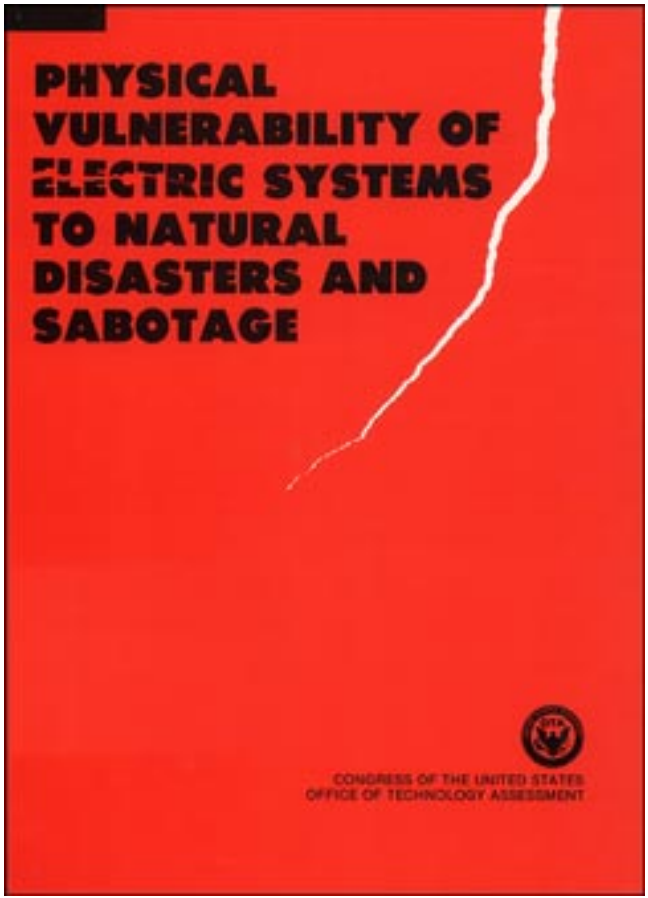
Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage

June 1990

OTA-E-453
NTIS order #PB90-253287



Recommended Citation:

U.S. Congress, Office of Technology Assessment, *Physical Vulnerability of Electric System to Natural Disasters and Sabotage*, *OTA-E-453* (Washington, DC: U.S. Government Printing Office, June 1990).

For sale by the Superintendent of Documents
U.S. Government Printing Office, Washington, DC 20402-9325
(order form can be found in the back of this report)

Foreword

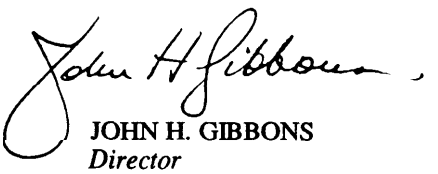
This assessment responds to requests by the Senate Committee on Governmental Affairs and the House Committee on Energy and Commerce to evaluate the potential for long-term electric power outages following natural disasters and deliberate sabotage. This report complements earlier OTA reports: *Electric Power Wheeling and Dealing-Technological Considerations for Increasing Competition;* and New *Electric Power Technologies—Problems and Prospects for the 1990s.*

This country has enjoyed remarkably reliable electric service for the most part. Very few blackouts have affected many people for more than a few hours. Nevertheless, much worse blackouts are possible which could cause enormous disruption and expense for society. It is the intent of this report to analyze how such disasters could happen and how the risk could be reduced.

OTA examined the effects on an electric power system when various components are damaged and how the system can be restored. Present efforts and potential options to reduce vulnerability are described. Also, specific policy measures are analyzed and grouped according to whether they are likely to be implemented and their costs.

This report contains no information not readily available from other public sources that would assist saboteurs in destroying electric power facilities and causing widespread blackouts. An analysis of the vulnerability of specific equipment is included in a separate appendix that is under classification review **by** the Department of Energy. This appendix will be made available only under appropriate safeguards by the Department of Energy.

OTA appreciates the generous assistance provided by our workshop participants as well as other individuals who contributed to this report by providing information, advice, and substantive reviews of draft materials. To all of the above goes the gratitude of OTA and the personal thanks of the project staff.



JOHN H. GIBBONS
Director

Electric System Vulnerability Workshop Participants October 18, 1989

Edward Badolato
CMS, *Inc.*

Lex Curtis
Westinghouse ABB

John Edwards
New York State Energy Office

Michehl Gent
North American Electric Reliability Council

A. Leonard Ghilani
RTE Power Products

Henry Hyatt
Federal Emergency Management Agency

James Jackson
Southern California Edison Co.

Frank Kroll
Arizona Public Service Co.

Charles Lane
U.S. Secret Service

Joseph Muckerman 11
U.S. Department of Defense

Jeffrey Palermo
Casazza, Schultz & Associates, Inc.

Bernard Pasternack
American Electric Power Service Corp.

Stanley Trumbower
U.S. Department of Energy

Joseph Walter
Maryland Public Service Commission

Emmet Willard
Private Consultant

John Williams
U.S. Department of Energy

John Wohlstetter
Contel Corp.

Frank Young
Electric Power Research Institute

Physical Vulnerability of Electric Power Systems to Natural Disasters and Sabotage
OTA Project Staff

Lionel S. Johns, *Assistant Director, OTA*
Energy, Materials, and International Security Division

Peter D. Blair, Energy and Materials Program Manager

Alan T. Crane, *Project Director*

Robin Roy, *Analyst*

Joanne M. Seder, *Analyst*

Administrative Staff

Linda Long Phyllis Brumfield

Contributors

Lillian Chapman
A. Jenifer Robison
Daniel Yoon

Contractors

Casazza, Schultz & Associates, Inc.

Acknowledgments

Glenn Coplan
U.S. Department of Energy

Lex Curtis
Asea Brown-Boveri

James Dodd
Virginia Power Co.

Gene Gomelnik
North American Electric Reliability Council

Richard Gutleber
Virginia Power Co.

Roger Hamrick
Virginia Power Co.

Eric Haskins
Edison Electric Institute

Michael Hunt
Asea Brown-Boveri

Robert Mullen
Department of Energy

David Nevius
North American Electric Reliability Council

Hilton Peel
Virginia Power Co.

Kyle Pitsor
National Electrical Manufacturers Association

Charles Rudasill
Virgnia Power Co.

Charles White
National Electrical Manufacturers Association

Additional Reviewers

Steinar J. Dale
Oak Ridge National Laboratory

James S. Gilbertson
Federal Emergency Management Agency

Darriell Jones
Federal Bureau of Investigation

Monte Strait
Federal Bureau of Investigation

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the reviewers. The reviewers do not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

Contents

Boxes

Tables

Chapter 1
Introduction and Summary

INTRODUCTION

The reliability of U.S. electric power systems has been so high that the rare occurrences of major blackouts have been prominent national and even international news items. The most notable incidents—in South Carolina after Hurricane Hugo, in Seattle after the 1989 cable fire, New York City in 1977, or almost the entire Northeast in 1965—have demonstrated that blackouts are very expensive and entail considerable disruption to society.

