industry’s main sectors. Domestically, a multitude of security measures have been introduced. The Department of Homeland Security was created to bring together key border and transportation security agencies, such as the INS, the U.S. Customs Service, and the U.S. Coast Guard. Moreover, the Transportation Security Administration (TSA) was established within the Department of Transportation (DoT) to coordinate national transportation security efforts. Internationally, a variety of security initiatives have been implemented, including ‘smart border’ agreements with Canada and Mexico; transport security pacts with the G-8, the International Civil Aviation Organization, the International Maritime Organization, and the World Customs Organization; as well as international container security programs with the world’s largest ports.

The report explains how the unique characteristics of each sub-sector make the industry inherently vulnerable, and offers specific examples of the weaknesses of transportation systems. The paper also offers an analysis of potential physical threats to the sector and examines the possible consequences should an attack occur. Finally, the report suggests additional measures to successfully secure the industry, particularly relating to surface and mass transit systems, which are still extremely vulnerable to terrorist strikes.
All modes of transportation currently rely on a multitude of information systems for critical operations and peripheral tasks. These systems are often poorly secured against cyber attacks that could allow terrorists to disrupt systems directly or manipulate information that could create vulnerabilities or facilitate attacks. Information systems in the transportation sector are usually highly interconnected with other IT infrastructures, opening them up to additional vulnerabilities. An example that illustrates this point is the phone hack by two teenagers seeking free long-distance telephone service that crashed a switch crucial to the operations of the Worcester, Massachusetts, airport.¹ As a result of the cyber attack, normal telephone communications were severed, the airport’s runway lighting system was disabled, and voice and radio communications with the planes in the area and approaching to land were disrupted. The airport went down for about 6 hours. This chaos was a result of an unintentional incident and one can only imagine what an intentional attack could achieve if aimed at an air traffic control center, a railway operations or switching center, or similar facilities whose systems are automated.

Indeed, increasing reliance on computers and communications technologies to collect, store, process and disseminate information in transportation systems makes them attractive targets. Attackers could break into passenger or cargo systems to help smuggle terrorists or WMD into the country. Many airports, for instance, are known to use unprotected wireless networks that could allow access to key operational systems.² Intelligent Transportation Systems (ITS) and the SCADA (Supervisory Control and Data Acquisition) systems at pipelines and railways are also vulnerable to unauthorized intrusions, viruses and worms, and denial of service attacks. This area warrants serious attention, but physical threats are currently more immediate.

The conclusions arrived at in this report are based on a thorough review of open-source material, participation in transportation sector forums, and conversations with transportation operators, government representatives, and other subject matter experts.

Authors of this report:

Eric Goetz (egoetz@ists.dartmouth.edu)
Research Analyst, IRIA

Input and assistance received from Trey Gannon, Robert Gray, and Jacqueline Lee.


² ‘Wireless LANs: Trouble in the Air’, Bob Brewin, Dan Verton and Jennifer Disabatino, Computerworld, January 14, 2002
Aviation Security

For obvious reasons the aviation industry has been the main area of focus since September 11, 2001. After all, planes were the weapons of choice in the most devastating terrorist attack on American soil. A multitude of security measures have been introduced to enhance aviation security and close the holes exploited by the Al Qaeda hijackers. The new security posture found expression in the Aviation and Transportation Security Act (ATSA)\(^3\), which President George W. Bush signed into law on November 19, 2001. The law is designed to create a new federal security force not just for aviation, but across all modes of transportation. The government underlined its commitment to aviation security by authorizing sustained funding in this area. For instance, the President’s Budget for 2003 requests $4.8 billion to fulfill the mandates established by the Act.\(^4\)

Aviation Security Measures Since Sept. 11, 2001

Aviation security measures adopted to date include:

**Passenger and Baggage Screening**

The ATSA federalized the passenger and baggage screening force under the control of the TSA. The agency has deployed more than 55,000 employees to screen both baggage and passengers, and the ATSA mandates that security personnel be subjected to background checks and performance assessments. Deadlines were met to screen all passengers (November 17, 2002) and baggage (December 31, 2002) at all 429 commercial airports in the U.S.\(^5\) The baggage screening deadline was met by installing over a thousand new EDS CAT-scan and explosive trace detection machines, and using bomb-sniffing dogs, manual searches and bag matching techniques. Prior to the Sept. 11, 2001 attacks, barely 5% of checked bags were screened for explosives. Efforts are also underway to screen U.S. mail and cargo on passenger flights.

**Restricting Access to Planes and Airport Facilities**

The ATSA calls for improvements to airport perimeter security or access to key facilities, such as air traffic control facilities, airport facilities, parked aircraft, aircraft servicing equipment, and aircraft supplies (including fuel). Automobile parking facilities within airport perimeters or adjacent to airport facilities were secured, but some restrictions on parking have been lifted in recent months. Access restrictions to planes and airport facilities have been implemented through the use of additional security personnel, access controls, and screening measures. The introduction of new tools and technologies, including biometrics and sensitive area surveillance systems, are also being considered in this area. Security checks also include performing more random searches throughout airports, verifying employees’ identifications, completing comprehensive background checks on passengers and employees, and matching them against intelligence watch lists.

---

\(^3\) Aviation and Transportation Security Act – Public Law 107-71, 107\(^{th}\) Congress’, November 19, 2001


\(^5\) ‘TSA meets baggage screening deadline’, Matthew Weinstock, Government Executive, December 30, 2002
Air Marshal Program
The air marshal program has been initiated and will become a pillar of the new aviation security regime. The ATSA puts the TSA in charge of the air marshal program and requires air marshals on all high-risk flights. Thousands of air marshals are currently already in action and the TSA expects to spend more than $1 billion by the end of 2003 training and deploying air marshals on U.S. domestic and international flights.6

Strengthening Airplane Security
The ATSA introduced several security measures to protect the cockpit and the aircraft in general against hijackers. Most U.S. airlines have installed cockpit doors secured with locks to prevent terrorists from entering the cockpit. Discussions are underway to introduce international cockpit door standards. The ATSA also mandates the installation of video monitors or other devices to alert pilots in the flight deck to activity in the cabin. Furthermore, pilots will soon be allowed to take handguns into the cockpit for protection, assuming they undergo appropriate training.

Remaining Aviation Vulnerabilities
All these measures have significantly improved aviation security and lowered the risk of hijackings or sabotage. However, vulnerabilities remain in the aviation industry.

Training and Diligence of Security Personnel
One of the main problems is ensuring the proper training and diligence of security and screening personnel. Before Sept. 11, 2001, screeners were poorly paid, trained and motivated. Now that screeners and other security personnel have joined the federal workforce, their commitment and performance have improved. It is only natural, however, that during a transition period when personnel is recruited, trained, and background checks are conducted, performance remains patchy. Furthermore, clear guidelines and operational procedures for security need to be developed and applied, and strategies implemented to motivate and retain staff.

