

Special Report: Aftermath of Terror

Industries That May Be Vulnerable Race To Boost Security and Limit Disruptions

The attacks on the World Trade Center and the Pentagon have touched off a storm of inspections and analysis by government and industry officials asking the same grim question: What city, or what structure, might be next?

Authorities haven't divulged evidence of any impending attacks, but precautions are proliferating nonetheless. At water reservoirs around the country, security is tighter and recreation is prohibited. Power stations, chemical plants and tourist attractions are under increased watch. Densely populated and high-profile areas are widely considered the most likely potential targets. Depending on what they want to accomplish, terrorists could train their weapons on traditional wartime targets, such as military bases, or key infrastructure, such as electrical grids. They could attack with computers, with bombs, with hazardous chemicals or with biological agents.

"The book on terrorism risk is being written as we go along," says Dick Andrews, vice president for emergency planning at **ABS** Consulting, a firm that often advises governments on disaster-preparedness. The tack local and state governments have taken so far is to identify possible targets and vulnerable spots in their own areas, such as military installations, large sports stadiums and well-known attractions.

Redundancy is an important principle of infrastructure security. Computers, electrical power lines -- anything that might be damaged or destroyed -- needs a fall-back system. Even more important are common-sense measures, Mr. Andrews says. Water officials, for example, might decide to keep vehicles at least 100 feet away from a crucial pumping station to limit the risk of damage from truck bombs.

But the most effective protection is increased intelligence-gathering, terrorism

experts emphasize. State and local officials are working with the Federal Bureau of Investigation and other agencies to identify targets, but they concede they have no idea where terrorists might strike next.

Wall Street Journal reporters around the country looked at the vulnerabilities of particular infrastructure, industries and other areas and how they are being addressed. Their findings follow.

Bridges

At first glance, it might appear that bridges would be tempting targets. But most of the nation's approximately 600,000 bridges probably aren't attractive for terrorism because they are so lightly traveled, says Paul D. Thompson, a Castle Rock, Colo., bridge-design consultant. "Even on a huge bridge, the number of fatalities would be so small," he says.

Still, the Golden Gate Bridge in San Francisco has been closed to pedestrians and bicycles since the morning of the attacks and will remain so at least until Friday. "The bridge is an icon that is recognized around the world, and we have to be mindful of that fact," says Mary Currie, a spokeswoman for the Golden Gate Bridge, Highway and Transportation Districts.

In New York, the George Washington Bridge is under stricter watch, says Dan Bledsoe, a spokesman for the Port Authority of New York and New Jersey. Law-enforcement personnel have an increased presence, he says, and have been told to inspect vehicles entering the bridge when necessary.

-- Sarah Lueck

Water Supply



AP Photo

Police officers in New York checked a panel truck crossing the Manhattan Bridge from Brooklyn.

A major source of concern among the public is the nation's water supply. "It's a great fear, but it's not so real," says Luciana Borio, a senior fellow at Johns Hopkins University's Center for Civilian Biodefense Studies. Dangerous bacteria that might be dumped into a reservoir are likely to be diluted before they reach the public, and purification systems probably would kill them before they were consumed. Still, Dr. Borio warns, "just because we think [biological attacks] are hard doesn't mean they can't happen."

Perhaps a more realistic worry is that terrorists would cut off the water supply to a populated area. Most communities already have redundant

In an effort to ease congestion, new traffic rules went into effect Thursday allowing only cars with two or more passengers to enter lower Manhattan before noon.

water systems, with alternative pipelines and tanks in case main sources are disrupted, says Diane VandeHei, executive director of the Association of Metropolitan Water Agencies, which represents some 350 water agencies supplying cities with populations of more than 100,000. Within the next six months, the agencies will have an electronic-information exchange that will allow them to communicate with the federal government about potential threats in encrypted messages, she says.

Since the attacks, water supplies are getting more scrutiny and security. In New York, recreation such as fishing and hiking at the state's 19 reservoirs is banned, and roads that pass over areas of open water are under guard -- all to protect a system that supplies nine million people. Water inspectors have increased testing and sampling. "It's costing us a lot of money," says Charles Sturcken, chief of staff at the New York City Department of Environmental Protection.

-- Sarah Lueck

Chemicals

Thousands of chemical plants across the country harbor storage tanks and pipelines full of deadly materials; if released through a rupture or explosion, these chemicals could spread poison clouds that could injure or kill on a large scale.

By the afternoon of Sept. 11, major chemical companies had activated crisis plans and heightened security measures at all their plants around the world. Industry safety experts are now taking a fresh look at their safeguards to see if they are adequate. "The rules have changed," says Susan Roth, a spokeswoman for the American Chemistry Council, an industry group. "The kinds of threats we're looking at have expanded."