As damaging as these blackouts have been, much worse events are possible. Under several different types of circumstances, electric power ***systems*** could be damaged well beyond the level of normal design criteria for maintaining reliability. Seismic experts expect that several parts of the country could experience significantly larger earthquakes than the one that hit California in 1989. Hurricanes even more damaging than Hugo could move along the Gulf of Mexico or up the Atlantic coast, maintaining their strength rather than losing it inland. Either type of natural disaster could damage many electric power system components, causing widespread outages over a long period of restoration and recovery. Even more ominously, terrorists could emulate acts of sabotage in several other countries and destroy critical components, incapacitating large segments of a transmission network for months. Some of these components are vulnerable to saboteurs with explosives or just high-power rifles. Not only would repairs cost many millions of dollars, but the economic and societal damage from serious power shortages would be enormous.

Electric utilities normally plan for the possibility of one, or occasionally two, independent failures of major equipment without their customers suffering any significant outage. If the system can be better protected, or made sufficiently resilient to withstand greater levels of damage, then the risk of a major, long-term blackout will be reduced. However, any such measures will cost money. Utilities are taking some steps, but apparently, generally consider the risk to be too low to warrant large expenditures, which would ultimately be borne by their customers, or by stockholders if the State utility commission did not approve inclusion of these costs in the rate base.

However, the consequences of a major, long-term blackout are so great that there is a clear national interest involved. Steps that may not be worthwhile for individual utilities could make sense from the national perspective. The purpose of this report is to explore the options for reducing vulnerability and place them in context. It first reviews the threat from both natural disasters and sabotage to determine what damage might occur. However, an analysis of the probability of any of these threats materializing is beyond the-scope of this study. Chapter 3 reviews the impact of major blackouts that have occurred, in order to help understand the costs of an even greater one that might be experienced eventually. Chapter 4 estimates the effect on the system when various critical components are damaged, and how the system can be restored. Chapters 5 and 6 describe present and potential efforts to reduce vulnerability. Finally, chapter 7 suggests how Congress could act, depending on how seriously the problem is viewed.

SUMMARY

Causes and Costs of Extended Outages

A variety of events, both natural and manmade, can cause power outages. Widespread outages or power shortages lasting several months or more are unlikely unless significant components of the bulk power system—generation and transmission-are damaged. The most probable causes of such damage are sabotage of multi-circuit transmission facilities, and very strong earthquakes or hurricanes.

The bulk power system is vulnerable to terrorist attacks targeted on key facilities. Major metropolitan areas and even multi-state regions could lose virtually all power following simultaneous attacks on three to eight sites, though partial service might be restored within a few hours. Most of these sites are unmanned, and many are in isolated areas, with little resistance to attack. Powerplants can also be disabled by terrorists willing to attack a manned site, or isolated from the transmission network by high-power rifle fire outside the site.

None of the attacks on electric power systems in the United States has been large enough to cause widespread blackouts, but there are reasons for concern that the situation may worsen. Small-scale, unsophisticated attacks on power systems have

occurred here. Power systems in other countries, especially in Latin America and Europe, have suffered much worse and more frequent damage. Latin American and African countries have suffered outages of several weeks. Terrorist attacks in this country have not been a major problem over the past decade, but that could change rapidly. Terrorists could select power systems as targets if they want to cause a large amount of economic disruption with a relatively small effort. Efficient selection of targets would require more sophistication than has yet been shown by terrorist groups in the United States, but the required information and expertise are available from public documents as well as from foreign terrorist groups. In addition, some foreign groups might want to strike directly at the United States.

Hurricanes and earthquakes can also have a devastating effect on power systems, but the pattern of destruction would be much different than after a large-scale attack by saboteurs. Hurricanes affect distribution systems much more than generation and transmission. The relatively low lines are vulnerable to falling trees, flooding, and flying debris. Restoration may be a monumental task lasting several weeks or even months, but replacement parts are readily available, and utilities are experienced in the type of tasks required. However, the lingering blackouts following Hurricane Hugo demonstrated that greater advanced planning may be warranted. For instance, some types of transmission towers failed in the high winds, suggesting that more resilient designs should be used in vulnerable areas. Utilities along the Gulf and Atlantic coasts, areas vulnerable to hurricanes, should be studying the lessons learned from Hugo.

Earthquakes are quite capable of destroying generation and transmission equipment as well as distribution systems. However, where facilities have been constructed to withstand earthquakes, as in California, it is unlikely that more than a few key pieces of equipment would be damaged. The greatest concern is when an earthquake hits an area where seismic disturbances have not been considered in the design of equipment. The central Mississippi valley, the southern Appalachians, and an area centered around Indiana have the highest potential for earthquake damage. No plausible natural disaster should damage the bulk power system so badly as to cause widespread power outages for more than a few days if utilities have taken adequate precautions. Utilities normally can restore power fairly quickly unless multiple circuits are interrupted.

However it might occur, a long-term blackout is extremely expensive. Direct impacts include lost production and sales by industrial and commercial firms, safety (e.g., incapacitated traffic and air system controls), damage to electronic equipment and data, inconvenience, etc. Indirect costs include secondary effects on firms unable to conduct business with blacked-out firms, public health (e.g., inoperable sewage treatment plants), and looting. Table 1 summarizes the costs of the 1977 blackout in New York City, which lasted for about 25 hours. Blackouts of a few hours or days have been estimated to cost $1 to $5 per kilowatt-hour not delivered, far greater than what the power would have cost had it remained uninterrupted. Predicting costs for any specific longer-term outage is very uncertain because costs depend on many factors including the customers affected, the timing and duration of the outage, and the degree of adaptation customers and utilities can achieve to mitigate the outage.

Unless the damage is extremely severe, at least partial power could be restored in a matter of hours. Full restoration may take many months if a large number of key pieces of equipment have been destroyed. In the interim, customers would be faced with rolling blackouts, voltage reductions, or lower reliability. An additional impact is that the cost of the power that is available will be high if some of the most economical generating stations are damaged or isolated from loads by transmission system damage and therefore idled.

Component Vulnerability and Impact on System

Three factors determine the importance of any individual component—its susceptibility to damage; the effect on the power system of its loss; and the difficulty of its replacement or repair. These factors vary with particular circumstances. For example, generating stations can be destroyed by saboteurs willing to enter the plant, but the presence of utility employees performing their normal functions is a deterrent. However, if an insider is involved, sabotage becomes much easier. Similarly, the vulnerability of generating stations to earthquakes is low if they have been designed to withstand them and high otherwise.