There have been several instances where individuals have passed through security with firearms or other weapons without being detected. Crackdowns at Chicago’s O’Hare International and Midway airports against employees using fake IDs yielded a surprising number of offenders.7

Ground Security
Some perimeter and access control measures also remain inadequate. For instance, mechanics and other ground staff often still gain access to airplanes without passing through metal detectors.8 Areas near terminal facilities, airplanes and runways represent points of vulnerability as explosives could be placed in these areas or they could host attackers with shoulder-launched missiles.

7 ‘25 Chicago airport workers arrested’, Associated Press, December 11, 2002
8 ‘Attendants question ground security’, Blake Morrison, USA Today, April 4, 2002
Implementing the Air Marshal Program
The implementation of the air marshal program has also drawn criticism and there have been claims that new policies could endanger passengers. Despite policies that require at least two marshals on each assigned flight, marshals in the New York field office were told, in November 2002, they would have to fly alone if their partners call in sick. Aviation security analysts contend putting lone marshals on flights might enable a group of unarmed hijackers to take a gun from a marshal. In addition, marshals must accept any seat an airline offers. Such a policy contradicts the program's standard operating procedures, calling for marshals to have unobstructed access to the jet's aisle and, preferably, to sit near the cockpit to protect it from hijackers. Even if they believe their cover has been blown before a flight, marshals in the Atlanta field office have been told they must continue with their missions.9

Air Cargo Security
Air cargo remains an area of concern for aviation security experts. In January 2003, the General Accounting Office (GAO) found that air cargo remains vulnerable and security measures are either ongoing or have not been completed.10 About 22% of air cargo is shipped on passenger flights, but only a small percentage of it is currently inspected or scanned. Following the terrorist attacks on Sept. 11, 2001, the TSA banned passenger airlines from carrying cargo items weighing more than 16 ounces, as it is widely held that lighter bombs will not cause a commercial jet to crash. The longer-term aim is to check all cargo and mail using explosive-detection devices, bomb-sniffing dogs or manual searches similar to the screening of passenger baggage. The GAO recommends that the TSA develop an air cargo security plan, with specific deadlines to increase inspections of cargo and expand background checks on workers who pack and ship goods.

Small Airports
While the nation’s largest airports have significantly improved security measures, thousands of small airports remain relatively unprotected. Perimeter security, passenger screening and background checks for personnel are virtually non-existent at some of these facilities. An incident in January 2003 whereby a man in the Frankfurt area stole a motorized glider and threatened to crash it into the European Central Bank headquarters highlights the problem.11 Securing all small airports against such events would cost billions and would be unnecessary. Even if a small plane were crashed into a building or landmark, it could not cause anywhere near the damage of a commercial airliner because it is much lighter and carries only a fraction of the fuel.

Terrorist Threats Against Aviation Systems
Despite all the new security measures, terrorists still pose a threat to aviation. Historically, hijackings or airline sabotage have been popular and successful terrorist

---

9 ‘Air marshals charge new policies could endanger passengers’, Blake Morrison, USA Today, December 18, 2002
tactics. Moreover, vulnerabilities remain in the aviation industry, and attacks against airplanes and related facilities - or using jets as terrorist weapons – promise high impact, numerous casualties and serious disruptions.

**Hijackings, Planes as Weapons**

Terrorists could still attempt to hijack airplanes in order to force concessions, or to crash the planes into buildings, landmarks or infrastructure targets, such as nuclear power plants. As shown by the shoe-bomber Richard Reid, terrorists are also still out to blow up airplanes. Al Qaeda’s chief of operations in the Persian Gulf region, Abd al-Rahim al-Nashiri, was recently taking flight lessons near the strategic shipping lanes in the Strait of Hormuz before being arrested by authorities of the United Arab Emirates. He was said to be planning new terror strikes against U.S. interests in the Persian Gulf at the time of his capture, including shipping targets.12

**Missile Attacks Against Planes**

As was shown by an attempted missile attack on a passenger plane in Kenya in November 2002, planes are also under threat from the ground.13 Terrorists could use shoulder-launched surface-to-air missiles against commercial aircraft in the U.S. or abroad. Such weapons are readily available on the black market, and terrorist groups, including Al Qaeda, Hizbullah and Chechen separatists, are known to have them in their possession.14 U.S. airports and airlines will need to review procedures to protect against similar attacks and an interagency task force may be established to examine the issue. Israel recently decided to equip all its civilian passenger planes with countermeasures against shoulder launched anti-aircraft missiles.15

**Future Aviation Security Measures**

For aviation security to be successful in the long-term, it requires a sustained commitment to (and funding for) new security measures. Additional initiatives and technologies, such as a passenger-profiling system, bombproof cargo containers, and more and better screening tools for explosives and WMD, should be undertaken. The TSA is currently testing bomb-proof cargo containers made by California-based TelAir International to counter the threat of explosives bringing down an airliner. The new containers, which are made of a composite variant of Kevlar, are flexible and designed to bulge but not break in a blast.16 The government and airports are also poised to acquire additional scanning devices for explosives and other materials, and research into new scanning technologies is ongoing.

13 ‘Airports asked to review missile attack measures’, Kathleen Koch, CNN, November 30, 2002
14 ‘Experts fear SA-7 missile poses threat to airliners’, Isabel Vincent, National Post, November 29, 2002
Maritime Security

Shipping and the nation’s ports are vital for the U.S. economy and the military. Nonetheless, shipping, ports, coastal facilities, and shipping containers remain highly vulnerable to terrorist attacks. As with aviation, the maritime system could be targeted directly or used as a weapon or delivery system for attacks.

Maritime Security Measures Since Sept. 11, 2001

Secondary emphasis has been placed on maritime security due to the urgent need to address aviation problems. A number of security initiatives have been launched, but most have not yet been fully implemented. On November 25, 2002, President Bush signed into law the Maritime Transportation Security Act (MTSA)\(^{17}\), a key bill aimed at improving security at U.S. seaports and preventing terrorists from using the maritime transportation system to mount attacks on America. The MTSA will strengthen security by imposing broad security requirements on the maritime industry, including a comprehensive assessment of the sector, the authorization of an increased number of security officers and screening equipment, and the building of important security infrastructure at seaports.\(^{18}\)

Much has already been done to better understand threats and vulnerabilities and protect the maritime system from terrorist attacks. Initial security measures include:

**Enhanced Physical Security of Port Facilities**

All the major U.S. ports have implemented a variety of physical security measures since Sept. 11, 2001 to prevent easy access for terrorists to ships, facilities or cargo. Under the MTSA, all vessels and facilities on or near the waters subject to U.S. jurisdiction have to undergo assessments to identify those at high risk of being involved in a transportation security incident.\(^{19}\) Physical security has been improved through the deployment of fences, surveillance cameras and additional security personnel to guard facilities, as well as limiting vehicular traffic around seaports. Additional security measures have been added at facilities that handle hazardous materials. Better training and pay for port police and security personnel could further improve security. Access control measures and security checks have been introduced at some facilities. Port personnel – especially those with access to sensitive areas - will be subjected to background checks, and access to facilities everywhere will be controlled using identification cards.

