95138

ANL/OTD-EEST/CP--95138

CONF-971246--

INFRASTRUCTURE: A TECHNOLOGY BATTLEFIELD IN THE 21ST CENTURY*

Harvey Drucker

Associate Laboratory Director
Energy and Environmental Science and Technology
Argonne National Laboratory
9700 South Cass Avenue
Argonne, Illinois 60439

for submission to

Violent Conflict in the 21st Century:
Causes, Instruments, and Mitigation
December 5–7, 1997

sponsored by
Midwest Consortium for International
Security Studies

* Work supported by the U.S. Department of Energy under contract W-31-109-Eng-38.

DISCLAIMER

Portions of this document may be illegible electronic image products. Images are produced from the best available original document.

INFRASTRUCTURE: A TECHNOLOGY BATTLEFIELD IN THE 21ST CENTURY

by

Harvey Drucker

1 INTRODUCTION

The twentieth century will no doubt be remembered as the era of civilization's technological evolution. During this century, we have progressed from an agrarian society to an industrial society, to a high-tech information society. A major part of this technological advancement has involved the development of complex infrastructure systems, including electric power generation, transmission, and distribution networks; oil and gas pipeline systems; highway and rail networks; and telecommunication networks. Over the past several decades, we have come to rely more and more on these systems. This reliance will be even heavier in the twenty-first century.

Our dependence on these infrastructure systems renders them attractive targets for conflict in the twenty-first century. Hostile governments, domestic and international terrorists, criminals, and mentally distressed individuals will inevitably find some part of the infrastructure an easy target for theft, for making political statements, for disruption of strategic activities, or for making a nuisance.

The President's Commission on Critical Infrastructure Protection, which was established on July 15, 1996, confirms the importance of infrastructure in our society. Justification for the formation of this Commission was given as:

> "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[1]

Due, in part, to the complex nature of our current infrastructure systems, in which each component is intricately linked to the others, incapacitating a significant portion of any system is becoming easier. In the past, the manner in which a society's infrastructure was disrupted was somewhat involved. A contingent of troops would be sent to secure control of a major road, trade route, or river crossing. An airplane would be dispatched to drop a bomb on a facility such as a power plant. Today, disruptive techniques are substantially easier to use and can have dramatic effects. A small vial of a toxic chemical dropped in a subway can incapacitate or kill thousands and shut down the public transport network. A computer virus can be injected into a major computer database and destroy critical records or operational data, thus shutting down a facility.

The current situation regarding the vulnerability of our infrastructure can be summarized in three major points.

1. Our dependence on technology has made our infrastructure more important and vital to our everyday lives. This, in turn, makes us much more vulnerable to disruption in any infrastructure system.

2. Technologies available for attacking infrastructure systems have changed substantially and have become much easier to obtain and use. Easy accessibility to information on how to disrupt or destroy various infrastructure components means that almost anyone can be involved in this destructive process.

3. Technologies for defending infrastructure systems and preventing damage have not kept pace with the capability for destroying such systems.

A brief review of these points will illustrate the significance of infrastructure and the growing dangers to its various elements.

2 INFRASTRUCTURE DEPENDENCE ON TECHNOLOGY

ENERGY INFRASTRUCTURE

To illustrate the first point, our increased dependence on infrastructure systems, consider electric power, which is one of the most important elements of the energy infrastructure.

- In November 1965, the northeastern portion of the United States suffered a widespread electrical blackout. Thirty million people were affected by this blackout that lasted up to 13 hours in some locations. Almost 800,000 people were trapped in New York City subways, elevators, and skyscrapers. The official cause was attributed to failure of a circuit breaker at a power station in Niagara Falls, Ontario. The utilities affected were so unprepared for this situation that the lights illuminating the control panels themselves had gone out. The cost of this disruption was estimated to be in the millions of dollars, but was reduced somewhat by the presence of a full moon on the night of the outage.

- On July 2, 1996, more than 30 years later, an electric transmission line sagged into a tree, most likely because of unusually hot weather. Electric power to 2 million customers in 14 western states was interrupted by this single event.

- On August 10, 1996, only one month later and shortly after pronouncements had been made that the July disruption would not happen again, another electric line sagged into another tree. A short while later, three more high-voltage lines were also shorted due to more power lines sagging into trees. This time, electrical service to 4 million customers in 14 states and 2 Canadian provinces was interrupted. The cost of these outages was estimated at between $0.7 and $4.0 billion.