Widespread, long-term blackouts could only be caused by damage to several circuits isolating

Table l-Cost of the New York City Blackout—1977[a]

Impact areas	Direct ($million)		Indirect ($million)	
Businesses	Food spoilage	$1.0	Small businesses	*$155.4*
	Wages lost	5.0	Emergency aid	
	Securities industry	15.0	(private sector)	5.0
	Banking industry	13.0		
Government			Federal Assistance	
(Non-public services)			Programs	11.5
			New York State	
			Assistance Program	1.0
Consolidated Edison	Restoration costs	10.0	New capital equipment	
	Overtime payments	2.0	(program and	
			installation)	65.0
Insurance[b]			Federal crime	
			insurance	3.5
			Fire insurance	19.5
			Private property	
			insurance	10.5
Public Health Services			Public hospitals-	
			overtime, emergency	
			room charges	1.5
Other public services	Metropolitan Transportation		MTA vandalism	0.2
	Authority (MTA) revenue:		MTA new capital	
	Losses	2.6	equipment required	11.0
	MTA overtime and		Red Cross	0.01
	unearned wages	6.5	Fire Department	
			overtime and damaged	
			equipment	0.5
			Police Department	
			overtime	4.4
			State Courts	
			overtime	0.5
			Prosecution and	
			correction	1.1
Westchester County	Food spoilage	0.25[c]		
	Public services			
	equipment damage,			
	overtime payments	0.19		
Totals		$55.54		$290.16

[a]Based on aggregate data collected as of May 1,1978.
[b]Overlap with business losses might occur since some are recovered by insurance.
[c]Lotting was included in this estimate but reported to be minimal.

Note: These data are derivative, and are neither comprehensive nor definitive.

SOURCE: Systems Control, Inc., Impact ofAssessrnent *of the* 1977 New York City Blackout (Washington, DC: US Department of Energy, July 1978), p. 3.

generating capacity from loads. No single failure should have a significant effect on power flow to customers since most utilities maintain sufficient generating and transmission reserves to accommodate such failures. If more damage occurs, either to generating stations or the transmission system connecting them to loads, the system can separate into islands. When these islands form, some have too much or too little generating capacity for their loads and lose all power. Other islands with approximate balance can maintain power, disconnected from the remainder of the system. The pattern of break up is not predictable, depending on the location of loads, which units are operating, the configuration of the transmission system, and the nature of the initiating event. Under extreme contingencies, substantial outages will occur. Modern protective circuitry should prevent the type of cascading failures across an entire system that occurred in the Northeast blackout of 1965, but there are many uncertainties over system behavior under untested conditions.

Power systems can be constructed to ride out almost any earthquake or hurricane with only minimal damage to components that would require months to replace. Most customers of an adequately prepared system will have their power restored within a day or two, though extensive damage to transmission and distribution lines may mean some outages for a few weeks. As noted above, however, a major earthquake east of the Rocky Mountains

would cause major problems because few facilities are designed to withstand such an event.

Sabotage could cause the most devastating blackouts because many key facilities can be targeted. Substations present the greatest concern. The transmission lines themselves are even easier to disrupt because they can be attacked anywhere along the line, but they are also much easier to repair. Generating stations are somewhat more difficult than substations to attack because they are manned and often guarded.

Substations are used at generating plants to raise the low voltage of the generator to the level of the transmission system, and near load centers to reduce the voltage for the distribution network. The former are partially protected by the routine activity at powerplants, but few of the latter have any more defense than a chain-link fence. In some cases, an attack can be carried out without entering the facility.

The destruction of two or three well-selected substations would cause a serious blackout. In many cases, most customers would be restored within 30 minutes, but this damage would so reduce reliability that some areas would be vulnerable to additional blackouts for many months. Virtually any region would suffer major, extended blackouts if more than three key substations were destroyed. Some power would be restored quickly, but the region would be subject to rolling blackouts during peak demand periods for many months. The impact would be less severe at night and other times when demand is normally less than peak, because utilities then would have a better balance of supply and demand. The greater the generating and transmission reserve margin, the less would be the impact on customers, because it is easier for utilities to find ways to get power delivered despite the damage.

Current Efforts To Reduce Vulnerability

Utilities historically have expended great efforts to ensure reliability, but only over the past few years have they started to take seriously the possibility of massive, simultaneous damage on multiple facilities. Awareness of the threat, however, has not yet led to the implementation of many measures to counter it. Few if any utilities plan their system and its operation to accommodate multiple, major failures, and key facilities are still unprotected.

Most of the actions the industry has taken have been instigated by the North American Electric Reliability Council (NERC) and the Edison Electric Institute (EEI). NERC completed a major study of vulnerability in 1988. Some of the recommendations have been adopted, while others are still under review. EEI has a large and active security committee which facilitates information exchange on physical protection of facilities.

The Federal Government's role for the most part has focused on national security issues—how to keep facilities operating which are vital to the United States during times of crisis. There has been less concern over the damage to the civilian economy that a major power outage would cause. The National Security Council is the lead agency for emergency preparedness, with the Federal Emergency Management Agency serving as adviser. Both of these agencies consider many vulnerabilities in addition to energy. Energy concerns are included in the new Policy Coordinating Committee on Emergency Preparedness and National Mobilization (PCC-EP/NM).

The Department of Energy (DOE) has prime responsibility for energy emergencies. DOE's Office of Energy Emergencies (OEE) was created to ensure that industry can supply adequate energy to support national security and the Nation's economic and social well-being. Most of OEE's activities have been directed at national security issues, but other efforts have included information exchanges with State governments, disaster simulations, and contingency planning. OEE also operates the National Defense Executive Reserve Program, which recruits civilian executives from the electric power industry among others to provide information and assistance in case of national emergency. DOE also has established a threat notification system to alert energy industries to potential problems.

The Department of Defense administers the Key Assets Protection Program. The Program's purpose is to protect civilian industrial facilities essential for national defense from sabotage during a crisis. The Program has identified electric power facilities required for vital military installations and defense manufacturing areas and coordinated plans for their protection with the owners.

Two trends that may increase vulnerability should be noted. First, the U.S. electrical equipment manufacturing industry has declined with the slow-

down in utility growth. Many production facilities have closed and the skills of their work forces have been largely lost. In addition, imports of equipment have risen to about 20 to 25 percent of the total market, and most U.S. production capability is controlled by foreign companies. The concern regarding vulnerability is that in a major emergency, say if all the transformers at several substations are destroyed, foreign companies may lack the incentive U.S. companies would have in expediting the restoration of service. If a worldwide resurgence of growth has filled their order books, will foreign companies accord adequate priority to U.S. emergency needs? There is no definitive answer to this question. Some observers see no problem while others are quite concerned.

Second, power systems reserve margins are dropping as growth in demand exceeds construction. Reserve margins have been unusually high and still are in some areas, so utilities find this trend economically beneficial. If a major disaster such as discussed in this report occurs, however, extra reserve margin would be extremely valuable in restoring service to some customers. Utilities would have additional options in finding ways to generate and transmit power. These options are disappearing as margins return to planned levels.

Policy Options To Further Reduce Vulnerability

Measures to reduce vulnerability can be grouped according to whether they prevent damage to the system, limit the consequences of whatever damage does occur, or speed recovery. An obvious way to prevent damage is to improve physical security and earthquake resistance for key facilities. The most problematic sites can be fairly well-protected against casual or unsophisticated attacks. The initial cost for walls around the transformers, crash-resistant fences, and surveillance systems would be a few percent of the replacement cost of the facility. Protection against a sophisticated attack would be extremely expensive, and probably not very effective unless response forces are near.

