Manhole Security

Protecting America's Critical Underground Infrastructure

Irwin M. Pikus, PH.D., J.D.

November 2006

Table of Contents

Irwin M. Pikus, Ph.D., J.D.

Dr. Pikus is a physicist and attorney who served the United States government in Senior Executive positions dealing with science, technology and national security over a 25 year span. Prior to that, Dr. Pikus led research projects in the aerospace and electronics industry. He was appointed a Commissioner of the President's Commission on Critical Infrastructure Protection and since his retirement from government service has provided expert and consulting services in critical infrastructure protection to a number of public and private organizations. He is currently Visiting Professor of Systems Engineering at the University of Virginia. Dr. Pikus chairs the Methodology sub-committee of ASCE's Water Infrastructure Security Enhancements Standards Committee and was principal investigator for the ASCE-EPA project on early warning systems for water utilities.

Acknowledgements

The following individuals provided comments and insight critical to the development and editing of this paper:
Ed Badolato, President & CEO of Integrated Infrastructure Analytics, Inc. (IIA), and former Deputy Assistant Secretary for Security, Department of Energy (1985-1989);
Ronald W. Bergmann, Los Angeles Deputy Police Chief (Retired);
Tony Hurley, Director of Operations Support for Toledo Edison, Board member, FBI InfraGard Network, Toledo chapter;
Paul M. Joyal, Vice President, National Strategies Inc. and former Director of Security for the US Senate Select Committee on Intelligence (1984-1989);
Dr. Conrad Keyes, Emeritus Professor of Civil Engineering, University of New Mexico, and Chair of the Water Infrastructure Security Enhancements Standards Committee of ASCE;
John A. McCarthy, Executive Director, Critical Infrastructure Protection Project, George Mason University;
William Odom, Lieutenant General, US Army (retired), and Senior Fellow at the Hudson Institute.

Executive Summary

Over the past five years, a series of terrorist attacks around the globe created new imperatives to protect civilian populations. High among these priorities is maintaining the integrity of a nation's critical infrastructure. Most citizens take for granted the vast utility network that lies underground in nearly all major urban areas. Lying just a few feet beneath the pavement is a complicated web of pipes, wires, cables, and other conduit that transport electricity, natural gas, telecommunications, potable water, waste, and steam. In addition to the utility networks, particularly in urban areas, much rail transportation and some road traffic is underground. The entirety of this network is accessible through one common avenue – manholes.

Manholes are simply the street side access point to underground infrastructure including public utilities and telecommunications. They are mostly found in urban areas, where a substantial portion of critical infrastructure is housed underground. However, the overwhelming majority of manholes in the United States are not secured.

The lack of manhole security provides terrorists and other individuals intent on doing harm and damage with considerable opportunity to easily disrupt and damage business and commerce, and generate significant loss of life and injury. It is therefore imperative that high-risk manholes be secured.

Manholes of the highest risk of attack and most severe consequences – classified as Tier I – are located at critical utility junctions and/or near strategic locations. A manhole supplying access to an electrical transformer near the New York Stock Exchange is an example of a strategic location. The second highest risk manholes – Tier II – are found in or near key landmarks including transportation hubs and centers of commerce or government. For example, a manhole near the Lincoln Memorial is a Tier II manhole. A manhole found on a main street in a suburban center is a Tier III manhole, and a manhole located in a National Park is classified as Tier IV.

Categories of Risk and Consequences of Attack on Manholes

Category	Risk Level	Consequences	Characterization
Tier I	High	Severe	Strategic locations including: urban centers; key infrastructure intersections; centers of business, industry, and government
Tier II	Moderate to High	Moderate to Severe	Significant landmarks, transportation hubs, public gatherings
Tier III	Moderate to Low	Moderate to Low	Suburban areas; rural and agricultural regions
Tier IV	Low	Low	Rural/low-population density areas; national parks; wildlife centers

Given the importance of securing manholes in protecting critical infrastructure and key resources, an analysis of various alternatives for manhole security was reviewed. The most practical, effective, and affordable solution to protecting critical underground infrastructure is to secure Tier I and II manholes with a self-contained, independent, and locking manhole barrier device.

Securing manholes is a vital step to ensuring the protection of the United States' critical infrastructure and critical assets and thwarting terrorist and other intentional attacks. To that end, we recommend that Congress take the following steps:

1. Examine new statutory requirements that Tier I and II manholes be secured nationwide by both public and private sector entities. Examine requiring the owners and operators of manholes to assess vulnerabilities and identify tier I and II manholes.
2. Examine appropriating and allocating new funds for urban centers and strategic locations to purchase and install manhole barrier devices for all Tier I and Tier II manholes.
3. Examine incentives such as tax and insurance credits for owners of manholes, including municipalities and corporations – particularly utilities and telecommunications companies – to purchase manhole barrier security devices, and direct the Department of Homeland Security to include manhole security in best practices, policies and procedures.
4. Examine supporting further direct study of this issue by GAO and CRS.

Without manhole security, the United States risks suffering significant consequences resulting from open and spontaneous attacks on underground infrastructure including incalculable economic damages, large numbers of civilian casualties, and considerable disruptions to our urban way-of-life.

Introduction

Most governments rely on critical infrastructure and key elements to ensure quality of life, economic prosperity, and national security. This infrastructure is vulnerable to disruption and degradation from natural disasters, accidents, vandalism, and terrorist attacks. In large urban centers, critical segments of this network lie just below the surface of sidewalks, roads, parks, and buildings. Protecting these assets and limiting access to them is a central objective in homeland security.[1] In fact, the 9/11 Commission noted that funding for emergency preparedness should be allocated based on risks and vulnerabilities, and that funding also address the need for teamwork across public and private sector entities.[2]

Protecting infrastructure that is on or above the surface is accomplished by either deterring or deflecting attacks, hardening, or limiting or preventing unauthorized access. For example, erecting protective walls, fences, and other structures, using monitors or guards, and even camouflaging key resources are all familiar techniques for protecting critical infrastructure. In contrast, securing the underground network in large population centers requires a different approach.