**Increased Patrols of Waterways, Coastline, Ports and Coastal Facilities**

The U.S. Coast Guard has stepped up patrols of waterways, coastal waters, ports and infrastructure facilities on the coast since Sept. 11, 2001. In this context, the Coast Guard may start using remote controlled unmanned aerial vehicles (UAVs), similar to those now

---

\(^{17}\) ‘Maritime Transportation Security Act - Public Law No. 107-295, 107\(^{th}\) Congress’, November 25, 2002


\(^{19}\) The Coast Guard has begun a process of comprehensive risk assessment of seaports across the nation, including an assessment of security conditions of 55 U.S. ports over a 3-year period with a private firm, TRW Systems, and another limited assessment to identify high risk infrastructure and facilities within specific areas of operation.
used for wartime surveillance in Afghanistan, to patrol the nation's coastal regions for security threats. More than 100 security zones were established around particularly sensitive or vulnerable coastal installations, such as major naval bases, key landmarks like the Statue of Liberty, power plants, and oil refineries near major cities. Permanent no-entry zones could be established and enforced through a combination of remote sensors, drones, fixed impediments to ship movement, and even shore-based guns as a last resort. Patrons in major harbors and on waterways in large urban areas have been increased and ships entering U.S. ports are being boarded and checked for explosives and WMD. Despite the efforts of the Coast Guard not all ships can be inspected at sea and cargo containers are seldom scanned for dangerous materials. Recent initiatives include prescreening ships and cargo before they reach America to help identify high-risk vessels. These vessels could be prevented from entering port near large U.S. cities unless they are first inspected at sea. Alternatively they could be re-routed to smaller U.S. ports, well away from large population centers. The Coast Guard will be aided by the Sea Marshal program, and maritime safety and security teams set up at ports to safeguard the public and protect vessels, harbors, ports and waterfront facilities.

**Creation of Databases to Track Cargo, Ships and Seamen**

U.S. intelligence agencies have set up large databases to track cargo, ships and seamen in a search for anomalies that could indicate terrorists on approaching ships or ‘high-risk’ cargo. As part of this program, the Coast Guard has established new rules for ships approaching the U.S. Ninety-six hours before reaching a U.S. port (changed from 24 hours), they must provide data about their cargo, the names and passport numbers of the crew, the ship’s corporate details, and recent port calls. This information is fed into intelligence databases and merged with other data, such as satellite photos of ships or ports. Such advanced information technologies promise to facilitate a certain level of pre-screening and identifying high-risk ships and cargo.

**International Agreements to Improve Vessel and Port Security**

Since Sept. 11, 2001, the U.S. has entered into several international agreements with other maritime nations to help protect the sector against terrorist attacks. As the U.S. is an integral part of a complex global maritime network, security solutions can only be achieved in cooperation with others. Amendments to the International Convention for the Safety of Life at Sea (SOLAS), which was passed by the International Maritime Organization (IMO) and signed by 108 countries, will help secure passenger and cargo ports around the world by requiring monitoring of facilities and passengers, additional fencing and lighting, and security checks of people and vehicles from July 2004. The International Ship and Port Facility Security Code is a further international security

---

20 ‘Drones To Serve As Coastal Watchdogs’, Hartford Courant, December 13, 2002
22 ‘15 Freighters Believed to Be Linked To Al Qaeda’, John Mintz, Washington Post, December 31, 2002
initiative developed in collaboration with the IMO. Some of the cargo security initiatives described below also rely heavily on an international approach.

**Container Security and Protection Against WMD**
The government and individual ports have launched several projects to help identify high-risk containers and prevent them from entering the country. These programs include the development of standards to enhance the physical security of cargo containers, implementing long-range vessel tracking systems, and anti-terrorism assessments of foreign ports. If dangerous cargo does reach the U.S., it is hoped that it can be spotted before it can be transported to urban centers or other strategic locations.

- **U.S. Customs Container Security Initiative (CSI)** – The U.S. Customs Container Security Initiative plays a pivotal part in the effort to protect international maritime trade. The CSI, launched in February 2002, initially seeks to solicit the participation of the world’s 20 ‘mega ports’ that account for a large percentage of container traffic, and their host governments. The main objectives of the CSI are to: (1) use automated information to identify and target high-risk containers; (2) pre-screen those containers identified as high-risk before they arrive at U.S. ports; (3) use detection technology to quickly pre-screen high-risk containers; and (4) use smarter, tamper proof containers. To facilitate detection of potential security concerns at the earliest possible opportunity, CSI will be implemented at ports that send large volumes of cargo containers into the United States. As of November 2002, 11 of the world’s top 20 seaports - representing over two-thirds of all of the containers shipped to U.S. seaports - had joined U.S. Customs in CSI to protect global commerce from the terrorist threat.

- **Advanced Manifest Regulation** – As of February 2, 2003, the U.S. Customs Service will start enforcing its advanced manifest program that requires shippers and ocean carriers that bring goods into the U.S. to electronically submit complete container manifest information through the Automated Manifest System (AMS) 24 hours before the container is loaded on a vessel. The initiative is aimed at improving cargo container security and preventing the introduction of explosives or WMD into the U.S. At present, container information often does not reach authorities until cargo is already in transit or has arrived in the U.S. Non-compliance could result in heavy fines.

- **Operation Safe Commerce** – Congress has allocated funding for this project to help the DoT and the Customs service to identify existing vulnerabilities in the container supply chain and develop improved

---

26 ‘Shippers, ocean carriers scramble to meet customs deadline’, Linda Rosencrance, Computerworld, January 23, 2003
methods that ensure the security of cargo entering and leaving the U.S. The project will act as a test-bed for new container security techniques and technologies, including GPS tracking and electronic container seals. Pilot projects involve the three largest U.S. container ports of entry (Los Angeles/Long Beach, New York/New Jersey, and Seattle/Tacoma), with plans to turn the initiative into international standards within twelve months.

- **Customs Trade Partnership Against Terrorism** – C-TPAT is a partnership between the business community and Customs that is designed to enhance the security of international supply chains. Companies volunteer to undertake measures that will reduce vulnerabilities in their supply system and are certified by Customs once they have successfully addressed all security concerns. In the event of a security incident, certified companies benefit from their participation as their containers are less likely to be delayed by inspections and they will be among the first to resume their import operations into the U.S. Future plans include the creation of special shipping lanes – E-Z Lanes – that expedite transportation through check-points for businesses that are willing and able to ensure point-of-origin and in-transit security.