It is clear that electric power disruptions have significant costs associated with them. Industrial processes are interrupted and manufacturing components spoiled. For example, during one power outage, a Chevrolet plant reported losing 350 engine blocks when high-speed drills froze while boring piston holes. A computer chip manufacturer estimated that it could lose $30 million from a 20-minute power outage if a batch of chips were in process during the outage. In general, it is estimated that the cost of power disruption can range from $1/kWh to $5/kWh, although some estimates are as high as $20/kWh. In addition to these tangible and quantifiable costs, are the more difficult to measure social costs. For example, disruption of traffic signals and other safety devices can lead to increased accidents and loss of life. The failure of security and alarm systems and lack of lighting have often resulted in looting and rioting, thus adding to the costs of power outages.

Part of the reason for the high vulnerability of the electric power system results from the fact that electric utilities typically design their systems for cost efficiency. While reliability has traditionally been a major part of utility planning, the increasingly competitive market is putting more emphasis on the bottom line. This often leaves utilities vulnerable to disruptions. For example, extra-high voltage and large generation step-up transformers, used by virtually all electric utilities, are all manufactured abroad because of lower production costs. The manufacture time is about 6 to 12 months. These items are transportable only by special rail cars (Schnabel cars), of which there are only 13 in the United States and 1 in Canada. Thus, a transformer damaged by hostile attack cannot be replaced quickly.

As another example, in the current cost-conscious market, electricity generation reserve margins are being curtailed. Capacity expansion is at a virtual standstill. Further, reserve margins are likely to be reduced by 50% over the next decade. Thus, in the event of a disruption at a single power plant, it will be increasingly difficult for a utility to make up the difference from another source. Very little excess capacity will be available to spare.

Adding to these vulnerabilities of the electric power system is the fact that reliance is increasingly being placed on automated control equipment. More and more utilities are implementing Supervisory Control and Data Acquisition (SCADA) systems that allow for remote manipulation of valves, pumps, generators, substations, and other elements of the system. Such automated systems are attractive because they reduce company operating costs. However, these computerized control techniques render the entire system more vulnerable to interference by computer hackers.

The oil and gas industry is another major component of the energy infrastructure that is also vulnerable to disruption. as evidenced by past events.

- The winter of 1972–1973 was exceptionally cold and resulted in the diversion of natural gas supplies to lucrative spot market sales. This diversion caused several major cities to come within hours of losing their natural gas supplies because of the loss of downstream pressure.

- In April 1997, a militia group planned to blow up a Texas refinery as a cover for a bank robbery. The target was a hydrogen sulfide (H_2S) plant. Fortunately, federal agents were able to thwart this attempt before it was executed. If successful, this plan would have caused extensive loss of life.

One of the main objectives of the energy sector (and of business in general) is to increase economic efficiency. However, because our energy system is so streamlined, this goal has the side effect of increasing vulnerability to attack and disruption. For example, the number of oil refineries has declined from more than 300 in the early 1980s to 161 at the end of 1996; this smaller number of plants is operating at 93% capacity. In the case of pipelines, one pipeline, originating in Texas, delivers more than 50% of the gasoline and heating oil to 13 East Coast states. Consider natural gas. Chicago has six city gates, that is, major valves that connect the natural gas local distribution system with long-distance transmission pipelines. At peak demand periods, all six gates must be functioning properly to keep up with demand. A malfunction of even one component can result in massive disruption.

OTHER INFRASTRUCTURES

Although disruptions to the energy system infrastructure can have serious and widespread effects, there is no shortage of additional examples of our dependence on other systems.

Transportation

Air travel has been the target of terrorist attacks for many years. Passenger security checks were initiated 25 years ago, in 1972. Yet in 1988, Pan Am Flight 103 was blown up over Lockerbee, Scotland, by a small amount of explosives in a cassette player. While not so common in U.S. airspace, attacks on airliners are all too common in the rest of the world.

Although not as dramatic in terms of newspaper headlines, the railroad system is subject to major disruptions. The railroads carry large quantities of chemicals used in manufacturing and agriculture. In 1991, a tank car containing 19,000 gallons of pesticide derailed near Dunsmuir, California. The resulting spill effectively sterilized a 45-mile stretch of the Upper Sacramento

River. A small community noted for its excellent fishing grounds was economically devastated by the spill.