The underground infrastructure in American cities is vast. Among the critical networks having substantial and vital elements below the surface are:

> **Communications** – telephone lines, cables, fiber optics, and a variety of switching, relaying and controlling apparatus are often underground. These systems carry financial transactions, emergency communications, sensitive and often classified government communications, in addition to private communications and entertainment.
>
> **Electric power** – some power generating stations, transmission lines, control and transformer apparatus and much of the power distribution system is below the surface. Electricity has become an essential resource and large power outages have widespread impact throughout the economy and society as a whole.
>
> **Natural gas and related energy** – natural or manufactured gas as well as gasoline and other petroleum products are transported through subsurface pipelines not only in cities but in many outlying areas as well. In some locations, centrally produced steam is also distributed through underground pipes.
>
> **Water supply** – most of the water distribution system, water storage, as well as some treatment facilities and raw water transport lines are below ground. Potable water is essential to maintain public health and proper sanitation, fire fighting, and a wide range of other industrial, business, and personal applications.
>
> **Wastewater and storm water** – disposal of wastewater and storm water runoff is largely through underground pipes and tunnels. Public health can be severely affected if this system fails to function properly.
>
> **Transportation** – particularly in urban areas, much rail transportation (including commuter, long distance and some cargo traffic) is underground. In addition, in several locations even road traffic is routed substantial distances through subsurface tunnels.
>
> **Underground courses** – provide unmonitored and uncontrolled access to buildings and facilities connected to certain of these infrastructures.

Underground infrastructure must be accessible in order to perform routine maintenance, repairs, upgrades, and monitoring and control functions. The usual method for providing access to underground infrastructure is through portals in the surface – manholes.

Manholes are simply the street side opening to an underground vault used to house access points to a variety of public utilities. Covers generally are round to prevent them from falling inside the hole, are made primarily from iron, and typically weigh around 100 pounds.[3] Manhole ownership varies from location to location and as a result of large networks of private manholes, most provide access to only one or two utilities. In a number of the nation's largest cities, a substantial number of manholes provide access to multiple infrastructures.[4]

The most common type of manhole covers rely on their weight to sustain coverage under foot and motor traffic as well as to hamper unauthorized access by vandals. Despite their weight, it does not require significant effort to remove a manhole cover. In fact, hooks or pry-bars allow an individual to easily and quickly lift a cover.

Pranksters and scrap metal thieves continually demonstrate that the weight of the manhole cover is not adequate to secure access to the critical infrastructure located underground in American cities. For example, theft of manhole covers increase when scrap metal prices rise in some urban areas.[5] There are a number of approaches to securing manholes by controlling access to the cover. Most of these approaches focus either on locking the cover itself, detecting intruders, or physically sealing or hardening of the manhole. These approaches utterly fail in purpose and cost. Aside from being wholly cost-ineffective, they fail to provide a usable and practical security mechanism.

This paper provides an analysis of the risk to the subterranean critical infrastructure in the U.S., and suggests the most practical, effective, and affordable mechanism for securing Tier I and II manholes – a self-contained, independent, and locking manhole barrier device.

Ownership and Control of Manholes

There are over 22 million manholes in the United States and their ownership and/or control does not follow a simple rule. In some jurisdictions they are owned or controlled by municipal authorities while in others, private entities own and control them. In the case of private ownership and control, even when several infrastructures are accessible through the manhole, there is typically a single owner of the access portal. In these cases, contractual agreements dictate that all the relevant enterprises can provide access and exercise a measure of control of the manhole.

The entry portal – the manhole cover – is most frequently on the surface in a public area, such as a street or sidewalk. Regardless of manhole ownership, municipal authorities govern the general characteristics of manhole covers pertaining to their effects on pedestrian and motor traffic, and outline parameters for when and how work in manholes may be conducted. The proper functioning of underground infrastructure is the responsibility of the owner/operator of the infrastructure. To the extent that malfunctions might affect public interests (mainly safety), municipal authorities can impose constraints and liabilities on the underground infrastructure itself.

At present, the responsibility for protecting underground infrastructure from attack is with the owner/operator of individual components of infrastructure. In situations where several networks are accessible through a single manhole, responsibility for security is shared through contract. There is currently no federal legislation requiring protection of manholes from intruders or unauthorized personnel; however, FEMA recommends that all manholes over 10 inches in diameter in strategic locations be secured to prevent unauthorized opening.[6] Nor is there any evidence of state or local laws or ordinances on the subject. In fact, the 9/11 Commission noted that funding for emergency preparedness should be allocated based on risks and vulnerabilities, and that funding also address the need for teamwork across public and private sector entities.[7]

Characterizing Manholes and Underground Infrastructure

The number of manholes in a city and the types of infrastructure accessible in each manhole are highly variable. Population density, the city's age, and the mix of public and private ownership are key factors in determining the nature of the underground utility network. For comparative purposes, this paper provides an overview of underground utilities and manhole density for the cities of New York, New York, and Los Angeles, California; describes additional data on Washington, DC and Baltimore, Maryland; and extrapolates that data to the broader U.S. population.

New York City

Manholes in New York City are owned and maintained by public and private utility and telecom companies. As a result, manholes in New York are highly specialized to service only the utility that owns that space. Estimates for the total number of manholes in the city range as high as 600,000.[8] Manholes normally represent the start and stop of various utility conduits, and points where two conduits join together. The hole generally measures 12 feet by 8 feet, with a depth of approximately eight feet. Despite their covers, manholes in New York, particularly those housing the power infrastructure, are often at least partially filled with water and muck washed down from the street above.[9]

Manholes in New York City house the following critical infrastructure:

- The Empire City Subway Company (ECS), a subsidiary of Verizon, was granted exclusive right to build and lease underground infrastructure for all communications services in Manhattan. ECS owns 11,000 manholes and 58 million feet of varied conduit. It rents space mostly to telecommunications and cable providers and its lines carry everything from traditional phone calls to signaling for fire alarms, traffic lights, and police call boxes.[10]

- Unlike most parts of the U.S., New York City's local power distribution network is largely underground. Most of the transformers used to step down electric voltage to the level required in residential or business use are located in underground rooms or vaults. Connecting businesses and residences to the underground network would be impossible without manholes.[11]

- Con Edison, New York City's energy provider, owns and maintains 83,043 miles of underground cable and 246,092 manholes in the five boroughs, 20,630 miles of underground cable and 59,120 manholes are owned and maintained in Manhattan alone.[12]