- **Pilot Programs to Screen Containers for Explosives and WMD** – Several U.S. ports are testing technologies to scan containers for explosives or WMD before they are loaded onto the dock, or before they leave port. Early experiments with scanning systems installed on cranes have been disappointing, but other scanning devices that look for radioactive material appear to be working well. For instance, Virginia’s Norfolk International Terminals is now scanning 5,000 container trucks a week for radiation just before they carry their goods out of the port. The program will soon be expanded to VPA’s Newport News Marine Terminal and Portsmouth Marine Terminal. However, even these scanning devices are only able to detect radioactive material and not other types of explosives, such as C-4.

**Remaining Maritime Vulnerabilities**

Despite these promising efforts, maritime security currently remains wholly inadequate. Multiple vulnerabilities remain that could easily be exploited by terrorists to attack vessels, port facilities, or coastal infrastructures – or to smuggle WMD or explosives into the country to be detonated at a later time. The extensive size, open accessibility, and metropolitan location of most ports ensure a free flow of trade, but these factors also make the monitoring and controlling of traffic through the ports virtually impossible.

---


30 Ibid.,
Vessel, Port and Coastal Security
Ships, such as oil tanker, warships, cargo ships or cruise liners, are vulnerable because they are large, slow-moving, difficult to maneuver, and have strategic value. Past attacks, including the bombing of the USS Cole, highlight this vulnerability. Risk assessments have shown that some of America’s largest ports (and port facilities) also remain vulnerable. Fences, security patrols and access control systems are often inadequate to prevent determined attackers from entering the port perimeter. A lack of patrol boats and law enforcement officers leaves many critical port facilities largely unprotected from a land- or waterborne attack. Fuel and chemical storage depots, sometimes containing extremely hazardous materials, are often above ground and could be targeted by attackers from land or sea. The U.S.’s 361 ports vary in size, functions, and capabilities, and each one presents a unique set of vulnerabilities.

Critical infrastructures located on the coast or on inland waterways also remain vulnerable to waterborne attacks. Bridges, power plants or oil refineries have few protections against approaching ships carrying explosives or other harmful materials. Similarly, coastal cities, such as New York or Los Angeles, have few safeguards against aggressors from the sea, except some harbor patrols.

Cargo Vulnerabilities
Despite recent initiatives, cargo containers are still far from secure and could be used by terrorists to introduce explosives or WMD into the country. In 2001, U.S. Customs processed more than 214,000 vessels and 5.7 million sea containers carrying goods worth approximately $800 billion. Around 90% of the world’s cargo moves by container. It is unclear exactly what percentage of these containers is actually checked upon entry into the U.S. – estimates range between 2-10%. That leaves at least 90% of all containers entering the country unchecked, and documentation requirements for containers are still easy to circumvent. Customs now receives data on shipments 96 hours before they are supposed to reach the U.S. border, but there are no controls over what happens to the containers en route. Container routes are so complex that each individual container may pass through dozens of points before reaching its final destination. Containers are vulnerable to tampering at each of these points as most containers currently have little more than a cardboard seal to verify the integrity of the contents. Material in the container can potentially be tampered with not only by the manufacturer/supplier of the material being shipped, but also by the carriers who are responsible for shipping the material, and the personnel who load containers onto ships, trains and trucks. Exporters who make arrangements for shipping and loading, freight consolidators who package disparate shipments into containers, and forwarders who process the information about what is being loaded onto ships, are among the many other people who interact with the

31 ‘Port security lagging’, Aldrin Brown, Orange County Register, November 24, 2002
cargo or have access to the records of the goods being shipped.\textsuperscript{34} Furthermore, the automation of the maritime transportation system has increased the vulnerability of the sector by introducing more opportunities for terrorists to access important shipping data. Terrorists can tap into inadequately protected information networks that provide real-time traffic information and purchasing data, which can be used to identify cargo in transit.

**Terrorist Threats Against Maritime Systems**

Terrorists pose a serious threat to maritime security. Al Qaeda is known to have a maritime military manual that classifies ships, showing different classes of vessels, where to hit them and how much explosives you need.\textsuperscript{35} In addition, Al Qaeda has a history of nautical attacks and the group’s tactics indicate an increase in strikes against shipping and port facilities as part of the push to hit economic targets. U.S. intelligence officials have identified cargo freighters that they believe are controlled by Al Qaeda and could be used by the terrorist network to ferry operatives, bombs, money or commodities over the high seas.\textsuperscript{36}

**Attacks Against Vessels**

Terrorists, and particularly Al Qaeda, threaten ships directly. In 2000 a small boat filled with explosives was rammed into the USS Cole in Yemen, and in October 2002, the French-owned supertanker Limburg was attacked in similar fashion in the Persian Gulf region.\textsuperscript{37} These incidents and intelligence from the region indicate that terrorists may be stepping up attacks against shipping, especially in the Middle East where a successful strike would have heightened symbolic value in light of a possible military conflict with Iraq. Not only oil tankers and warships are under threat – future attacks could target all kinds of commercial shipping, including cargo ships, cruise liners or even ferries, anywhere in the world.\textsuperscript{38}

**Attacks Using Vessels as Weapons**

Terrorists could hijack a ship en route to the U.S. or they could register a ship in ‘flag of convenience’ nations, which often ask for almost no information from shipping firms that ‘flag’ their vessels with them, and use it for terrorist activities; or they could purchase a legitimate shipping company and its vessels to carry out acts of terrorism without coming under suspicion. These ships could be loaded with explosives and crashed into other vessels, port facilities, critical infrastructures, or population centers on the coast. Alternatively, oil tankers or vessels carrying hazardous materials could be used as terrorist weapons. The types of vessels mentioned above, major ports, coastal oil depots, power stations, harbors or bridges could be ideal targets for such attacks. Maritime attacks may also involve the use of small underwater craft, such as small submarines or

\textsuperscript{34} ‘Container Security – Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges’, Op. Cit.,
\textsuperscript{35} ‘International shipping vehicles vulnerable to terrorist attacks, FBI warns’, Gregory Katz, Dallas Morning News, December 1, 2002
\textsuperscript{36} ‘15 Freighters Believed to Be Linked To Al Qaeda’, Op. Cit.,
\textsuperscript{37} ‘Warnings From Al Qaeda Stir Fear That Terrorists May Attack Oil Tankers’, Keith Bradsher, New York Times, December 12, 2002
\textsuperscript{38} ‘International shipping vehicles vulnerable to terrorist attacks, FBI warns’, Op. Cit.,
underwater motor-propelled sleds for divers. Some terrorist groups are known to have experimented with such methods. The Maritime Intelligence Group reports that radicals from the Jemaah Islamiah (JI), a group linked to the Al Qaeda network, have been trained in sea-borne guerilla tactics, such as suicide diving and ramming, developed by the Liberation Tigers of Tamil Eelam (LTTE). Terrorists could also gain unauthorized access to ships and port facilities to place explosives. At least one Al Qaeda operative is known to have been in the process of obtaining an international seaman's license that would allow him into any port in the world without a visa.