However, even if key facilities are protected, there is little that can be done to protect transmission lines against a saboteur with a high-power rifle. It is easy to destroy insulators on a transmission tower or the line itself, either of which will incapacitate the entire line. Such damage can be repaired quickly if sufficient replacements are on hand, but the saboteur can repeat it even more quickly in a different portion of the line or on other lines. Key transmission lines can thus be kept out of service (or at least kept unreliable) for long periods.

Protection of key facilities can also be enhanced by improved planning and coordination with the FBI to provide warning, and police or military forces to provide rapid response. Utility employee training can also be expanded to include greater awareness of suspicious activities and recognition of sabotage, so warning can be given to other facilities. These suggestions also have been made by NERC's National Electric Security Committee and have been adopted by NERC's Board of Trustees in October 1988.

Measures to limit the consequences of damage include improved training of system operators to recognize and respond to major perturbations, improved control centers and other system modifications, and increased spinning reserves. The intent of these steps is to isolate the damaged areas and keep as many customers as possible on-line. Rapid action can prevent the disruption from spreading as far as it otherwise might.

Measures to speed the recovery focus on the large transformers. The recovery period could be greatly reduced if more spares can be made available. One way would be to use those spares that utilities normally consider necessary for their own reliability but which are not actually in service at the moment. Legislation to relieve utilities of liability over potential blackouts in their own areas resulting from the absence of this equipment may be necessary. Alternatively, utilities could purchase spares for key equipment and store them in secure locations, or a stockpile of at least the most common transformers could be established.

A stockpile might entail initial costs of about $50 to $100 million for the step-down transformers used to lower voltage from the transmission system for use on a distribution network. Step-up transformers at generating stations are less standardized than step-down transformers. They employ a greater variety of voltages and different physical layouts for the high current bus from the generator. There is much less likelihood of finding a suitable spare, and a stockpile would have to be sizable. A less expensive alternative would be to stockpile key materials (copper wire, core steel, and porcelain)

and, in an emergency, to use preexisting designs instead of custom designing for the particular application. Under these conditions, manufacturing time could be reduced from over 12 months to about 6 months for four prototype units and two to three per month thereafter. However, the product would lack the optimization and state-of-the-art improvements of a custom-designed unit. Suboptimal transformers, whether stockpiled or manufactured generically, would be less efficient, resulting in significantly higher operating costs. Hence these expedited transformers might have to be replaced when better ones can be produced.

In addition to the measures intended to reduce the vulnerability of the existing system, the evolution of the electric power system can be guided toward inherently less vulnerable technologies and configurations. In particular, a system that emphasizes numerous small generators close to loads is, overall less vulnerable to sabotage. However, the total relative costs of moving toward dispersed systems are not clear, and substantial government incentive might be necessary to expedite the trend toward smaller units. Another step would be to improve standardization of system components to make stockpiling, equipment sharing, and emergency manufacturing easier. However, there are good reasons for the diversity of components, and standardization would result in some loss of efficiency of the system. Greater use of underground cables would also offer some advantages compared with overhead lines, though if damage does occur, replacement of cables is much slower and more costly.

These measures are listed in table 2. Some measures are already being addressed to some degree by the industry and government. Policymakers can accept this level of progress if present trends seem adequate for the level of threat. Alternatively, a more activist approach can be taken to enhance these steps and add others. Some of the steps listed would be quite expensive, but others would have nominal costs. Considering the present budget constraints, funding new costly initiatives will be justified only if the threat is seen as serious. Therefore table 2 notes whether the activity is being addressed under present trends, whether it can be implemented at low cost, or whether it would be relatively expensive. Several items appear in two categories, indicating differing levels of implementation, or planning in one and implementation in another. Utilities can be mandated to make these investments without government financial assistance, but that will make implementation more difficult unless they are assured of passing the costs on to their customers.

The appropriate level of government intervention is a matter of value judgment and opinion. The level of threat, both sabotage and natural disaster, cannot be quantified, and the costs of a major outage are highly dependent on the exact nature of the outage. If a worst case scenario is experienced, the costs would be much greater than all the measures discussed here. If a very strong earthquake occurs and suitable reinforcements avert major damage to the power system, or if terrorism increases in this country, then even very large investments will have been justified.

However, it is also impossible to quantify the degree to which these measures would reduce vulnerability. It is relatively easy to counter low-level threats, including almost all natural disasters, or prevent them from causing massive damage. It is much harder to counter any threat more serious than a small, unsophisticated terrorist group, though the recovery from the damage can be expedited. Furthermore, even greatly increased resistance to sabotage might just move the problem elsewhere. As noted above, if saboteurs can't destroy substations, they can still cause blackouts by shooting power lines. Alternatively, they can turn to other parts of the infrastructure, such as telecommunications or water supplies. Thus, it is questionable how much protection society would be buying.

It is possible to reduce vulnerability, but at a cost. Any of these measures can be justified if the threat is estimated to be sufficiently serious. Not taking any action is an implicit decision that no action is worthwhile. With the level of terrorism in this country as low as it is, many people will be skeptical of the need for any action, especially major investments such as increased reserve margins or stockpiles. However, terrorism could increase much faster than the measures to counter it could be implemented. If this seems plausible, then at least planning and other low-cost measures should be started earlier. If a rapid increase in terrorism seems at all likely, then even expensive measures are reasonable insurance. There is no "correct' answer as to which is the most appropriate approach.

Table 2—Options To Reduce Vulnerability

	Present trends	Low cost	Moderate to major investments
A. *Preventing damage*			
Harden key substations-protect critical equipment with walls, toughen equipment to resist damage, etc.			x
Surveillance (remote monitoring) around key facilities (coupled with rapid-response forces)			x
Maintain guards at key substations			x
Improve coordination with law enforcement agencies to provide threat information and coordinate responses	x		
B. Limiting consequences			
Improve emergency planning and operator training	x	x	
Modify the physical system; improve control centers, increased reserve margin, etc.			X
Increase spinning reserves		x	X
C. Speeding recovery			
Contingency planning for restoration of service	x	x	
Clarify legai/institutional framework for sharing reserve equipment	x		
Stockpile critical equipment (transformers) or any specialized material			X
Assure adequate transportation for heavy equipment	x	x	
Monitor domestic manufacturing capability		x	
D. General reduction of vulnerability		x	
Emphasize less vulnerable technologies			
Encourage decentralized generating systems	x	x	

SOURCE: Office of Technology Assessment, 1990.

Chapter 2
Causes of Extended Outages

Virtually everyone in the United States has some experience with power outages lasting at least a few minutes. Blackouts that last for a day or more are headline-making news, such as the 1989 storm damage in Washington, D.C. that kept some people without power for several days. Hurricane Hugo, one of the most destructive storms to strike North America this century, caused extensive damage to electric utilities in its path and left many people without power for several weeks. Over the last decade, concerns have begun to be raised about the possibility of extended blackouts due to intentional damage to electric power and other energy systems (e.g., sabotage). U.S. electric power systems have been targets of numerous isolated acts of sabotage. None has been serious enough to cause significant impact, but there is increasing recognition that a concerted effort by saboteurs could blackout major regions of the country.