Many chemical plants are surrounded by residential neighborhoods, schools and businesses. The industry's vulnerability was highlighted in 1984 by the spill at a Union Carbide plant in Bhopal, India, where casualties were on par with those of the World Trade Center attacks. In 1999, U.S. industry officials protested a law that required companies to evaluate their "worst-case scenarios" for a chemical disaster and post the details on the Internet. The requirement was scaled back after the Federal Bureau of Investigation's chief of domestic terrorism, Robert M. Burnham, testified before Congress that such details "would provide targeting tools and new ideas to criminals and terrorists."

Dangers also exist outside plants. Truckloads of dangerous chemicals could be hijacked in transport. Terrorists might steal or purchase large amounts of innocuous chemicals that could be used to make more deadly agents, says industry safety consultant Rod Gerwe. The chemistry council's Ms. Roth says the industry is working closely with government agencies to assess those threats.

A U.S. Justice Department project to calculate the vulnerability of chemical plants to terrorism is under way and may now be speeded up.

Meanwhile, companies are re-evaluating the amount of chemical information they provide on their Web sites. They have stepped up security patrols, begun expanding video surveillance, closed plant entrances and clamped down on visitor access. Many companies are cooperating with the rail and trucking industries to strengthen security for transporting chemicals, including screening drivers. Some companies are considering closer screening of their own employees, as well.

-- Susan Warren

Electrical Power

The nation's electrical system is too big to fully protect against attack. But it has one primary defense against disaster: redundancy.

The electric system is designed to remain energized despite the occasional loss of power plants or transmission lines. Electric-grid operators can quickly ramp up power plants that are standing by or reroute electricity over alternate pathways.

But geography makes supplying electricity to some places more problematic. Manhattan and San Francisco, for example, have relatively few in-city generating plants and, because they are largely surrounded by water, have limited options for bringing in power if primary transmission lines are damaged.

Some grid officials worry not enough is being done to bolster redundancy. Terry Winter, chief executive of the California Independent System Operator, which manages that state's high-voltage transmission system, says the trend in recent years has been to add more or bigger cables to existing power-line routes instead of creating new ones that would add redundancy. It's cheaper, and avoids fights with residents who don't want transmission lines near them.

Since the Sept. 11 attacks, security improvements have largely focused on protecting the nation's electric-system nerve centers. That means grid-operator control rooms -- which already occupy unmarked, guarded buildings -- are being more heavily patrolled. And computer systems are again being checked for resistance against hacker attacks.

In addition, officials worry about the security of nuclear power plants. Critics say they aren't adequately shielded against terrorist attack. The Nuclear Regulatory Commission intends to re-examine security measures.

Even so, "I'm very concerned about where these attackers may want to go next," says William Museler, chief executive of the New York Independent System Operator.

Theme Parks

Adding more visible security is tricky for theme-park operators like [Walt Disney Co.](#) and [Vivendi Universal SA's Universal Studios](#), which have built their image on escapism and don't want to pop the bubble of fantasy. At Disney, for example, security has always been present but low key. People familiar with the company say that its security department has long employed former government agents who can interact with the intelligence community. Disney also has bomb-sniffing dogs that go through the parks at night, and trains its staff in identifying unusual situations or objects. Disney has debated using metal detectors at its gates, but never has.

Throughout the current crisis, Disney officials have said that law-enforcement and government officials tell them there is no reason to believe the theme parks should be considered any more of a target than other public places. Nonetheless, the Disney parks have added checks of backpacks and the like at their front gates. Universal says that it has also "heightened security" at its parks in Florida and California. That means bag checks at the gate, armed guards and metal detectors at its park in Universal City, Calif.

Disney said that crowds were again on the rise throughout last week in both Florida and California, and attendance over the weekend was much closer to normal—down about 10% to 20% from the same period a week ago.

Universal also reported stronger weekend crowds. Both companies said they were drawing more heavily from the local area around each park, as airplane travel by tourists continues to be light. Weekday attendance continues to be a bigger challenge.

—Bruce Orwall

Stadiums

With crowds of as many as 100,000 packed like marbles in a jar, and a relatively relaxed atmosphere, sports stadiums have always been areas of security concern. Yet the most dramatic attack on a sports site has been in fiction—a terrorist-piloted blimp that crashes into a Super Bowl in the book and movie "Black Sunday."

"We've always had the situation where someone who is bent on smuggling in a weapon and really trying to do something could do limited damage," says Milt Ahlerich, the National Football League's director of security and a former FBI agent. "I think people are more than willing ... to put up with a little inconvenience to feel safe when they're in the stadiums."