**Attacks Using Containers as Delivery Systems**

The most frightening terrorist threat to maritime security involves terrorists smuggling explosives or WMD into the U.S. using cargo containers. The weapon could be detonated upon arrival at the port or at any strategic point along the container’s route. Targets could include strategic transportation nodes, symbolic landmarks or large population centers. In addition to death and destruction, any such attack using WMD would undoubtedly have a shocking effect on the national psyche. It would also bring international cargo transports – and with it the global economy – to a halt until other containers could be searched for further weapons. In a wargame scenario in October 2002, sponsored by consulting firm Booz Allen Hamilton, two dirty bombs were discovered in Los Angeles and Minneapolis before they could be detonated. Despite the fact that no actual damage had been caused, every port in the U.S. was closed, costing the economy $58 billion dollars. The Brookings Institution estimated that a WMD shipped by container or mail could cause damage and disruption costing the economy as much as $1 trillion. This figure seems plausible given that the recent West coast port closure cost the nation “approximately $1 billion per day for the first five days, rising exponentially thereafter.”

**Future Maritime Security Measures**

To reach an acceptable level of security, the maritime sector will require the development and implementation of a comprehensive security strategy, as well as sustained funding to support that strategy. The TSA, other government entities, and the private sector are clearly starting to address the vulnerabilities in the maritime area.

**Vulnerability Assessments / Security Standards**

A crucial first step will be to conduct comprehensive vulnerability assessments at the nation’s seaports. Despite the vital role ports play in linking America to the world, both

---

40 ‘Experts says Islamic Militants Trained for Sea Attacks’, Reuters, Wednesday, January 22, 2003
economically and militarily, studies on port vulnerability for the nation’s fifty largest ports are not scheduled to be completed for years. This schedule needs to be stepped up. Ports often do not understand the threats facing them because they do not have access to intelligence data. Therefore, they are unable to match threats with vulnerabilities to determine high-risk targets. Out of necessity, there will undoubtedly be a window of vulnerability, but more must be done to analyze vulnerabilities and create mechanisms to help share intelligence reports. Industry-wide security standards must be developed to create benchmarks for security.\(^{45}\) For instance, at present, there is no generally accepted requirement for how high a perimeter fence should be, where access controls are necessary at ports, or what form they should take.

**Funding**

In addition, funding must be provided to allow the coast guard and ports to adopt security measures. In the aftermath of Sept. 11, 2001, Congress provided billions of dollars to help protect the aviation industry. Equally large sums will be necessary for maritime security.\(^{46}\) The federal government – in the form of the TSA – has already made grants worth a total of $93.3 million available for port assessments and improvements at critical national seaports.\(^{47}\) In addition, various pilot programs, such as Operation Safe Commerce, have received federal money, but much more needs to be done to help ports and coastal facilities enhance security. The Coast Guard would also benefit from an infusion of funds to recapitalize its ageing fleet and shoreside facilities, and allow it to meet its expanded responsibilities.\(^{48}\)

**Planning and Coordination**

Another key area is planning and coordination. In order to prevent and deter future attacks, and to be able to respond effectively in case of a terrorist event, Harbor Safety Committees have been set up to improve the coordination of efforts between federal (including intelligence, FBI, Customs, Immigration, and the Coast Guard), state, local, and private law enforcement agencies.\(^{49}\) These agencies get together to discuss, coordinate and rehearse potential terrorist scenarios. Training exercises and simulations will help to establish who is in charge and what roles each entity should play. Further, the TSA will help nominate port and vessel security officers to further improve coordination.

---

\(^{45}\) The U.S. Coast Guard has published security guidelines on vessels and port facilities ([http://www.uscg.mil/hq/g-m/nvic/index00.htm](http://www.uscg.mil/hq/g-m/nvic/index00.htm)). While these are helpful, they are not completely comprehensive and are only meant to bridge the gap until final regulations are released.

\(^{46}\) According to Rear Admiral Larry Hereth, U.S. Coast Guard, first year security costs for maritime and port security could reach about $1.4 billion. Overall, up to $10 billion of security spending could be necessity in the coming years. Remarks by Rear Admiral Larry Hereth at the Transportation Safety and Security Workshop, GWU Institute for Crisis, Disaster, and Risk Management, GWU Transportation Research Institute and The International Emergency Management Society (TIEMS), Washington D.C., January 28/29, 2003


Port and Coastal Protection

Ports would be safer if potentially dangerous vessels could be intercepted before they reach the U.S. coast. Therefore, coastal surveillance and the protection of ports and coastal facilities should be improved. Port perimeter security and access control measures also need to be enhanced. Work has started in this area, but security measures are ad hoc and not centrally coordinated. Strong maritime security will require the smart adoption of new tools and technologies in the fight against terrorism. These would include computer programs to help sift through information on vessels, crews and cargo in search of anomalies, or to match seamen or port employees against terrorist watch lists. IT resources and GPS technology can also help track the location of ships and cargo in transit in near real-time.

New Technologies

New technologies should be applied to the pressing issue of cargo security. U.S. Customs is already using sophisticated scanning devices capable of providing images of the contents of a container. Scanning tools must be more widely deployed, as is already the case at ports in other countries, such as Singapore or Rotterdam. Some devices are already in use to detect radioactive material being introduced into the U.S. New technologies must be developed to scan for other WMD and other types of explosives. As they become available, these new devices should be brought into service to protect the most strategic ports first as it will initially not be possible to scan all containers. Finally, tampering with containers during their journey can be prevented by using electronic seals, such as are already being tested as a part of the DoT’s ITS intermodal freight projects\(^50\) and Operation Safe Commerce. The different container security initiatives described above offer hope that technology can help secure containers from the moment they are filled with goods, throughout their often complex journey, to the final destination where they are unloaded.

Surface Transportation Security

Surface transportation is extremely difficult to define. It consists of a diverse array of long distance passenger and freight vehicles and facilities; mass transit vehicles and facilities; and related infrastructures. These include trains, trams, subways, buses, trucks, railways lines, highways, stations, depots, control facilities, bridges, tunnels etc. This complex network of systems is absolutely essential for everyday life and the national economy. The least emphasis has been placed on this area because it was perceived as least pressing, and also because it is hardest to protect. By their very nature, surface transportation systems need to be open and accessible, and have thousands of entry points. Numerous key assets are distributed over a wide area, and some routes are static. All these factors mean that fully protecting surface transportation is impossible. However, the recognition that a certain amount of uncertainty and risk is unavoidable should not be cause for resignation. By learning from past tactics and collecting intelligence on future threats, it is possible to apply security measures that: help detect

\(^{50}\) See U.S. Department of Transportation, ITS Intermodal Freight Operational Test - [http://www.ops.fhwa.dot.gov/freight/opsANDsafe/itsops/opstest.htm](http://www.ops.fhwa.dot.gov/freight/opsANDsafe/itsops/opstest.htm)
and deter attacks; raise the likelihood that terrorists will be apprehended; and improve
emergency and consequence management to limit casualties and disruptions. Dual-use
security measures – that reduce crime or bolster passenger safety or comfort - are also
attractive for surface transportation.