- Gas manholes in New York contain pressure checkpoints called "regulators." These devices can automatically increase or decrease the flow of natural gas to meet certain pressure levels. Maintaining the correct pressure in natural gas lines is essential to maintain service.[13]

- Steam pipes are also owned and operated by Con Edison in New York. These pipes are located between 4 and 15 feet below ground. Manholes are used to provide access to valves and vents for errant steam created by water coming in contact with service lines.[14]

- New York City's sewer system includes over 6,000 miles of pipes ranging from 6 inches to more than 89 inches in diameter. Sewer manhole covers contain slots, or vents, in them to provide for ventilation of any gas building up underground and avoid possible explosion. The spacing of manholes depends on the size of the pipe – the larger the pipe the less likely it will clog thus allowing a wider distance between manholes. Sewer manholes are composed of a shaft that widens from two feet at the top to four or five feet at the bottom to allow a bit of maneuverability.[15]

Los Angeles

Ownership of manholes in Los Angeles is split between the local government and private utility companies. The majority of manholes are owned by the city through the Department of Public Works and the Department of Water and Power. Natural gas and telecommunications utilities own the remaining manholes, some of which are the smaller square and rectangular vaults that provide access to valves and other regulators. Based on publicly available information noted below, it is estimated that nearly 200,000 manholes exist in LA; this does not include vaults, hand holes (small openings with access to valves), or other related access points.

The underground utilities and infrastructure in Los Angeles includes:[16]

- The Los Angeles Department of Water and Power (LADWP) is a wholly-owned city entity. LADWP provides all water and electricity services to city residents. Los Angeles encompasses approximately 470 square miles making the Department one of the largest municipal utilities in the U.S. LADWP owns 13,081 manholes, 11,230 square/rectangular vaults, 13,000 hand holes, and 20,000 underground transformers.

- The Department of Public Works, Bureau of Sanitation holds the responsibility for all solid waste collection and wastewater collection and treatment in Los Angeles. The Bureau owns and maintains over 140,000 manholes, most of which are located on public streets.

- Natural Gas service in Los Angeles is provided by private industry through Sempra Energy. Sempra does not maintain traditional manholes in the city, rather their service is regulated through a series of square and rectangular vaults at street level.

- Telecommunications, internet, and cable services are all provided through private industry in Los Angeles, primarily through AT&T, Verizon, and Time-Warner Cable. These companies do not provide public data on the number of manholes they own and service in Los Angeles, but estimates are in the tens of thousands.

Washington, DC and Baltimore, Maryland

Ownership of manholes in Washington, DC is largely private. Potable water, sewage and wastewater, electricity, telephone service, and natural gas-lines conduit all run beneath city streets and sidewalks. In Baltimore, manhole ownership is split between public and private entities. Potable water and wastewater and sewage systems are all owned and operated by the city's Department of Public Works, Bureau of Water and Wastewater. Telephone service, electricity, and natural gas utilities are the property of private companies. Total estimates for numbers of manholes in these two cities are not available, however some individual data exists:

- The DC Water and Sewer Authority (DC WASA), a semiautonomous entity, manages 1,300 miles of water lines, 675 miles of sanitation pipes, and 652 miles of combined pipes. In total DC WASA owns and maintains 48,990 manholes to service its sewage and wastewater management system.[17]

- The City of Baltimore's Bureau of Water and Wastewater owns and maintains 3,400 miles of water lines, 9,100 fire hydrants, and 16,000 manholes. The manholes provide access to both the water and wastewater network.[18]

Extrapolating to the National Level

Based on the data noted above for Los Angeles and New York City, as well as similar data for Washington DC and Baltimore, we can extrapolate a total estimate of the number of manholes in the United States. In general, manhole data is not specific and not necessarily complete (for example, our research did not provide estimates of number of manholes servicing natural gas utilities). This estimate provides a rough calculation for the number of manholes that may exist in the U.S., but is likely an underestimate. Adjusting for population size, it is possible to estimate the total number of manholes in the U.S. at approximately 22 million.[a] This estimate includes all categories of manholes at all tiers of risk.

a Estimate of total number of manholes in the U.S. was calculated using the following formula: (Number of Manholes in Service Area) x Total U.S. Population = Population of Service Area

Potential Threats to Underground Infrastructure through Manholes

Though there is no federal law, given the importance of the underground utility and telecommunications infrastructure accessible through manholes, the federal government and, in particular, the Department of Homeland Security and Federal Bureau of Investigation (FBI), have noted the importance of securing manholes from potential attack and sabotage.[19]

There are several possible objectives for potential attacks on underground infrastructure through manhole access:

- Corruption of communications capabilities (producing interfering/jamming signals into telecommunications systems);

- Complete disruption of critical utility service (severing electric power, water, gas or telecommunications lines; destroying key regulatory and control apparatus);

- Contamination of potable water and/or air (introducing a toxic biological or chemical agent into drinking water; release of chemical or biological agent in a mass transit system);

- Theft and misappropriation (tapping information flows; siphoning energy; gaining surreptitious control over information systems);

- Divert attention from another larger attack or disrupt critical utility service to assist with another attack;

- Use conduits to inject and transport gas or chemical vapors and/or liquids into buildings to initiate an evacuation, introduce poisoning, or as a means to facilitate an explosion.

To achieve any of the objectives noted above, a terrorist need only gain access to one or more strategic manholes. There are many costs associated with such a security breach, ranging from loss of life and injury, to eroding public confidence, to significant economic damages. Officials at all levels of government train regularly in preparation for attacks and natural disasters. In a cyber warfare simulation conducted by the U.S. Naval War College in July 2002, coordinators of the scenario estimated that even if terrorists had access to over $200 million, state-level intelligence, and five years to plan that a coordinated cyber warfare attack would damage key elements of the U.S. online infrastructure, but not cripple the system. However, one simulation leader noted that *"a satchel bomb thrown down a manhole in Manhattan would be far easier, far cheaper, and still fairly destructive."*[20]

The following provides greater detail into the consequences of an attack on critical infrastructure:

Disruptions to Communications Capabilities

Surreptitious intrusion into telecommunications and information systems would be difficult to detect but could result in corruption of critical messages and databases. While these consequences are unlikely to include death or serious injury, they could seriously affect matters of governance such as national security and the economy. If contemporaneous with an emergency event, disruption could then amplify the deadly and injurious effects of that event by disrupting essential emergency communications.