This chapter focuses on extended outages caused by natural disasters and sabotage and their resulting effects on electric power systems. The impacts of extended outages, including costs, are discussed in chapter 3.

NATURAL HAZARDS

Natural hazards with the potential to cause extended blackouts include earthquakes, hurricanes, tornadoes, and severe thunderstorms. Each affects the power system differently. In general, earthquakes could damage all types of power system equipment, and are the most likely to cause power interruptions lasting more than a few days. Hurricanes primarily affect transmission and local distribution (T&D) systems, but the resultant flooding could damage generating equipment. Tornadoes and severe thunderstorms affect T&D lines directly through wind damage, and indirectly through downed trees, etc. Freak occurrences can cause particularly high levels of damage. In October 1962, for example, the only hurricane in recorded history to hit the west coast of the United States left parts of Oregon and Washington without power for up to 2 weeks, primarily because of the time needed to clear downed trees.

Earthquakes

An earthquake's actual impact depends on the population density and/or level of development in the affected area, the type of soil or rock material, the structural engineering, and advance warnings and preparation. For both loss of life and property damage, the most damaging earthquake of this century was Tangshan, China, in 1976 (Richter 7.8). Over 250,000 people died, and 20 square miles of the city were flattened.[1] The 1988 Armenian earthquake and the recent San Francisco Bay earthquake provide painful reminders of a strong earthquake's capacity to do damage and the importance of good seismic design and construction and emergency preparedness planning to mitigate the impacts (see box A).

Earthquakes sometimes result in compound disasters, in which the major event triggers a secondary event, natural or from the failure of a manmade system. In urban areas, fires may originate in gas lines and spread to storage facilities for petroleum products, gases, and chemicals. These fires often are a much more destructive agent than the tremors themselves because water mains and fire-fighting equipment are rendered useless. More than 80 percent of the total damage in the 1906 San Francisco quake was due to fire.

Most of the United States has some risk of seismic disturbance. The series of earthquakes that struck New Madrid, Missouri were probably the most severe in North America. The tremors were felt as far away as Boston. The first quake, which occurred in December 1811, may have been stronger than the 1906 San Francisco earthquake; it was followed in 1812 by hundreds of after-shocks.[2] According to the American Association of Engineers, it is very likely that a destructive earthquake will occur in the Eastern United States by the year 2010. The central Mississippi valley, the southern Appalachians, and an area centered around Indiana have the highest

[1]Robert Muir Wood, *Earthquakes and Volcanoes (New* York, NY: Weidenfeld & Nicolson, 1987).

[2]Robert Redfern, *The Making of a Continent (New* **York, NY: Times Books, 1983).**

Box A—The Armenian and San Francisco Earthquakes' Effects on Electric Power Systems

On December 7, 1988, Armenia was struck by a 6.9 magnitude earthquake-the most destructive to hit the region in centuries. Hundreds of buildings, including hospitals, schools, apartments, and industrial facilities, were destroyed. At least 30,000 people were killed and some 500,000 were either left homeless or jobless. Several large cities in the epicentral region sustained massive damage and high casualties. Leninakan, population 290,000, was 80 percent destroyed and Kirovakan, population of 150,000 was also heavily damaged. The city closest to the epicenter, Spitak, was completely destroyed. [1]

The high death toll was caused by the collapse of buildings, many of which were constructed of masonry and precast concrete. Building materials-such as structural steel and wood, which are more flexible than concrete—are in short supply in Armenia. Steel-frame buildings and other steel structures, such as construction cranes, sustained far less damage than concrete structures. Also, the lack of emergency preparedness planning contributed to the catastrophe. [2]

In contrast, the October 17, 1989 San Francisco Bay Area earthquake did not result in the catastrophic loss of life and property that was experienced in Armenia. The 7.1 magnitude earthquake was the strongest to hit the area since 1907. The death toll is at least 66 people and approximately 3,000 injured. The quake caused an estimated $7 billion in **damage in northern California.**[3] However, the growing California population, particularly in the earthquake-prone areas, could lead to a much greater loss of life and property in the future. Like Armenia, California lies within a large seismically active area. Unlike Armenia, though, California has one of the most comprehensive and up-to-date emergency preparedness plans in the United States and perhaps the world. For example, in June 1989, Pacific Gas & Electric (PG&E), the largest electricity supplier in the area, performed a company-wide earthquake emergency exercise. This exercise proved invaluable in responding to the real thing 4 months later, according to PG&E.[4] In addition, a great deal of attention is given to seismic considerations in structural design, engineering, and construction. These and other factors can mitigate the impacts of a major earthquake disaster.

Armenia[5]***-In*** Armenia, electricity was interrupted for 4 to 7 days in the epicentral area. Two substations were severely damaged or almost totally destroyed. A 220-kV facility in Leninakan sustained damage to capacitor racks, ceramics, and circuit breakers. The 110-kV facility near Nalband was almost totally destroyed. The under-reinforced masonry and precast concrete control house collapsed and struck nearby equipment as it fell. Transformers, circuit breakers, and capacitor banks were severely damaged. Soviet authorities had to bring in a rail-mounted substation to restore power to the region.

The two-unit Armenian Nuclear Powerplant, located 75 kilometers south of the epicenter, continued to operate during and after the earthquake. But, the plant was eventually closed because the units required substantial additional seismic reinforcement to remain safe, and the price was considered prohibitive.

No damage to steel transmission towers throughout the region was reported. Wooden poles also survived intact, except for a few cases where partially rotted poles snapped at their bases.

San Francisco—About 48 hours after the San Francisco earthquake, electricity had been restored to all but 12,000 of the 1 million customers affected. About half were those in the Marina District of San Francisco, which sustained heavy damage.[6]

The Moss Landing powerplant and high-voltage switchyards, located near the earthquake's epicenter, were heavily damaged. PG&E indicated that a 340-ton air preheater was knocked off its pedestal and the bottom dropped out of an 800,000-gallon raw water tank, creating a bog.[7] Only one section of a 230-kV circuit near Moss Landing was knocked down. However, substantial damage was reported to distribution lines, especially in the Santa Cruz area. Damage to distribution lines in San Francisco was limited because most are located underground.[8]

---

1 "Real-World Lessons *in* Seismic Safety," *EPRI Journal*, June 1989, p. 23.

2 Ibid.

3, 'California *Governor* Signs *Earthquake* Relief Measures, ' *Washington Post, Nov. 7,* 1989, p. A-14.

4 "PG&E Credits Mock Earthquake Drill in Responding Quickly to Real Thing,' *Electric Utility Week,* Oct. *30, 1989,* p. *3.*

5 "Real World Lessons in *Seismic Safety, "* op. cit., footnote 1.