Surface Transportation Security Measures Since Sept. 11, 2001
Although security efforts in this area are somewhat lagging there has been some progress.
Security measures to date include:

Planning, Coordination and Training
Many surface transportation and mass transit operators have improved planning and
coordination efforts with law enforcement, emergency managers, first responders and
other organizations. Terrorism prevention, rapid response and successful crisis
management require smooth cooperation between the multitude of entities and
jurisdictions often affected by an attack on surface transportation. Coordination with
local, state and federal authorities can also open channels of communication that can be
used to share threat information. Constant training and drills, including simulations and
field exercises, are extremely important to ensure readiness, test plans and identify
potential problems. Since Sept. 11, 2001 security drills have focused increasingly on
hijacking and hostage taking, chemical and biological weapons attacks, bombs, and other
terrorist actions.

Physical Security and Access Control
As with aviation and maritime security, initial efforts in the surface transportation sector
have placed heightened emphasis on improved physical security of - and access control
to – transportation assets, such as vehicles, tracks, switching and control facilities, freight
areas, and infrastructures. However, due to the massive number and wide dispersal of
assets, only the most critical assets can be secured. Perimeter security measures include
additional fences and barriers, surveillance cameras, intrusion detection systems, and
more and better lighting. Access to some areas, such as vehicular access to some train
stations, has been restricted. In addition, employee access to critical facilities, including
transit control centers, dispatch, and bus storage facilities, has also been restricted
through the use of employee IDs. The TSA is currently developing a multi-modal
transportation worker identification credential system that could involve hundreds of
thousands of transportation workers across all sectors, including those in surface
transportation and public transit. 51

Additional Security Personnel
As a temporary security measure, all kinds of surface transportation and mass transit
organizations have employed additional security staff to deter and prevent terrorist
attacks. A more visible presence of security guards and other security personnel on
vehicles, or at stations, infrastructures or other facilities, will provide relief until other
security measures are introduced. Law enforcement agencies have also deployed
additional officers to surface transportation facilities, and increased patrols at stations.

51 ‘Transit Industry Prepares for Anniversary of Sept. 11 With Increased Security’, Federico Cura,
Passenger Transport, September 9, 2002
Staff and Passenger Awareness
To supplement security personnel, surface transportation and mass transit operators have sought to train and educate transport staff concerning terrorist threats to increase awareness and vigilance. Public awareness campaigns are also being employed to get travelers involved in their own protection. Public service announcements are played asking passengers to be on the lookout for suspicious people or packages in stations and on vehicles, and to notify authorities in case of danger. However, while such campaigns extend the eyes and ears of security personnel, they may also foster anxiety and lead to false alarms.

Remaining Surface Transportation Vulnerabilities
Efforts to secure surface transportation have only minimally reduced the risk of terrorist attacks. Countless vulnerabilities remain in the surface transportation sector and cannot all be eliminated. Surface transportation, more than any other transportation system, must learn to live with these risks to a certain extent. These systems offer a concentration of people and a richness of tempting terrorist targets. Moreover, the anonymity and easy escape routes that surface transportation systems offer potential attackers further increases their vulnerability. Different kinds of surface transportation systems have different vulnerabilities, and all are linked in a complex network of interrelated services. To be able to offer the services our society and economy require, surface transportation and mass transit systems must remain accessible, convenient and inexpensive. Because of this level of accessibility, surface transportation simply cannot implement the security checks that are common in the aviation sector – and, to a more limited extent, in the maritime realm.

Infrastructure Vulnerabilities
Surface transportation and mass transit systems remain vulnerable in numerous ways. The system’s infrastructure – railways, highways, bridges and tunnels – remains at risk because it spans the entire country and cannot be completely secured. Railway lines and highways often pass through remote areas and it is impossible to totally restrict access to them. Fencing and other security measures are in place to protect critical transportation nodes, but they still remain vulnerable. Severing key rail or road arteries would probably not cause substantial loss of life, but could result in severe economic disruption. Mass transit tracks are less vulnerable because trains pass over them more frequently and they are usually in populated areas.

The U.S. has thousands of bridges and tunnels across the country, which remain vulnerable to terrorist attacks. There are few physical safeguards to protect these infrastructures from being damaged or destroyed, although it should be noted that actually destroying a bridge or tunnel requires extensive planning and engineering knowledge.

Key bridges and tunnels exist that have a heightened strategic or symbolic value - five major bridges and one tunnel that link Ontario to Michigan and New York account for
70% of all the trade between the U.S. and Canada;\textsuperscript{52} the Chesapeake Bay tunnel is crucial for civilian and military uses;\textsuperscript{53} the Golden Gate Bridge, Bay Bridge and Coronado serve thousands of travelers daily and have immense symbolic value. Other bridges and tunnels are vital to the delivery of natural resources to fuel the economy and may also host oil or gas pipelines or communication links. Other infrastructures, such as control centers or rail switching yards, may also be vulnerable. These high-risk targets must be identified and offered particular protection through enhanced perimeter security, more security personnel, and electronic monitoring systems. Attacks on transportation infrastructures could kill many people, result in serious financial losses and weaken the morale of society. Natural disasters have demonstrated the resiliency of surface transportation systems. Service on damaged parts of the transportation system is usually restored rapidly and disruptions are held to a minimum. However, the system remains vulnerable to a determined attack against several key infrastructures or nodes.\textsuperscript{54}

**Station and Vehicle Vulnerabilities**

Stations and vehicles also remain vulnerable. Despite improved physical security measures and a heightened police presence, access to, and movement within and between, subway, bus, tram, and rail systems is free and unrestricted. Baggage and cargo undergoes little or no security checking. This makes the system vulnerable to the introduction of explosive devices, or worse, WMD. Cars and trucks face no obstacles to freely traveling on the nation’s highway network, and can enter major cities and population centers largely unchallenged. Freight and hazardous materials that are transported around the country are also vulnerable to manipulation at numerous points where they are stored, loaded and unloaded, or simply pass through.