Widespread Power Outages

Disruption of electric power distribution lines could have widespread economic impacts to businesses, consumers, and government. In most cases, however, the site of the disruption can be somewhat readily located and the outage could be fixed without extensive delays. On the other hand, destruction of transformers or control gear could take considerably longer to repair with consequent longer duration outages. Many critical users of electric power such as hospitals and nursing homes have emergency power supplies but these usually have the ability to run for only a few days. Outages longer than that could cause major health problems along with serious economic and governance problems.

Threat to Potable Water and Sewer System

A number of studies have shown that toxins, particularly biotoxins such as ricin and abrin, are available in large quantities and can be introduced into municipal water supplies in quantities sufficient to cause thousands of deaths as well as widespread illness. These chemicals can be injected into water supply pipes through the use of a pump (whose output pressure just exceeds that of the pressurized line) and a small valve, e.g. a bleeder valve. It would take only a couple of hours to set up an apparatus to perform the contamination within a manhole and it could operate as long as the quantity of contaminant held out. Finding the source of contamination would likely take much longer than the contamination process and consequent effect to be accomplished. Such an attack would not only cause personal injuries but would likely have a very strong effect on morale and public confidence. Sewage lines are not generally recognized as potential targets but, in fact, very serious consequences can ensue from several kinds of attack. For example, dumping quantities of volatile materials can produce a highly explosive situation causing economic damage as well as personal injury.[21] Moreover, there is the potential for disrupting the bacterial processors that sanitize sewage into environmentally acceptable sludge by dumping material into sewers that kill off the bacteria used in the process with consequent public health impact.

Attacks on Public Transit

Accessing transportation lines (e.g., subway systems) through unsecured manholes in order to deploy explosives or chemical/ biological agents would result in large numbers of dead and injured, in addition to the destruction of assets and disruption of the flow of commuter and cargo traffic. The resulting loss of public confidence and psychological impacts would be large and may impact future governance.

The damage that may be done through the illegal use of manholes is substantial. The American Academy of Actuaries estimated in March 2006 that a mild CNBR (Chemical, Nuclear, Biological, Radiological) attack on the DC Metro area, possibly using the metro system as a point of dispersal, would cost the city approximately $106.2 billion. A larger attack may cost the District up to $196.8 billion, where a smaller CNBR attack would cost NYC $446.5 billion.[22]

Consequences of an Underground Attack on Critical Infrastructure

In addition to the general discussion in the previous section, it is possible to detail examples of service disruptions resulting from failures in underground critical infrastructure of the U.S.

Corruption of Telecommunications Services

The increasingly complicated and intertwined communications network in the U.S. may prove an attractive target for terrorist attack. Given the complexity of the network, it is unlikely that all communications services could be compromised by a single underground attack. However, strategic explosions, or attacks on other forms of critical infrastructure (such as electrical systems) may create a cascading effect limiting the ability of first responders and citizens to communicate.

When the Twin Towers of the World Trade Center were attacked and collapsed on September 11, 2001, a number of underground facilities in the area were destroyed. Verizon, the primary local phone carrier in New York City, lost two major switching facilities. Increased traffic on other carrier lines and lost cellular towers created a virtual communications blackout in the city and along a large part of the Eastern seaboard.[23] The destruction of Verizon's two switching facilities in lower Manhattan also impacted the ability to reopen U.S. stock markets following the attack.[24]

In addition, it was estimated that repairs, including 300,000 telephone lines, one phone switching station, and six miles of electrical cable were to cost $2 million.

The estimated total cost for replacing the basic infrastructure is $7.4 million. Business disruption due to the inaccessibility of the immediate area and the lack of operational utilities were estimated at $21 million.[25]

Sewer Gas Explosion

According to the U.S. Government Accountability Office (GAO), the most vulnerable component of a municipal wastewater system to terrorist attack is the underground sewer network.[26] Sewer networks crawl for miles beneath busy city streets and reach all corners of urban areas. A series of sewer explosions in Guadalajara, Mexico in 1992, while not resulting from terrorism, demonstrate the potential impact of a coordinated underground attack on a major urban area.

Multiple explosions in the sewer system in Guadalajara over the course of a four-hour time period destroyed more than six miles of sewer lines. In the most affected areas, high traffic streets were reduced to rubble, much of which crumbled into the 25-foot deep sewer trenches. Although estimates vary, the explosions were attributed with 206 deaths, 1,460 injuries, damage to 1,148 buildings, 350 businesses and 505 vehicles were destroyed, and left approximately 15,000 people homeless.[27]

The explosions in Guadalajara were caused by hexane leak from a nearby oil processing plant. Residents in the affected area began to smell unusual odors from sewers and drains a few days before the explosions occurred. Despite an investigation into the causes, and the flushing of sewer lines by the fire department and corresponding opening of manhole covers to allow excess gas to escape, the explosions rocked the city.[28]

Biological Attack on Potable Water

Even before the attacks of September 11, 2001, maintaining the integrity of the U.S. water infrastructure was identified as a key national security priority.[29] A number of experts believe that the risks of a bioterrorist attack on the water system are small because it is difficult to introduce quantities of biological agents sufficient to cause widespread harm. A biological agent's potential as a weapon includes its stability in water, virulence, culturability in the quantity required, and resistance to detection and treatment.[30] For these reasons, most experts agree that the potential consequences of a biological attack on the water system are more likely widespread illness and panic, rather than the immediate and substantial loss of life associated with more traditional forms of terrorist attack. Access to the water distribution network through manholes in high density population centers allows a terrorist the opportunity to bypass some of the challenges associated with the stability and concentration of a bioterrorism agent on a system-wide scale, and provides the opportunity to cause significant levels of infection and personal injury.