In 1995, an Amtrak passenger train was derailed in Arizona. The cause of the derailment was sabotage to the track by an extremist group. One person was killed, and 100 were injured in the accident.

Telecommunications

Telecommunications have become an essential part of our daily lives. A 1988 fire in a local telephone switching center in Hinsdale, Illinois, caused the loss of 355,000 phone lines for several weeks. The phone company alone estimated its lost business at $1 million per day. The loss to other businesses that were left without phone service for up to a month was in the hundreds of millions of dollars.

In January 1990, a software bug in the AT&T long-distance switching network affected all 114 switching centers. Although the company was able to recover in a relatively short time, the disrupted communications left many businesses with substantial losses.

Even the emergency phone system is not immune. In 1992, a computer hacker intruded into the 911 system in New Jersey, Maryland, and Virginia. The hacker attempted to inject a virus into the database that would provide incorrect information to emergency responders (fire, ambulance, and police).

Banking

The nation's banking and finance system has developed an extensive and intricate electronic infrastructure that is now crucial to its operation. More than 1 billion credit cards are now in circulation in the United States; more than four cards for every man, woman, and child in the country. Transactions with these cards, which are processed electronically, account for over $500 billion in annual expenditures and half of all consumer debt. Despite extensive security measures, the system is still open to attack. Recently, an MCI employee stole credit card numbers from a company computer and sold them to an international criminal group. The loss was estimated at $50 million.

Water Supply

Even a basic infrastructure such as water supply has become a point of vulnerability. More than 80% of the U.S. population is served by some form of public water distribution system. Private wells are becoming increasingly rare. The residence time of water in a large public system is usually less than one week. Thus, any contaminant (chemical, biological, or nuclear) introduced into a water supply system can quickly spread to a large population.

3 EASY ACCESS TO TECHNOLOGY AND INFRASTRUCTURE VULNERABILITY

The second point regarding infrastructure vulnerability involves the increased capability and feasibility for attacking infrastructure. Threats to infrastructure can be grouped into three categories: natural disasters, human error, and planned attacks. Natural disasters can often be anticipated to some degree. For example, earthquake zones, hurricane-prone areas, and floodplains can easily be identified. Although the occurrence of these events cannot be prevented, the extent of damage caused by them can be dealt with through intelligent and appropriate planning and preparation. Human error is random but can be minimized by increased training and quality assurance activities.

Planned attacks are much harder to deal with and can be attributed to a number of perpetrators, including hostile governments, organized groups such as terrorists, disgruntled employees, malicious intruders, criminals, economic and industrial saboteurs, and mentally distressed individuals. Damage caused by such attacks can be physical, which includes damage to, or destruction of, infrastructure components and operational interference. Such attacks can also involve cyber damage, which includes damage to computer systems, jamming, and introduction of misinformation.

Bombs

The traditional physical attack on infrastructure is the use of a bomb. Technological advances have made it easier to obtain the raw materials for constructing bombs. In 1988, plastic explosives inserted into a cassette player brought down Pan Am Flight 103 and killed 270 people. While very effective, plastic explosives are still not readily available. In 1996, however, readily available products such as fertilizer and motor fuel were loaded into a rental truck that was used to destroy the federal building in Oklahoma City, resulting in the deaths of 168 people. The raw materials used in this bomb are readily available to anyone.

Chemical Weapons

Some chemical weapons are also relatively simple to make. The sarin used in the 1995 Tokyo subway attack was made from readily available chemicals. Five canisters containing liquid sarin were placed in the subway cars. The liquid vaporized, and the sarin was distributed through the ventilation system throughout the subway cars, resulting in 11 deaths and 5,500 injured.

Ricin, a toxin made from beans, is about 6,000 times more potent than cyanide. In 1993, a militia member was arrested with a quantity of ricin that was to be mixed into skin cream. The application of even a small amount of the skin cream would have resulted in death.

A number of books and pamphlets with directions for manufacturing a chemical weapon have been published. Some are readily available to anyone through the Internet. Attempts to curtail the publication of this type of material have encountered legal arguments regarding freedom of speech.

Biological Weapons

Biological weapons are becoming increasingly attractive. In 1995, a white supremacist ordered a batch of bubonic plague from a distributor of microorganisms. This is the same organism that was responsible for killing three-quarters of the population of Europe in the fourteenth century. The package containing the bubonic plague organisms was delivered to the white supremacist's house via Federal Express. The only illegality committed was that he fraudulently used a laboratory letterhead to order the organisms.