**Terrorist Threats Against Surface Transportation Systems**

Historically, terrorist attacks on surface transportation systems have been extremely common. In fact, roughly one-third of all terrorist attacks worldwide target surface transportation systems, with the weapon of choice usually being explosives.\textsuperscript{55} Attacks are relatively evenly split between rail systems (trains, subways, stations, and rails) and bus systems.\textsuperscript{56} Past examples of terrorist strikes against surface transportation abound. In 1995 and 1996, Algerian terrorists set off several bombs in the Paris subway; Palestinians have carried out numerous suicide bombings of buses in Israel; IRA bombers have blown up various railway and subway vehicles and infrastructures during their long-running terrorist campaign in the UK; and Aum Shinrikyo’s sarin gas attack on Tokyo’s subway in 1995 raised the bar by introducing WMD into the terrorist arsenal.\textsuperscript{57} All these

---

\textsuperscript{52} ‘America Still Unprepared – America Still in Danger’, Op. Cit.,

\textsuperscript{53} ‘MTI Report S-01-02 – National Transportation Security Summit, Washington D.C., October 30, 2001’, Mineta Transportation Institute, College of Business, San Jose State University

\textsuperscript{54} ‘Basic Characteristics of Freight Rail Transportation in the United States’, Report of the President’s Commission on Critical Infrastructure Protection, 1997

\textsuperscript{55} ‘Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview’, Brian Michael Jenkins, The Mineta Transportation Institute, College of Business, San Jose State University, October 2001

\textsuperscript{56} Ibid.,

\textsuperscript{57} For a detailed list and analysis of past terrorist attacks on surface transportation see ‘Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview’, Op. Cit., and
examples give clues to the kind of threats the U.S. faces in the war on terrorism. Although little open source information is available on Al Qaeda’s intentions in the area of surface transportation, history can serve as a guide to possible threats. America has already encountered terrorist plots targeting surface transportation systems in New York. In 1993 Islamic extremists planned to set off truck bombs in New York’s tunnels and on bridges. In 1997 terrorists planned to detonate bombs in Brooklyn’s Atlantic Avenue subway station, which serves 10 subway lines and functions as a Long Island Railway terminal.\(^{58}\) These plots were thwarted.

The threat of terrorist attacks on surface transportation systems remains high due to the potential to disrupt society and the economy, and because security improvements in the aviation and maritime sectors make surface transportation relatively more attractive. To highlight this threat, the DoT issued a terrorist threat advisory to the transit industry in May 2002 indicating that subway systems were a possible target and that the industry should remain in a heightened state of alert.\(^{59}\) Urban centers and strategically important targets are under much greater threat than rural regions, or systems with no strategic value. For example, mass transit systems in New York City, Washington D.C. or Chicago are at much greater risk of attack than local bus services in the Midwest. This point should be considered when developing security strategies.

**Conventional Explosives**

Terrorists could place conventional explosives in surface transportation or mass transit vehicles, at stations, or at other facilities. There are many precedents for these kinds of bombings on trains, buses or subways. Explosives could be placed in cars or trucks next to stations; in bags, suitcases or packages in terminals or on vehicles; or hidden somewhere in stations or on vehicles, such as in trashcans, behind advertisements, or in bathrooms or maintenance rooms.\(^{60}\) The openness of the systems, the myriad access points, and the concentration of people makes this scenario a grave threat.

**Weapons of Mass Destruction**

Terrorists could also place explosives or WMD on rail cars or trucks – possibly in intermodal containers – and detonate them at strategic points. For this purpose they could use large amounts of conventional explosives, dirty bombs, explosive devices containing chemical or biological agents, or nuclear weapons. The explosive devices could be brought into the country via land or sea while container screening remains patchy, or they

---


\(^{59}\) ‘Mass Transit – Challenges in Securing Transit Systems’, Testimony before the Subcommittee on Housing and Transportation, Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Statement of Peter Guerrero, Director Physical Infrastructure Issues, General Accounting Office, September 18, 2002

could be assembled by terrorist cells already in the country. Such a weapon could be delivered to almost anywhere in the U.S. via rail or road in intermodal containers. Alternatively, it could be placed on a train or truck at freight transfer terminals. As freight trains pass through major population centers and critical transportation choke points – trucks, too, have almost unlimited access to cities and other key infrastructures – an explosive device introduced in this fashion could cause severe damage to human lives and property.

There is a real threat of terrorists releasing chemical or biological agents on subway systems, railways or buses, or at stations or terminals. They could thereby use the surface transportation or mass transit system to deliver deadly substances to hundreds of thousands of people. The 1995 sarin gas attack in the Tokyo subway provides a dangerous blueprint for how such an attack could be launched. The arrest of several men – possibly with links to Al Qaeda – in the UK in January 2003 for producing ricin indicates that terrorists may be interested in using these deadly weapons. Any number of dangerous radiological, chemical, or biological substances, including ricin, sarin, sodium cyanide, mustard gas, or anthrax, could be unleashed upon an unsuspecting urban population. Cleverly placed bags or packages could allow these deadly agents to be distributed below ground throughout a mass transit system - with its tunnels, moving trains, stations, and ventilation shafts - and up through ventilation shafts and station egresses above ground to an entire city.

**Hazardous Materials**

Trucks or trains carrying fuel or hazardous materials also pose a significant threat. Terrorists could use these vehicles as both weapons and delivery systems. Roughly 800,000 hazardous material shipments by truck occur each day, and about 2,000 pass through New York City each day. Thousands of hazardous material transports are conducted by rail daily. If not properly protected, these materials could be detonated at government buildings, landmarks, in populated areas, or at strategically important points. News reports indicate that corrupt individuals at state Motor Vehicle Departments have illicitly sold hazardous materials permits to people with Arabic surnames. A variety of measures have been discussed to address this threat. Hazardous material transporters could be required to develop new notification procedures to provide authorities with advance warning that chemicals or other materials will be passing through their jurisdiction. Debate has also focused on requiring background checks for individuals.

64 ‘The Use of Technology In Preparing Subway Systems For Chemical/Biological Terrorism’, Dr. Anthony J. Policastro and Dr. Susanna P. Gordon
66 ‘New York Senator Charles Schumer says truck security is lax’ Newsday, December 23, 2002
transporting hazardous materials, and developing new identification systems for drivers, possibly using biometrics technology. Some experts have suggested removing hazardous-materials warning signs from vehicles because they could help terrorists with target selection, but this may endanger first responders at regular accident sites. Other suggestions include restricting access for trucks carrying hazardous materials to particularly sensitive sites, and improving security at storage and transfer depots. Hazardous material transports could be equipped with GPS systems to monitor the location of dangerous vehicles and freight in real-time. If trucks carrying hazardous materials deviate from their pre-assigned route, technologies could be installed that allow for the engine to be disabled remotely to prevent a catastrophe. Such technologies are already under development and in experimental use.

Future Surface Transportation Security Measures
As has been explained, preventing attacks on surface transportation and mass transit systems is extremely difficult. Better physical security, vigilance, and an increased security presence will not prevent all possible attacks. Therefore, security strategies must focus on minimizing loss of life and disruption, and rapid recovery. Such successful consequence management will require excellent planning, coordination and training; sustained security funding; safer station and vehicle designs; the application of new tools and technologies; and creative thinking.

Planning and Coordination
Operators and authorities around the country are already engaged in intensive planning and coordination efforts, which include conducting thorough vulnerability and threat assessments to prevent and deter attacks, and respond to terrorist events. Training exercises and information sharing play a key role in this effort.