The Centers for Disease Control and Prevention (CDC) note that civilian populations are more vulnerable to biological attacks through the food and water supply. In 1984 an intentional contamination of salad bars with *Salmonella* resulted in widespread illness. In total 751 individuals became ill as a result of exposure in only 10 locations. The CDC identifies *Vibrio cholerae,* the bacterium that causes Cholera, as the most likely biological weapon for employ by terrorists in an inadequately disinfected water supply.[31]

Cholera is an acute intestinal infection with a short incubation period (from less than one day to five days) that can quickly lead to severe dehydration and death if treatment is not promptly administered. Seven global cholera pandemics have been recorded by the World Health Organization. The disease is spread through contaminated water supplies and large outbreaks may develop suddenly and without warning. When cholera appears in an unprepared community, case-fatality rates may be as high as 50%; in communities with well-developed diarrheal disease control programs, the fatality rate may be as low as 1%.[32] Because cholera is not common in the United States, due to effective chlorination/disinfection processes, it is not known what consequences would occur from a coordinated biological attack of this nature designed to defeat disinfection particularly in an urban center, where there are predominantly Tier I and Tier II manholes.

Steam Explosion

As noted in previous sections of this paper, a vast network of steam pipes exists between 4 and 15 feet below the streets and sidewalks of New York City. These pipes are governed by a network of valves and vents accessible by a series of unsecured manholes. The valves control the pressure and flow of steam throughout the system. Tampering with or simply turning valves off and on in strategic locations creates the possibility for explosions through the city along the steam pipe network. This could be done by a vandal, disgruntled employee, or contractor error.

An accident in 1989 provides an idea of the power of a coordinated effort to corrupt New York's steam delivery infrastructure. In this case, a large steam explosion in Gramercy Park killed two steam workers and one neighborhood resident. The explosion resulted from an increase of water condensation in the pipe that was turned off mistakenly during service. When the steam valve was re-opened by the workers, the 400 degree steam hit the cooler water condensed in the pipe with immediate explosive and deadly results.[33]

The impact on human life was mitigated by the efforts of steam workers to cordon off the area where work was taking place. A larger number of individuals could be affected if a steam explosion took place on a busy sidewalk with no advance notice or preparation.

Low Grade Explosion in Manhole

Simulations: Underground Attack Scenarios and Consequences

A number of local officials provided information on the estimated consequences of an attack on underground utility and telecommunications networks that provide the basis for the scenarios below. Based on this information and other data cited in previous sections of the paper we can broadly estimate the economic and other costs of an attack coordinated by accessing unsecured manholes.

Telecommunications

A series of powerful explosions in unsecured manholes disrupt traffic, power, telecommunications, and internet access throughout the Washington, DC area. The explosions result from a coordinated terrorist attack on three central telecommunications switching centers in Virginia, the District, and Maryland. The incident causes the channel signaling system and telephone network to collapse with recovery being intermittent and unreliable.

Terrorists struck the telecommunications network by accessing unsecured manholes housing underground power and fiber optic cable lines leading to the targeted facilities. Multiple devices detonate simultaneously both underground in streets bordering the facilities and above ground as emergency crews rush to the scene. Devices appear to be approximately 50 pound plastic explosives. The damage includes a 30 percent moderate to heavy damage of facilities.

Losses associated with the attack included equipment valued over $275 million, loss of service and business access estimated in excess of $300 million. 53 people lost their lives and over 140 were injured. Widespread panic and chaos grip the city. In the aftermath, the manhole owners and operators are exposed to a number of legal liabilities.

Potable Water and Sewer

An individual accesses the potable water supply in Baltimore through an unsecured manhole in order to introduce a biological agent. The resulting epidemic incapacitates 15,000 people. Nearly 200 individuals with weakened immune systems – particularly elderly city residents and children – die in the outbreak. Panic spreads while the city attempts to locate the source of the epidemic and public services are strained as roads become clogged with people attempting to flee the city and seek care. Hospitals are overcrowded and the city spends over $15 million to pay overtime for emergency and public health workers. City water supplies are flushed and chlorinated at a cost of $15 million. Loss of productivity to business was estimated at nearly $100 million.

Theft of Underground Equipment

Internet and voice over IP services are disrupted for several weeks in Los Angeles as a result of thieves stealing critical pieces of the underground infrastructure. Under the cover of darkness, a group of individuals access the internet network through unsecured manholes. Once inside the underground vaults, the thieves disconnect a series of electronic and optical amplifiers that maintain internet and voice over IP communications, in addition to cable television signals.

It costs the company over $300,000 to replace the stolen amplifiers, and the outage costs the company over $200,000 in lost revenue and significantly erodes customer good will. Surrounding businesses suffer between $100,000 and $350,000 in losses resulting from service interruptions and related costs.

Disruption of Multiple City Services

A disgruntled employee in the public works department of a mid-sized southwestern city plans an attack to disrupt multiple city services using his knowledge of the underground critical infrastructure. The employee identifies six underground vaults where the junctions of water, sewer, telephone, internet, natural gas, and electricity conduits are located. He accesses all six of these vaults through unsecured manholes to plant explosive devices.

The explosive devices are timed to explode just as rush hour in the city begins. The cascading effects of the explosions cripple the city's normal operations – power outages disrupt businesses, traffic lights are inoperable snarling traffic, telecommunications capabilities are hampered and at times completely disrupted, the water treatment plant is unable to function properly resulting in the discharge of millions of gallons of waste water into the local river, and police and other city workers are overwhelmed as they attempted to deal with traffic, public health issues, looting, and damage to critical infrastructure.

The attack costs the city over $500 million dollars in lost revenues to businesses, damage to infrastructure, and public service expenditures. It takes over three months to rebuild damaged critical infrastructure, and lingering effects of the attack continued several months beyond. The city also faces additional costs resulting from legal liabilities and expenditure of resources for several years to come.

Unauthorized Individual Accessing Critical Underground Infrastructure through an Unsecured Manhole

The Tiering System: Setting Priorities and Assessing Risks

There are over 22 million manholes in the United States, and as noted above the vast majority are not secured. It is not possible to immediately secure all manholes, and therefore it is critical to prioritize which manholes constitute the greatest level of risk and consequences associated with an attack. To this end, we propose a system of tiers to identify the characteristics of various manholes and prioritize their security.