6 "PG&E credits Mock Earthquake Drill in Responding Quickly to Real Thing," Op. cit., footnote 4.

7 "Coping With Loma Prieta: How PG&E's Gas and Power System Fared," *The Energy Daily,* vol. 17, No. 234, Dec. 12, 1989, p. 3.

8 "Earthquake Cuts Off a Million PG&E Customers; Two-Thirds Back in Day," *Electric Utility Week,* Oct. *23,* 1989, p. 2.

potential for earthquake damage.[3] An earthquake similar to the New Madrid series would seriously affect 12 million people in seven States.[4]

Impact on Electric Power Systems

More than any other natural hazard, major earthquakes are capable of producing almost complete social disruption in modern urban areas. Infrastructure, both above and below ground, may be shattered, and quick repair of below-ground items is almost impossible. Earthquakes can destroy all types of power system equipment, but the damage drops off rapidly with distance from the epicenter. Most structural research has gone into multi-story buildings, darns, nuclear powerplants, and storage tanks.[5]

Except for structures located at points of earth slippage, foundations in reasonably firm soil will tend to move with the ground without damage or relative displacement. Above grade, however, natural modes of vibration of the structure may be excited, amplifying the ground motion.[6] Depending on its age or size, a powerplant itself may survive a moderate-to-severe quake, but its stacks might not.

The only large generating plant damaged by the 1989 San Francisco earthquake was the Moss Landing facility, located about 20 miles south of Santa Cruz, the earthquake's epicenter. In addition, two 104-MW generating units at the Hunter's Point powerplant in San Francisco were briefly shutdown manually after the earthquake shed the load, but were returned to service within 24 hours. The quake also knocked out of service five small generating plants, totaling 467 MW, near San Luis Obispo, some 230 miles south of San Francisco, but did not affect the Diablo Canyon nuclear plant.[7]

The increase in transmission voltage over the years has resulted in larger substation equipment whose size makes it more seismically vulnerable. The increased susceptibility to damage is caused by two principal factors: 1) a drop of the frequencies of vibration into a lower and more severe region of the characteristic seismic frequency range, which produces an amplification of the seismic forces in the equipment; and 2) the inherent structural deficiencies—the brittle nature and low-energy dissipation properties-of electrical insulating material such as porcelain.[8]

In the 1971 San Fernando earthquake, failures occurred in many new extra-high-voltage (EHV) substations which had not previously been subjected to a strong seismic event. Subsequent studies by manufacturers and utilities resulted in modification of some of the existing equipment and extensive revision of the specifications for future substation equipment. The design criterion for seismic acceleration increased from 0.2 to 0.5 Gs in the most seismically active areas. The 1972 standard in Japan, where earthquakes are frequent, was 0.3 Gs.[9] The Institute of Electrical and Electronic Engineers has seismic qualification standards for power transformers, lightning arresters, circuit breakers, relays, etc. 10

During the 1989 San Francisco earthquake, PG&E experienced significant internal damage to a 500-kV substation located near the Moss Landing powerplant. Damage to circuit breakers and transformers at the substation isolated two 112-MW units that were operating at the Moss Landing facility at the time of the earthquake.[11]

Performance of transmission lines, towers, and poles under earthquake conditions generally has been excellent. Steel towers move with the ground and the acceleration stresses are well within the

---

[3]Coordinating Committee on Energy of the Public Affairs Council, American Association of Engineering Societies, *Vulnerability of Energy Distribution Systems to an Earthquake in the Eastern United States--An Overview,* December 1986.

[4]U.S. Geological Survey, National Center for Earthquake Engineering Research.

[5]Gilbert F. White and J. Eugene Haas, *Assessment of Research on Natural Hazards* (Cambridge, MA: The MIT Press, 1975).

[6]L.W. Long, "Analysis of Seismic Effects on Transmission Structures, " paper presented at the IEEE PES Summer Meeting and EHV/UHV Conference, Vancouver, BC, Canada, July 1973.

[7]"PG&E Credits Mock Earthquake Drill in Responding Quickly to Real Thing," *Electric Utility Week,* Oct. 30, 1989, p. 3; "Earthquake Cuts Off a Million PG&E Customers; Two-Thirds Back in Day,' *Electric Utility Week,* Oct. 23, 1989, p. 2.

[8]K.M. Skreiner and L.D. Test, "A Review of Seismic Qualification Standards for Electrical Equipment," *The Journal of Environmental Sciences,* May/June 1975.

[9]Ibid.

[10]IEEE 323.1974, standards for safety-related equipment.

[11]"PG&E Credits Mock Earthquake Drill in Responding Quickly to Real Thing," op. *Cit.,* footnote 7.

margins required for wind resistance. Wood poles are inherently more flexible than steel towers, and the flexibility reduces the seismic stress substantially.[12] However, earthquakes can cause transmission outages when tower foundations are subject to earth slippage. Detailed soil analysis, adequate footing design, and periodic inspection of existing foundations are essential. In the 1971 San Fernando earthquake, tower foundations failed that over the years had their strength reduced by erosion or adjacent excavation for roads or buildings.[13] The only major transmission line damage reported during the 1989 San Francisco earthquake was a section of 230-kV circuit between the Moss Landing powerplant and Watsonville. However, substantial distribution line damage was reported in areas close to the earthquake's epicenter.[14]

Hurricanes

The losses caused by a landfall hurricane are a function of the storm's strength and path and the area's population and economic development. Hurricanes are accompanied by torrential rains, typically 3 to 6 inches but more if the forward progress is slow. Winds can exceed the design of a total structure or its components and cladding, or cause hazards from windborne debris. The winds also produce disastrous sea surges and waves. A large proportion of the damage to coastal areas is caused by the storm surge, an influx of high water accompanying the hurricane. Other hazards include flooding of streams induced by the heavy rainfall and accelerated coastal erosion. Occasionally tornadoes accompany a hurricane.[15]

In the United States, most hurricane damage occurs in a narrow zone along the coastlines of the Atlantic Ocean and Gulf of Mexico. The trend is toward fewer deaths due to improved storm warning and management. However, property loss is increasing because of greater coastal development.[16]

Effects on Electric Power Systems

Hurricanes primarily affect T&D lines. High winds can damage or uproot T&D poles. Poles can also fall when soils become water saturated by accompanying torrential rains, as was the case in 1982 when Hurricane Iwa struck the Hawaiian Islands and in 1989 when Hurricane Hugo hit the Carolinas. Hurricane Hugo knocked out power to more than 1 million customers in the Carolinas. Many people were left without power for several weeks. High winds and flying debris downed transmission towers and several hundred miles of transmission lines, and falling trees knocked out thousands of distribution lines. Four utilities hardest hit by the September 22, 1989 storm have indicated that the cost of restoring service and cleanup may exceed $170 million. Insurers are expected to pay for about 10 percent of the cost.[17] See box B for a discussion of Hurricane Hugo's effect on the largest supplier of electricity in South Carolina.