Because of the potency of many biological organisms and their small size, only a small amount of biological material is needed to create serious problems. For example, a dose of less than 1.0 microgram of staphylococcus aureus enterotoxin in food can result in serious food poisoning. The U.S. Office of Technology Assessment estimated that a small plane could spray 100 kilograms of anthrax spores over the Washington, D.C., area, which could kill 1 to 3 million people.

Nuclear Weapons

With the fall of the Iron Curtain and the dissolution of the Soviet Union, even nuclear material is easier to obtain than in the past. In 1993, a thief stole 13.5 kilograms of highly enriched uranium from a Russian submarine shipyard. In 1994, police in the Czech Republic arrested three men with 2.7 kilograms of highly enriched uranium. German police reported 41 cases of nuclear material smuggling in 1991; in 1992, this had increased to 158; in 1993, there

were 241 cases; and in 1994, the number had risen to 267. In December 1995, Chechen rebels placed some radioactive material in a Moscow park.

Nuclear material has enormous destructive power and only a minimal amount is needed to build a crude bomb; between 3 to 25 kilograms (enough to fill two soft drink cans).

Cyber Weapons

Despite the ease of obtaining and building bombs and biological and chemical weapons, the weapon of choice is increasingly becoming cyber. In 1996, almost half of the Fortune 1000 companies polled reported that their computer networks had been successfully attacked. Forty percent of the companies surveyed indicated that they had experienced costs of over $500,000 per intrusion. Eighteen percent of the companies stated that they had experienced costs of over $1 million per intrusion.

In 1995, the Defense Information Systems Agency (DISA) ran a test to determine the ease with which unclassified computers could be penetrated. A total of 26,170 computers were subjected to simulated attacks. A small portion, 3.6%, were readily penetrated using simple, "front-door" techniques. A much larger number, 86%, were successfully penetrated when the attackers obtained access through a shared network. The results were very unnerving to the defense establishment.

Computer hacking has become something of a sport among its practitioners. Software tools with user-friendly, graphical user interfaces have been developed that enable the less capable hacker to enjoy the experience of breaking into computer systems. In August 1995, the DEFCON III convention was held in Las Vegas. The show was designed specifically for hackers to give them the opportunity to share experiences and to learn new techniques. A hacker's guide, *The Hacker Chronicles*, is sold on a CD-ROM for $49.95. Many hacker bulletin boards and newsgroups can be accessed on the Internet where information is exchanged and new techniques are shared. As with other publications on weapons, the control of the distribution of this information is frequently challenged on freedom-of-speech grounds.

4 LAG IN DEFENSIVE TECHNOLOGY FOR INFRASTRUCTURE

The third point regarding infrastructure vulnerability deals with the fact that the technology for defending infrastructure has not kept up with the capabilities for attacking it. Lacking an imminent, well-recognized, and serious threat to infrastructure, there is little incentive to invest in protective technology.

Physical, Chemical, And Biological Threats

Consider the most traditional protective measure — physical protection. Physical barriers such as fences and walls can often be used to prevent attacks on a facility. A facility can be "hardened" against bombs with reinforced structures and blast containment. The presence of security personnel and monitoring and detection systems can act as deterrents to possible attacks and can reduce the incidence of threats against infrastructure systems.

However, even with physical protection equipment and security procedures, many infrastructure elements are essentially unguarded. Major oil and gas pipelines, pumps, and compressor stations are openly identifiable and unprotected. The same is true for electric transmission lines, substations, and transformers. Telecommunication microwave towers are widely recognizable and, in most cases, defended only by a chain-link fence. Most municipal water supply reservoirs have little or no access restrictions.

Because many infrastructure facilities are owned by private companies, the cost of protection is weighed against the likelihood of attack and the possible extent of damage; due consideration is given to the impact on company profitability. Absent any regulatory pressure, expenditures on infrastructure protection will be limited by a company's ability to recognize potential threats and its understanding of the consequences of a successful attack.

The situation is compounded for chemical and biological threats by the lack of a suitable defensive technology. The best biological toxin detector currently available must be mounted on an Army Humvee, takes two highly trained technicians to operate, and requires 30 to 45 minutes to perform an analysis of four possible toxic agents. This equipment is recognized as only marginally suitable for battlefield conditions, where trained personnel and awareness of the dangers are abundant. Application to an attack in a municipal area is essentially impractical.