Tier I Manholes – Highest Risk

Tier I manholes are those for which the risks are highest. An attack on these targets is expected to lead to substantial loss of life and injury, significant economic loss, and undermine the morale and confidence of substantial segments of the community. Tier I manholes are those providing access to multiple critical infrastructures and those in or near strategic government installations, major tourist attractions, financial centers, sea ports, airports, public transport systems, and chemical and nuclear power plants. They would also include those along presidential motorcade routes. Terrorists are likely to view these as their preferred targets, precisely because of these consequences. They would also include those relevant to key national policy for example, key manholes near the nation's borders relevant to a border security policy or law.

Tier II Manholes – Second Highest Risk

Tier II manholes are those for which the consequences of attack would be less but still highly significant. They would include certain manholes in or near factories, ports, convention centers, stadiums, centers of commerce and other key economic sites within and outside major metropolitan areas. They might include certain privately owned manholes on university or business campuses. As a result of the moderately high level of consequence expected, they would have a moderately high probability of attack. These are manholes through which an attack would be expected to produce substantial personal injury, or major economic losses, or significant effects on governance, or major undermining of morale, or public confidence, or combinations of these consequences.

Tier III Manholes – Moderate to Low Risk

Tier III manholes would be those for which the consequences of attack would be considerably lower. For example, they might include manholes located in areas of low population density, such as outer suburbs, smaller towns, and rural areas through which access to much less critical infrastructure and assets might be gained.[b] These locations would be expected to have a comparatively low probability of attack because the consequences of any attack economically and in terms of casualties would likely be low.

Tier IV Manholes – Lowest Risk

Tier IV manholes would include those for which an attack would have the lowest expected consequences.

For example, they might be located outside of population centers and involve national parks or protected wildlife areas. These areas would almost certainly have a low probability of attack, as well as minimal economic and human losses should any attack occur.

Categories of Risk and Consequences of Attack on Manholes

Category	Risk Level	Consequences	Characterization
Tier I	High	Severe	Strategic locations including: urban centers; key infrastructure intersections; centers of business, industry, and government
Tier II	Moderate to High	Moderate to Severe	Significant landmarks, transportation hubs, public gatherings
Tier III	Moderate to Low	Moderate to Low	Suburban areas; rural and agricultural regions
Tier IV	Low	Low	Rural/low-population density areas; national parks; wildlife centers

b In its February of 2005, Design Standards for Communications Wiring Systems, The University of Utah requires that all manholes be fitted with a secure access system.

Mitigating Risk and Reducing Vulnerabilities

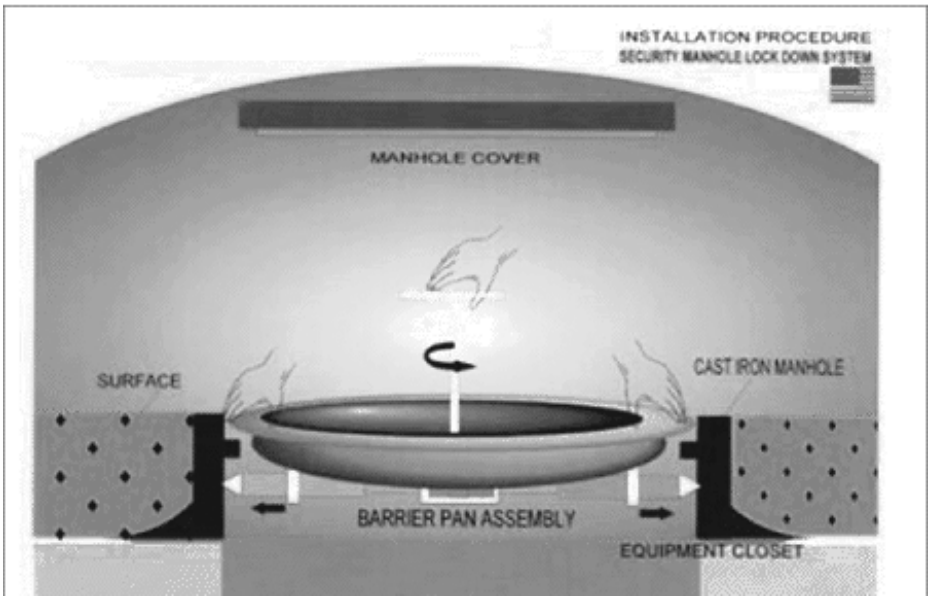
The key to preventing a terrorist attack on the U.S. critical underground infrastructure is to secure Tier I and II manholes. There are alternative ways of securing manholes, but the most practical, effective and affordable approach is by securing manholes with a self-contained and independent manhole barrier device.

Securing Manholes

There are a number of methods for securing manholes including intrusion detection, television surveillance, and hardening. None of these methods provides a practical barrier to prevent unauthorized access to manholes. Intrusion detection and television surveillance are detection mechanisms, not prevention devices. Hardening, or physically sealing the covers, proves expensive and inefficient. Experts estimate that it takes up to 120 minutes to weld a manhole cover shut and up to 60 minutes to open after sealing. In an emergency, the lack of easy access to underground utilities may prolong outages or worsen the problem altogether (for example if a terrorist were to gain access to a manhole and started an underground fire, it would take over an hour before firefighters could begin to fight the fire).

Securing the manhole with a barrier device is the most efficient and effective way to control access to underground infrastructure. In particular, a self-contained and independent manhole barrier device would be optimal. Currently, the only such system we were able to identify that meets these criteria is the Manhole Barrier Security Systems, Inc. (MBSS) device, which is listed on the GSA schedule.

As demonstrated in Figure One below, the goal of a secure manhole barrier device is to provide a physical barrier with a coded key lock to prevent unauthorized access. Unlike hardening methods, self-contained devices can more accurately control entry into manholes and be opened quickly by responders in the event of an emergency.



The Patented Manhole Barrier Security Systems, Inc. Device is the Only Self-Contained, Independent, and Locking Manhole Barrier Device. The MBSS Device Simply Sits Immediately Beneath the Manhole Cover. The MBSS Device Affords Redundancy and is Self-Contained. MBSS is a GSA Contract Holder.

Conclusions and Suggested Actions

The attacks of September 11, 2001 led to a new emphasis on protecting critical infrastructure in the U.S. In high-population density urban centers, much of the utility and telecommunications networks are underground. Access to these underground networks is primarily through street/sidewalk level manholes. Manholes are largely unsecured, creating the potential for unauthorized access and subsequent terrorist attacks on these networks. In order to mitigate the risk associated with an attack, securing manholes is essential. After investigating a variety of options to secure manholes, it is clear that employing a self-contained and independent manhole barrier device is the most practical, effective, and affordable measure to protect these underground assets.