Tornadoes and Thunderstorms

In the United States, tornadoes are most prevalent in a region known as "Tornado Alley' that extends from the western Texas Panhandle across Oklahoma, Kansas, southern Nebraska, and Iowa, but have been known to occur in all States.[18]

Tornadoes kill hundreds of people and destroy property valued at billions of dollars every year. The combination of high winds and the sudden drop in air pressure causes heavy destruction of everything in a tornado's path.[19] Heavy rain and large hailstones often fall north of the tornado's path. Tornado families occur when up to six tornadoes are spawned from the same thunderstorm.[20]

Severe thunderstorms can produce damaging lightning and high winds with the potential to cause extended blackouts. For example, the 1977 New York blackout began with a series of severe lightning strokes. Also, in 1989, a severe thunderstorm

[12] Long, op. cit., footnote 6.

[13] Albert W. Atwood, Jr., and Kenneth L. Griffing, comments on Long, Op. cit., footnote 6.

[14] "PG&E Credits Mock Earthquake Drill in Responding Quickly to Real Thing," op. cit., footnote 7, p. 3.

[15] White and Haas, op. cit., footnote 5.

[16] Ibid.

[17] "Damage Estimates From Hurricane Hugo Pegged at up to $170 Million," *Electric Utility Week*, Nov. 13, 1989, p. 5.

[18] "Tornado," *McGraw-Hill Encyclopedia of Science & Technology*, vol. 18, 1987.

[19] "Tornado," *Encyclopedia Americana*, vol. 26, 1986.

[20] "Tornado," *McGraw-Hill Encyclopedia of Science and Technology*, vol. 18, 1987.

Box B—Hurricane Hugo's Effect on South Carolina Electric & Gas Co.[1]

Hurricane Hugo was one of the most powerful hurricanes to strike North America in this century and the most powerful to strike the Carolinas. Property damages in North and South Carolina alone are estimated to be about $6.5 billion.[2] The hurricane caused extensive damage to electric utilities in its path. Hardest hit was South Carolina Electric & Gas Co. (SCE&G), the largest supplier of electricity in South Carolina. Of SCE&G'S 430,000 customers, 70 percent were blacked out during the storm. After 5 days, about 140,000, or 33 percent, were still without power. Full service was restored in less than 3 weeks.[3]

In Charleston and Summerville, transmission and distribution circuits were especially hard hit by high winds, flying debris, and falling trees. The distribution system in these two areas was almost completely leveled. While there was damage to the transmission system, the delay in repair was primarily due to the extent of the damage to the distribution system. No significant damage was reported to generating units or transmission substation equipment. However, a cooling tower at one 600-MW unit was destroyed. Temporary repairs were made and the unit was back in service in less than a week. Only one power transformer, a 115/230-kV unit, which served a distribution station, was damaged in the storm.

There was a lot of damage from trees that were broken and blown into the distribution and transmission systems. Before repairs could be made, roads, lines, and access had to be cleared. Since it had been over 30 years since a major hurricane had struck the area, there was an unusually large amount of debris from wooded areas. The debris, while often not damaging the system, still required crews to physically remove branches, etc. from the transmission towers, distribution poles, and conductors.

Throughout the SCE&G system, two-thirds of the transmission circuits were out of service immediately following the storm. About 300 towers, out of a total 24,000, were either toppled or broken. Contributing factors in the damage to the transmission system were the number of wooden pole transmission towers in the 230-kV and 115-kV systems and the amount of rain that preceded the storm. Soil conditions were especially poor in wet and low-lying areas. Transmission towers in those areas fell because the footing had become too soft and weak from the rain. SCE&G and other coastal utilities are reevaluating the foundation requirements of towers near marshes, swamps, and river crossings.

As many as 3,600 workers labored to restore electric service at SCE&G, with 75 percent of them working on the transmission and distribution systems. Over 90 percent of the workers were from neighboring utilities and private contractors. Line crews came from Alabama, Arkansas, Florida, Georgia, Mississippi, Louisiana, Maryland, Tennessee, Virginia, and Illinois. Many of the crews brought their own vehicles and specialized equipment. This was done as part of mutual assistance agreements among utilities.

1 Casazza, Schultz& Associates, Inc., "Vulnerability of Electric Power Systems to Sabotage and Natural Disasters," contractor report prepared for the Office of Technology Assessment, Nov24, 1989.

2 Edward v. Badolato et al., Clemson University, The Strom Thurmond Institute of Government and Public Affairs, "Hurricane Hugo—Lessons Learned in Energy Emergency Preparedness," 1990, p. 1.

3 There were still customers without service, but the problem was with the customers, not the utility. Many homes and businesses were too severely damaged to have service restored.

blacked out portions of the Washington, DC area for several days, primarily because of the number of downed trees.

Effects on Electric Power Systems

In general, property damage from tornadoes has declined sharply due to improved prediction and increased public awareness. Tornadoes are more likely to cause damage to transmission and distribution lines over a small geographic area than wipe out a substation or generating plant.

Thunderstorms are more widespread and consequently more disruptive. High winds, torrential rains, and lightning can wreak havoc on distribution lines.

Geomagnetic Storms

Large fluctuations in the Earth's magnetic field caused by solar disturbances are called geomagnetic storms. The Sun continuously emits a stream of protons and electrons called the solar wind. Solar disturbances such as sunspots and solar flares create gusts in the solar wind, with a more intense stream of charged particles emitted. When the solar wind hits the Earth's magnetic field it produces electric currents in the atmosphere, altering the magnetic

field (as well as causing the aurora borealis). Both solar activity and geomagnetic storms ebb and flow in an 1 l-year cycle, although large storms may occur at any time. The peak of the current geomagnetic storm cycle, which is expected to be the most violent yet recorded, is anticipated to arrive in approximately 1991.[21]

Effects on Electric Power Systems

Fluctuations in the Earth's magnetic field create electric potentials (differences in voltages) on the Earth's surface. The resulting electric potential differences of 5 to 10 volts per mile fluctuate very slowly and are typically aligned from east to west. Geomagnetically induced currents (GICs) flow wherever a power line connects areas of different electric potential. The magnitude of GIC depends on several factors including a power line's location, length, and resistivity relative to the resistivity of the ground. Areas with long east-west transmission lines and highly resistive geology typical of igneous rock formations are most likely to experience large GICs.

GIC produced in a power system may either damage equipment or merely take it out of service during the course of the geomagnetic storm. Both may lead to system outages. When struck by GICs, EHV transformers may overheat, resulting in permanent damage or reduced life. Voltages in transformers may drop significantly, leading to unacceptable loadings on generators and transmission lines resulting in their being taken out of service by protective relays. Harmonic distortions created in the transformers may cause misoperation of relays, too. Relays may operate when they shouldn't, resulting in equipment being taken out of service unnecessarily; they may also fail to operate when needed, resulting in damage to the attached equipment.

A very strong geomagnetic storm on March 13, 1989 damaged voltage control equipment in Quebec, resulting in the collapse of nearly the entire system for a 9-hour blackout. The same storm tripped protective relays in several areas of the United States and damaged several large transformers. One of these transformers, a step-up unit at the Salem Nuclear Plant in New Jersey, had to be removed from service, forcing the plant to shutdown for 6 weeks.