Since the attacks, pro leagues, colleges and even high schools have stepped up

security measures. League security officials have consulted with the FBI, the Secret Service, the Federal Aviation Administration, the Treasury Department's Bureau of Alcohol, Tobacco and Firearms, and others on how to bolster security. Much of the extra protection is behind the scenes: Bomb-sniffing dogs scoured Miami's Pro Player Stadium before a National Football League game there last Sunday, while planes were banned by the FAA from flying within three miles of certain events, unless they were descending into a nearby airport. That ban will remain in effect through this weekend, an NFL spokesman says.

Leagues and teams are advising fans to arrive at least 30 minutes earlier than they normally would to accommodate the new checks, which include car inspections in and around parking lots. The NFL has banned all coolers, backpacks, bags, fanny packs and large purses from stadiums indefinitely, and some teams are using walk-through metal detectors and wands at stadium gates. Security officials at PacBell Park in San Francisco, where baseball's Giants play, even have patted down children as they entered the park.

—*Stefan Fatsis*

Pipelines and Refineries

Pipelines that move natural gas and petroleum products have historically been targets of terrorism in other parts of the world. In Colombia, rebel groups have been bombing pipelines for years, in part because many are located above ground. "But even places where they go below ground have been targeted as well," says Frank Cilluffo, senior policy analyst with the Center for Strategic and International Studies, a Washington, D.C., think tank.

In the U.S., pipelines are typically 3 to 6 feet below ground. But information about the U.S. natural-gas pipeline grid has become more available due to deregulation, Mr. Cilluffo says. Detailed maps of each company's gas pipeline systems have been handed out at trade shows.

This kind of specific information has created problems in other countries. Five years ago, using information made available through industry deregulation, the Irish Republican Army tried to take down the United Kingdom's electric power grid. The attempt failed.

While pipeline companies face a daunting challenge trying to guard thousands of miles of lines, they do have systems in place to mitigate potential damage caused by a bombing. [Kinder Morgan](#) Inc., Houston, has sophisticated computer programs that will immediately shut down lines when they detect changes in pressure or flow rate, says Larry Pierce, a company spokesman.

Like chemical plants, refineries, which turn crude oil into the gasoline, jet fuel and diesel needed to run the country's transportation, are vulnerable. Since the attacks, refiners have beefed up security at plant gates and at docks where some coastal refineries receive their crude.

Buildings

Landmark buildings around the country have tightened security dramatically since two of the nation's best known towers were destroyed by suicide terrorists. Of course, security guards can't foil planes coming down from the sky, but they are taking steps to block attacks from the ground.

From New York's Empire State Building to Houston's Pennzoil Place to San Francisco's Transamerica Tower, building occupants who once walked straight to the elevators now must be screened by security guards who inspect their employee badges.

The John Hancock Building, Boston's tallest, permanently closed its 60th-floor observation deck, which had long been a source of security concern because it didn't have a dedicated elevator entrance and gave tourists access to the entire building. John Heavey, security director, says it was "the prudent thing to do."

The Empire State Building will open its observation deck to tourists this weekend for the first time since Sept. 11, but it will remain on a weekend-only schedule and only the Fifth Avenue entrance will be open, for an undetermined period, a spokeswoman says. The building has placed metal detectors and bag-screening stations at all five entrances for tenants and their visitors. Last week, when only one entrance was open, morning lines lasted two hours, one tenant says.

At the Sears Tower in Chicago, America's tallest building, tenants must display photo IDs to security guards and visitors must show driver's licenses and submit their bags for searches. A spokesman says access to loading docks has also been tightened. The observation deck has been temporarily closed.

—William M. Bulkeley

Agriculture

The clearest threat involves the nation's 4,000 crop-dusting aircraft. The federal government temporarily grounded crop dusters after investigators learned Mohamed Atta, a hijacker on one of the planes that flew into the World Trade Center, had researched aerial-spraying technology before the attack.

Bioterrorism experts have warned for years that a crop duster is uniquely equipped to quickly disperse deadly chemical or biological agents over a wide area. A crop duster, which carries hundreds of gallons of pesticide, is hard to track on radar. It hugs the ground and isn't equipped with transponders. But it is hard to fly and an unlikely hijacking target: Most have one seat.

Crop dusters are back in the air but banned from flying near major metropolitan

areas. The industry is taking inexpensive steps to increase security, such as locking chains around the propellers of idle planes. New models need an ignition key.

Fertilizer manufacturers are beefing up security around processing facilities that use poisonous gases and explosive chemicals to make their products. Most companies already employ guards and security cameras.

The U.S. Agriculture Department has told hundreds of government veterinarians stationed around the nation to keep a sharp eye out for any terrorist attempt to introduce animal diseases into the U.S. Of particular concern is foot-and-mouth disease, the highly contagious virus devastating the livestock industry in Britain.