On the basis of the above and the NIPP recommendations,[34] we propose that Congress take a number of steps to protect critical infrastructure through securing manholes. In particular, we recommend that securing Tier I manholes becomes an immediate national priority with Tier II manholes following shortly thereafter. In the short term, Congress should:

1. Examine new statutory requirements that Tier I and II manholes be secured nationwide by both public and private sector entities. Examine requiring the owners and operators of manholes to assess vulnerabilities and identify Tier I and II manholes.

2. Examine appropriating and allocating new funds for urban centers and strategic locations to purchase and install manhole barrier devices for all Tier I and Tier II manholes.

3. Examine incentives such as tax and insurance credits for owners of manholes, including municipalities and corporations – particularly utilities and telecommunication companies – to purchase manhole barrier security devices, and direct the Department of Homeland Security to include manhole security in best practices, policies and procedures.

4. Examine supporting further direct study of this issue by GAO and CRS.

Without manhole security, the United States risks suffering significant consequences resulting from an attack on underground infrastructure including incalculable economic damages, large numbers of civilian casualties, and considerable disruptions to our urban way-of-life.

Appendix A

Examples of Underground Infrastructure Vulnerabilities

Over the last several years, a number of vulnerabilities in underground infrastructure have been exposed. Not all of these events result from terrorist activity, but all demonstrate the potential consequences of an attack on the U.S. through unsecured manholes.

• In February, 2002, Italian police raided an apartment in Rome and subsequently arrested nine men suspected of planning an attack on the U.S. embassy through the underground infrastructure. Investigators believed that the men were planning to contaminate the subterranean water supply in the capital by accessing the water distribution network, specifically targeting the commercial area of Rome where the U.S. embassy is located. At least one of the suspects had suspected links to an Al Qaeda cell in Milan and all were linked to an Algerian organization allegedly financed by Osama bin Laden.[35]

• New York City police foiled a plot to attack train tunnels in the summer of 2006. Using a network of suicide bombers who would access the tunnels used by tens of thousands of commuters, the attacker would attempt to create large numbers of casualties and flooding to lower Manhattan.[36]

• In the summer of 2006, over 100,000 people were without power for 10 days in Queens as a result of overloaded and antiquated energy networks owned by Con Edison in New York City. The outage was exacerbated due to the extent of damage to underground infrastructure that required significant repair and replacement. In addition to losses for businesses and residential customers, the power outages interrupted train and air service. At LaGuardia airport, security screening was halted, while a number of subway train lines had to suspend service resulting from lack of electricity.[37] This illustration demonstrates the magnitude of costs associated with an attack on critical underground infrastructure.

• In March, 2002, Chicago police arrested a man wanted for vandalizing a number of power stations in Wisconsin, for trespassing in underground access tunnels to the city's mass transit system. The recently convicted suspect was found with a vial containing sodium cyanide-sodium carbonate. Police later discovered that this individual was storing large quantities of sodium cyanide and potassium cyanide in an underground vault connected to the subway system beneath the city's downtown Loop district.[38]

• In Pec, Kosovo, terrorists placed an explosive device inside a manhole located near a children's playground in what proved to be a failed assassination attempt.[39]

• Two explosions occurred within seconds of each other at a soccer stadium in Vladikavkaz, about an hour after a soccer match had taken place. One device had been planted under a sewage manhole cover near the entrance to the stadium, and was detonated by remote control.[40]

• As reported on CNN in June 2006 in San Diego, a 23-mile underground network between Mexico and the U.S. leads to approximately 500 manholes scattered across three square miles. This underground network and connecting manholes provides access to the United States to thousands of people from Mexico each year.[41]

• In 1979, two plant operator trainees at the Surry nuclear power station in Richmond, Virginia poured sodium hydroxide on 62 of 64 new fuel assemblies through a manhole opening in the floor.[42]

• Although not attributed to terrorist activity the following incident illustrates the potential impact of a breach in manhole security; in the summer of 2000 more than 40 manhole covers exploded in the Georgetown section of Washington, D.C., as a result of faulty electrical lines. The incidents cost the local power company PEPCO $30 million and four years of effort to repair the damaged ground around the manholes. The incidents disrupted commercial activity in and around Georgetown, and impacted transportation access to a significant part of the nation's capital.[43]

• A widespread power outage in July, 2006 in the Philadelphia suburb of Middletown costs the township an estimated $56,000. Costs to the township as a result of the outage included overtime for police and other municipal workers, renting and operating generators, buying ice, and hiring independent electrical contractors to restore power to traffic lights and other critical infrastructure.[44] This power outage demonstrates the economic impact that could be sustained with a simple breach of manhole security.

• Hundreds of New York residents were left without phone service when a crew from a power utility accidentally struck and severed five underground cables. In Hawaii, 3,500 phone customers lost service when a building contractor accidentally cut two sections of underground cable.[45] Both of these incidents resulted from utility crews gaining access to the wrong manholes. If a MBSS device was in place to secure these manholes, this error would not have occurred.