The cost of equipment is also a major issue. A single chemical toxin monitoring device suitable for use by a local fire department can cost up to $10,000. A single protective suit for a firefighter can cost $15,000. It is difficult to imagine local communities being able to allocate sufficient resources to deal with a major chemical or biological incident.

Cyber Threats

As difficult and expensive as it is to protect against physical, chemical, and biological threats, cyber protection is even harder. To quote James Settle, former director of the FBI's Computer Crime Unit, "You bring me a select group of 10 hackers and within 90 days, I'll bring this country to its knees." As melodramatic as the statement may sound, it reflects the insight of someone who has seriously investigated the problems and is well acquainted with the issues.

Cyber protection has taken many different paths, including passwords, firewalls, encryption, compartmentalization, virus checkers, limited message types, unerasable event logs, isolation from networks, digital signatures, and others. Despite these precautions, the DISA penetrability test in 1995 showed that 98% of computer intrusions were not even detected by users or system administrators. The victims never even knew that they were victims. In addition, for the 2% of the cases that were detected, only 5% were reported to the authorities. Most people did not even recognize the extent of the threat to which they had been exposed.

For 1995, the year with the most complete figures, the Pentagon logged more than 250,000 actual attacks on unclassified computers. A 60% penetration success rate was achieved. Even the military's equipment is not safe from attacks. Data for attacks on classified computers are not published.

5 RESEARCH NEEDS

It is clear that considerable R&D is needed to bring infrastructure protection into the twenty-first century. Increasingly, infrastructure protection is viewed as a series of interrelated efforts that include prevention, incident response, and recovery. By dealing with the different aspects of the protection problem, more effective and less costly solutions are being developed. R&D efforts are focusing first on components that address specific threats. Examples include the following:

- Hardened airline cargo containers that can withstand a bomb blast and minimize damage to the airframe.

- "Smart" materials technology, including ultrasonic and magnetic corrosion detection and shape-memory alloys that can detect small changes in structural components before failure.

- Imbedded fiberoptic materials that allow for rapid inspection of components for tampering.

- Microchip-based biosensors that can immobilize thousands of compounds (DNA, RNA, antibodies, etc.), perform thousands of interaction tests in parallel (hybridization, antigen-antibody binding, receptor-ligand binding, etc.), provide rapid biological threat analysis, and are inexpensive to use.

Research into computer protection is also developing new techniques such as:

- Intrusion detection systems,
- Advanced encryption techniques,
- Intrusion containment and isolation, and
- Rapid system recovery.

In addition to these component-level approaches, research is underway on system-level issues. These include:

- Vulnerability assessment methodologies,
- Risk management decision support,
- Incident response planning, and
- Information sharing.

These approaches are designed to provide a more complete view of the threat situation and will allow government, military, and private sector organizations to identify, evaluate, and plan for increasingly sophisticated threats to infrastructure systems.

Indicative of the extent of the need for additional infrastructure protection, the President's Commission on Critical Infrastructure Protection has recommended further R&D. The final report[2] calls for increasing federal spending on infrastructure assurance R&D from the current level of approximately $250 million to $500 million in fiscal year 1999. It also calls for further increases to $1 billion per year by fiscal year 2004. The final report proposes that the National Research Council prepare a national infrastructure research program that would lay out the needs and priorities for such a research effort. Joint efforts by government, the private sector, and academia will be needed to carry out this research.

The Commission report concluded:

> "The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis. However, we are convinced that our vulnerabilities are increasing steadily, that the means to exploit those weaknesses

are readily available, and that the costs associated with an effective attack continue to drop."[2]

An important final point needs to be made regarding infrastructure assurance. Technology can help prevent infrastructure damage and can assist in recovering from such damage. However, technology cannot prevent the dedicated, the highly sophisticated, or the lunatic from carrying out an attack. The hope is to minimize the risks. They cannot be eliminated.

6 REFERENCES

1. Executive Order 13010, 1997, President of the United States, *Federal Register,* Vol. 61, No. 138, July 17.

2. Report of the President's Commission on Critical Infrastructure Protection, 1997, "Critical Foundations, Protecting America's Infrastructure," Oct.