Funding
A recent GAO report found that, “According to our preliminary survey results and our interviews with transit agency officials, insufficient funding is the most significant challenge in making their transit systems as safe and secure as possible…the top three safety and security funding priorities of transit agencies are enhanced communication systems, surveillance equipment, and additional training.” The GAO further recommends that the Secretary of Transportation consider seeking a legislative change to allow all transit agencies to use federal urbanized area formula funds for security-related operating expenses. On January 14, 2003, Transportation Secretary Norman Mineta announced $15 million in Intercity Bus Security Grants through the TSA “to enhance security in the industry through initiatives such as driver protection, monitoring and...”

68 ‘DOT says 'hazmat' cargo label may draw terrorists’, Lee Bowman, Seattle Post-Intelligencer, November 23, 2002
69 ‘Deterrence, Protection and Preparation – The New Transportation Security Imperative’, Special Report 270, Panel on Transportation, Committee on Science and Technology for Countering Terrorism, Transportation Research Board of the National Academies, 2002
70 ‘Mass Transit – Challenges in Securing Transit Systems’, Testimony before the Subcommittee on Housing and Transportation, Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Statement of Peter Guerrero, Director Physical Infrastructure Issues, General Accounting Office, September 18, 2002
71 Ibid.,
communication equipment, passenger and baggage screening processes, and employee
training programs.”72

**Safer Stations and Vehicles**
Better surface transportation and mass transit security also requires making some changes
to vehicles and stations that could minimize their vulnerability to terrorism. Such
measures, which have been successful in the past in other countries and which are being
adopted by some operators in the U.S., include removing trashcans or replacing them
with blast proof container; removing materials that easily fragment or give off toxic fumes from vehicles and stations; improving lighting and lines of sight; installing
surveillance cameras; and locking storage and maintenance rooms. Other measures
necessitate thinking ahead and developing safer stations and vehicles. An example for
this would be building a subway station with good lighting, blast-resistant structures, air
filtration systems, emergency evacuation routes, and open spaces that provide broad
fields of vision.73 Better design will also produce additional benefits, such as reducing
crime, enhancing efficiency, and improving customer comfort.

**Tools and Technologies**
New tools and technologies should also be utilized to improve the security of surface
transportation and mass transit systems. Further research and development activity is
crucial in this area. Hazardous material transports could carry GPS tracking technology
and panic button and automatic engine-kill-switch technologies that could help halt truck hijackings in progress. In fact, GPS and other monitoring technologies could be used
more generally to check the location of passenger and freight vehicles. Smart card or bar
code technologies could be adopted for cargo containers or hazardous material transports
that could be used to check that shipments are in order. This could help identify and
screen high-risk transports, and prevent them from entering sensitive areas. Federal
agencies (including the Department of Energy’s PROTECTS Program [Program for
Response Options and Technology Enhancements for Chemical/Biological Terrorism in
Subways]) and the private sector are working on chemical, biological and radiological
detection devices and networks that could one day be deployed to provide early warning
of attacks involving WMD. The Washington Metropolitan Area Transit Authority
(WMATA) has received federal funding to install chemical detection systems at some of
its stations. If successful, this test project could be adopted by other surface transportation
operators. WMATA has further linked closed-circuit television (CCTV) surveillance
systems with intrusion detection software to provide timely notification of security
incidents.

72 ‘TSA announces grant program for bus security’, BusRide, January 20, 2003 -
http://www.busride.com/News.asp?Article=1037 or see ‘Secretary Mineta Announces $148 Million for
Transportation Security Programs To Fund Port, Intercity Bus, Cargo Grants’, Transportation Security
73 ‘Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on
Innovative Thinking
Due to its inherent vulnerability, the surface transportation sector will have to think outside the box to protect its facilities and passengers. While elaborate security checks involving screening devices or manual searches are impossible to implement at all access points, random checks in stations or upon entering vehicles may act as a significant terrorist deterrent. Using concealed detection and scanning devices at some locations may have a similar effect. Commercial bus carriers, including Greyhound, may start screening passengers for weapons with handheld wands at bus terminals. A more coordinated screening regime has not been fully ruled out for rail systems if the terrorist threat increases. However, such measures must be balanced against passenger privacy and convenience. Experts have also floated different kinds of passenger screening techniques for long-distance travelers that purchase their tickets in advance. This could involve feeding passenger information into a variety of government databases. However, such measures could be easily circumvented. Random passenger identity checks may be more effective. Marshals have also been proposed for surface transportation systems and may have a place in a comprehensive security strategy.

Conclusions
The transportation sector is important for the smooth functioning of society and the American economy. Given the inherent vulnerabilities of transportation systems to physical and cyber threats – both as targets and a weapons of terrorism – it is imperative that committed action be taken to deal with the insecurity of the sector. Since the Sept. 11 terrorist attacks, the perceived likelihood of such destructive events taking place has increased exponentially. In response, security has been heightened significantly in the aviation industry, making travel by air much safer. Initiatives have also been undertaken in the maritime sector to counter mounting threats, particularly in terms of cargo transportation. However, few measures have been implemented to enhance the security of the surface and mass transit sector, which is arguably the most vulnerable sub-sector because of the difficulty in developing non-prohibitive, cost-efficient security strategies.

Hence, although transportation security in the United States has been improved significantly since Sept. 11, vulnerabilities still remain throughout the sector. More effort in terms of a sustained commitment to the sector’s security, and additional funding is needed. Primary emphasis needs to be placed on high-vulnerability/high-impact areas where the best returns on investment can be expected; areas where vulnerabilities and threats clearly overlap also need to be addressed. A successful security strategy for the sector therefore depends on a rigorous assessment of the industry, appropriate prioritization of the assets, and comprehensive protective measures that also promote safe and efficient transportation.
Additional Resources

Reports


‘Combating Terrorism – Actions Needed to Improve Force Protection for DOD Deployment through Domestic Seaports’, United States General Accounting Office, Report to the Chairman, Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives – October 2002


Investigative Research for Infrastructure Assurance (IRIA) Group –
Institute for Security Technology Studies


‘Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview’, Brian Michael Jenkins, The Mineta Transportation Institute, College of Business, San Jose State University, October 2001 - [http://transweb.sjsu.edu/publications/TerrorismExOverv.pdf](http://transweb.sjsu.edu/publications/TerrorismExOverv.pdf)


Media Articles/Press Releases


‘Port security lagging’, Aldrin Brown, Orange County Register, November 24, 2002

‘Experts fear SA-7 missile poses threat to airliners’, Isabel Vincent, National Post, November 29, 2002
‘Shippers, ocean carriers scramble to meet customs deadline’, Linda Rosencrance, Computerworld, January 23, 2003
‘New York Senator Charles Schumer says truck security is lax’ Newsday, December 23, 2002

**Websites**
The U.S. Coast Guard has published security guidelines on vessels and port facilities (http://www.uscg.mil/hq/g-m/nvic/index00.htm).

**Legislation**

**Journals/Newsletters**