Appendix B

References

1. Cf. Critical Foundations: the report of the President's Commission on Critical Infrastructure Protection, White House Document October 1997; *Presidential Decision Directive 63: Critical Infrastructure Protection*, May 22, 1998; *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (NSPP); Homeland Security Presidential Directive HSPD -7, Dec 17, 2003; HSPD-9, Jan 30 2004.
2. National Commission on Terrorist Attacks Upon the United States, 9/11 Commission Report, Washington, DC: July 22, 2004.
3. Wikipedia, *Ibid.*
4. Kate Ascher, *The Works: Anatomy of a City*, New York: Penguin Press, 2005.
5. David Schaper, "In Chicago, Manholes on the Move," National Public Radio, *Morning Edition* (November 29, 2004).
6. FEMA, U.S. Department of Homeland Security, Reference Manual, Washington, DC: December 2003.
7. National Commission on Terrorist Attacks Upon the United States, *Ibid.*
8. Jennifer Chen, "Manhole Covers Take Manhattan," *Columbia News Service* (April 27, 2002).
9. Kate Ascher, *Ibid.*
10. Kate Ascher, *Ibid.*
11. Kate Ascher, *Ibid.*
12. Con Edison, "The Pressroom" *Coned.com* http://www.coned.com/pressroom (assessed September 11, 2006).
13. Kate Ascher, *Ibid.*
14. Kate Ascher, *Ibid.*
15. Kate Ascher, *Ibid.*
16. Los Angeles Deputy Police Chief Ronald Bergmann (Retired), Personal Communication (September 7, 2006).
17. Gans, Roger L. Manager, Planning and Design, DC Sewer and Water Authority. July 7, 2006.
18. Baltimore Department of Public Works, "About the Bureau of Water & Wastewater," June 26, 2006, http://www.ci.baltimore.md.us/government/dpw/water.html#about, (accessed 6 September 2006.)
19. FEMA, U.S. Department of Homeland Security, Reference Manual, Washington, DC: December 2003. U.S. Department of Homeland Security and Federal Bureau of Investigation, "Information Bulletin," Washington, DC: July 30, 2004.
20. Thomas C. Greene, "Mock Cyberwar Fails to End Mock Civilization," The Register, http://www.theregister.com/2002/08/30/mock_cyberwar_fails_to_end/ (accessed 18 October 2006).
21. In 1981 the Purina plant in Louisville , Ky had been discharging quantities of the volatile hexane into the wastewater system. Apparently, the gas built up in a section of Louisville's underground sewers and a spark from a passing vehicle is suspected of causing it to explode resulting in a massive cave-in of the street. Courier Journal – Louisvile, KY article July 13, 2003
22. "Actuaries Disclose Potential Terrorism Costs". American Academy of Actuaries. 31 March 2006. http://64.233.167.104/search?q=cache:b8hhEYu1ScgJ:www.actuary.org/newsroom/pdf/tris_march06.pdf+American+Academy+of+Actuaries,+CNB R+attack&hl=en&gl=us&ct=clnk&cd=2
23. Olga Kharif, "Telecom Stuck on Hold," *Business Week*, October, 2, 2001, http://www.businessweek.com/technology/content/oct2001/tc2001101_0830.htm, (accessed September 12, 2006).
24. Network World Staff, "Internet, Telecom Networks Put to Test in Wake of Terrorist Strikes on U.S.," *Network World*, September 17, 2001, http://www.networkworld.com/news/2001/0917attacks.html, (accessed September 12, 2006).
25. CNN.Com, "9/11 panel: Al Qaeda planned to hijack 10 planes," *Cnn.com,* June 17, 2004, http:// www.cnn.com/2004/ALLPOLITICS/06/16/911.commission/, (accessed September 20,2006).
26. GAO, "Securing Wastewater Facilities," March 2006: GAO-06-390; GAO, "Wastewater Security," January 2005: GAO_05-165.
27. Suburban Emergency Management Project, "The Guadalajara 1992 Sewer Gas Explosion Disaster," *SEMP Biot#356,* http://www.semp.us/biots/biot_356.html (accessed on September 9, 2006).
28. Suburban Emergency Management Project, *Ibid.*
29. "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." May 22, 1998, http://www.fas.org.irp/offdocs/paper598.htm.
30. Claudia Copeland and Betsy Cody, "Terrorism and Security Issues Facing the Water Infrastructure Sector," *CRS Report for Congress*, Congressional Research Service: Washington, DC, April 25, 2005.
31. Lisa D. Rotz, Ali S. Khan, Scott R. Lillibridge, Stephen M. Ostroff, and James M. Hughes, "Public Health Assessment of Potential Biological Terrorism Agents," *Emerging Infectious Diseases,* Centers for Disease Control and Prevention: February 2002, http://www.cdc.gov/ncidod/EID/vol8no2/01-0164 (accessed September 12, 2006).
32. World Health Organization, "Fact Sheet No. 107 – Cholera," *WHO Media Centre,* http:// www.who.int/mediacentre/factsheets/fs107/en/, (accessed September 12, 2006).
33. Kate Ascher, *Ibid.*
34. U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, February 2005.
35. Associated Press, "4 Arrested in Rome in Possible Cyanide Threat," USA Today http://www.usatoday.com/news/world/2002/02/16/rome.htm (accessed September 11, 2006).; CNN.com with Alessio Vinci, "Substance Found in Rome Raid is Cyanide Derivative" CNN.com, http://edition.cnn.com/2002/WORLD/europe/02/20/inv.italy.moroccans (accessed September 11, 2006). CNN.com, "Ninth Arrest in Rome Tunnel Probe," CNN.com, http://edition.cnn.com/2002/US/02/25/italy.arrests.
36. Pat Milton, The Associated Press, "FBI: Thwarted N.Y.C. Subway Involved Martyrdom," *San Jose Mercury* 48 *News,* http://www.mercurynews.com/mld/mercurynews/news/breaking_news/14990832.htm *(*accessed September 11, 2006).
37. Kristina Fiore, "Why L.I. Dodged a Queens-like Blackout," *New York Newsday*, 30 July 2006.; CNN.Com, "Power Outages Interrupt Train, Air Service in New York," *Cnn.com* http://www.cnn.com/2006/U/07/18/power.outage/index.html (accessed October 2, 2006).
38. Associated Press, "Vandal's Chemical Stash Discovered,"*CBS News*, http://www.cbsnews.com/stories/2002/03/11/national/main503482.shtml (accessed September 11, 2006).
39. The Center for Peace in the Balkans. "Kosovo Trial Witness Narrowly Escapes Death." 27 September 2003.
40. MIPT: Terrorism Knowledge Database. "Unknown Group Attacked Private Citizens & Property Target." 17 November 2002.
41. Anderson Cooper 360 Degrees. CNN Online. 13 June 2006.
42. Mahtadi, Hamid and Antu Murshid. The Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks: 1950-2005.
43. Pepco, "Pepco Files Report of Georgetown Manhole Investigation," 20 March 2000.
44. Chris English, "Power Outage Cost Township $56,000," *Phillyburbs.com*, http://www.phillyburbs.com/pb-dyn/news/111-07262006-688880.html (accessed October 2, 2006).
45. The Journal News Staff, http://www.thejournalnews.com/apps/pbcs.dll/frontpage, October 5, 2006.