—*Scott Kilman*

Railroads and Trucks

"I think everything is high threat now, there is no low or medium," says Edward R. Hamberger, president and chief executive officer of the Association of American Railroads, a trade group. "The good thing is that we are contained, definable. You can't hit a building with a train."

So far, railroads have stepped up inspection of equipment and tracks and beefed up security around bridges, tunnels, dispatch offices and telecommunications centers. They have increased their communications with federal transportation, military and security agencies. The industry brought in experts in foreign intelligence and Department of Defense operations to identify specific vulnerabilities.

Mr. Hamberger says he isn't aware of any credible terrorism threat against the rail industry.

Each major railroad has its own police force with powers to arrest, cross state lines and carry weapons. Now, there is additional thought to providing railroad police with counterterrorism training. Railroads also are considering new train-control systems that can automatically apply the brakes of a freight train in case of a hijacking or runaway train. Installing such a system on the nation's major rail routes would cost more than \$1.2 billion. For now, the main option for railroads is to derail such trains.

Trucking companies are tightening security at freight terminals with new electric fencing and are issuing identification badges to employees for the first time. They are urging drivers to exercise extra care while on the road, staying with their trucks as much as possible and frequenting familiar truck stops. Some companies are boosting the installation of satellite tracking systems for their trucks and trailers so they know where they are at all times.

Trucking executives say they aren't aware of any terrorists' plots involving the industry. But they are cooperating with government agencies that this week

stepped up background checks of drivers with permits to haul hazardous materials. These officials say that all the new security measures are increasing their costs, which they will have to pass on to customers.

—*Daniel Machalaba*

Seaports and Coastlines

Coast Guard stations around the country have tightened security substantially, and several ports that support industries such as tourism or petrochemicals are stepping up vigilance.

More than 30 Coast Guard vessels are currently deployed in New York Harbor. Across the nation, the Coast Guard is enforcing a range of new security measures on all ships entering U.S. ports. It already required overseas ships to provide a 24-hour alert of their pending arrival; now, that notification is being applied to all ships and must include identification of everyone aboard, the Coast Guard says. Contrary to persistent rumors, the Coast Guard says it is not denying entry to ships from specific countries.

The real action, however, is at the port level. In Houston, concern is raised by its status as the second-busiest petrochemical port in the world, as well as the adjacent 54-mile Houston ship channel. "The potential for that nightmare scenario exists on the shores and moves up and down the ship channel every day," says Petty Officer James Dillard. He says the Coast Guard is stepping up patrols of the ship channel and the shoreline—home to more than 100 industrial facilities—and the number of ships boarded for inspection has increased 20% since before the attacks.

In Miami, Coast Guard vessels are escorting all inbound and outbound cruise ships, cargo ships and tankers. In addition, the Guard has instituted a 100-yard security zone around each ship. A kayaker who violated the zone was stopped and then escorted out of the zone, says the Coast Guard's Luis Diaz.

In San Francisco, Coast Guard boardings are up slightly. The decision on whether to board is made after a review of several different factors, with the ship's country of origin being only one of them, says Tim Callister of the Coast Guard's San Francisco office.

—*Chris Adams*

Computers

The Bush administration for months has privately expressed concerns about the security of the Internet's 13 most important computers, called root servers, which manage global Internet traffic. These computers, controlled by universities, corporations, government agencies and research centers, are located throughout the U.S. and in Tokyo, Stockholm and London. "They are the most

important computers running out there," says Chris Wysopal, a cybersecurity expert for At Stake Inc. in Cambridge, Mass. "There would be major problems if they were to go down."

Some of these computers, such as the primary "A" root server in northern Virginia, operate within secure buildings, but others are far less protected. When congressional auditors recently checked the security surrounding them, "one of them was sitting in a professor's office at the University of Maryland," says Keith Rhodes of the General Accounting Office. "I would worry."

These computers act as master directories for the Internet, matching numerical addresses with more familiar Web-site names. The primary root server periodically sends replicas of the master directory to the other servers, which act as redundant backups and help prevent the primary server from being overwhelmed with data queries.

An official of the organization that coordinates the technical management of the Internet, the Internet Corporation for Assigned Names and Numbers, acknowledges there is "obviously a range of security on the root servers."

This official notes that during testing for the year-2000 rollover, experts determined that even the loss of nine of the 13 root servers would have only marginal impact on global Internet traffic. However, other experts point out that each of the root servers runs similar software. "They're redundant in that if you can bring one down you can bring down all of them," says Peter Neumann, a security expert at SRI International in Menlo Park, Calif.