SABOTAGE

No long-term blackouts have been caused in the United States by sabotage. However, this observation is less reassuring than it sounds. Electric power system components have been targets of numerous isolated acts of sabotage in this country. Several incidents have resulted in multimillion-dollar repair bills. In several other countries, sabotage has led to extensive blackouts and considerable economic damage in addition to the cost of repair.

Some terrorist groups hostile to the United States clearly have the capability of causing massive damage-the loss of so many generating or transmission facilities that major metropolitan areas or even multi-state regions suffer severe, long-term, power shortages. The absence of such attacks has as much to do with how terrorists view their opportunities as with their ability. U.S. electric power systems are only one target out of many ways of striking at America, and not necessarily the most attractive.

This section briefly reviews the range of acts of sabotage against electric power systems and the capabilities of different types of saboteurs. However, an analysis of the motivations and intentions of terrorists is beyond the scope of this study. Several referenced studies have considered this subject. The reader is also referred to a forthcoming OTA study "The Use of Technology To Counter Terrorism.'

Experience With Sabotage

United States

Over the past decade there were few notable acts of sabotage, and apparently none that were intended to cause harm other than to the local utility. The most common cause has been labor disputes. In July 1989, a tower on a 765-kV line owned by the Kentucky Power Co. was bombed, temporarily disabling the line. No arrests have been made. In 1987-88, power line poles and substations were bombed or shot in the Wyoming-Montana border area. Later in 1988, similar attacks were experienced in West Virginia. Such attacks had also occurred in 1985 in West

[21] This discussion is drawn from: "A Storm From the Sun," *EPRI Journal*, July/August 1989, pp. 14-21; V.D. Albertson, "Geomagnetic Disturbance Causes and Power System Effects," *ZEEE Power Engineering Review*, July 1989, pp. 16-17; J.G. Kappenman, "Power System Susceptibility to Geomagnetic Disturbances: Present and Future Concerns," *IEEE Power Engineering Review*, July 1989, pp. 15-16; and D. Soulier, "The Hydro-Quebec System Blackout of March 31, 1989," *ZEEE Power Engineering Review*, July 1989, pp. 17-18.

Virginia and Kentucky. All these attacks occurred during coal mine strikes.[22] Two Florida substations were heavily damaged by simultaneous dynamite explosions in 1981 in one of the most expensive incidents. Damages totaled about $3 million, but no significant customer outages resulted. No arrests have been made, but circumstantial evidence points to a contractor labor dispute.[23]

Incidents stemming from unknown motives include the cutting of guy wires and subsequent toppling of a tower on the 1,800-MW, 1,000-kV DC intertie in California in 1987. There was negligible impact on the power system, because the load on the line was light at the time and it was scheduled for maintenance the next day, so alternate power routes had already been arranged. Damage was repaired in about 4 days.[24] No suspects have been announced. Wooden poles were also cut in Colorado in 1980, bringing down a 115-kV line. The damage was repeated later in the year. Total costs were about $200,000 each time.

Another incident demonstrates that saboteurs can mount a coordinated operation. In 1986, three 500-kV lines from the Palo Verde Nuclear Generating Station were grounded simultaneously over a 30-mile stretch. It happened at a time when none of the nuclear reactors was operating, so no disruption occurred. Under different conditions, the reactors would have shut down. No arrests have been made.[25]

In 1989, several environmental extremists were arrested in the act of cutting a tower on a line in Arizona. The group, which reportedly had been inspired by Edward Abbey's *The Monkeywrench Gang*, had been infiltrated by the FBI. Two members of this group have prepared a manual detailing how to attack equipment and facilities, including power lines, deemed harmful to the environment.[26]

Since 1980, only Puerto Rico has experienced extensive attacks that might be characterized as terrorist, as opposed to labor disputes or vandalism. In 1980-82, many bombings occurred at substations and transmission towers. Some of these incidents have been attributed to Macheteros, a separatist group. Several of the resultant outages lasted for several days.

The FBI and other agencies do not maintain statistics on energy facility sabotage separately from those of other targets. The best available database is that developed from public sources by a private consultant to the Department of Energy, which records a total of 386 attacks on U.S. energy assets from 1980 through 1989, an average of 39 per year.[27] Electric power systems, mostly transmission lines and towers, were the target in a large fraction of these 386. This database may understate the problem because some utilities may not publicize attacks out of concern that more may be inspired.

Other Countries

Terrorist sabotage has been much more extensive and violent in Europe and Latin America than in the United States. Attacks have been made by separatists, radical revolutionaries, and anti-technology and anti-nuclear groups. A few examples will illustrate this:

France has experienced assassinations of energy officials as well as bombings, arson, rocket attacks on energy facilities, and grounding of transmission lines. The saboteurs included anarchic, separatist, and political terrorists, and anti-nuclear extremists.

West Germany also is familiar with bombings and assassinations from the Baader-Meinhof group, Red Army Faction, and other groups. In addition, there has been an intensive campaign to destroy transmission lines by cutting or bombing towers. In 1986 alone, about 150 acts of such sabotage were committed. Much of the violence has been by politically motivated or anti-nuclear extremists. Transmission lines from nuclear reactors have been a major focus, and the nuclear industry itself has been a target.

Attacks on electric power systems have been most severe in El Salvador. The Farabundo Marti National Liberation Front (FMLN) has repeatedly bombed or fired on transmission towers, substations,

[22]Robert K. Mullen, Consultant t. the U.S. Department of Energy, testimony at hearings before the Senate Committee on Governmental Affairs, Feb. 7-8, 1989, pp. 246-247.

[23]Kenneth Caldwell, Manager of Corporate Security Services, Florida Power& Light Co., personal communication, Feb. 7, 1990.

[24]*Electric Utility Week,* Aug. 10, 1987.

[25]Mullen, op. cit., footnote 22.

[26]Dave Foreman and Bill Haywood (eds.), *Ecodefense: A Field Guide to Monkeywrenching*, 2nd ed. (Tucson, AZ: Ned Ludd Books, 1987).

[27]Robert K. Mullen, personal communication Feb. 7, 1990.

and hydroelectric powerplants. Up to 90 percent of the entire Nation has been blacked out by the FMLN during some sabotage campaigns. The FMLN has even produced a manual detailing how to attack an electric power system. According to official sources, the FMLN has launched over 2,000 attacks on electric systems since 1980. The Sendero Luminosa (Shining Path) revolutionary group has adopted a similar strategy in Peru, frequently leaving Lima, as well as a 600-mile stretch of the country, blacked out or under power rationing for 40 to 50 days.[28]

Countries where insurgents or hostile forces have targeted electric power systems have found it worthwhile to take protective measures. Passive techniques, such as concrete sheaths around transmission tower legs, make them more difficult to topple. Some countries, including South Korea, maintain army conscripts at key facilities. Because of the expense of adequately protecting distributed systems, others simply repair the damage, and may design their systems to be easily repairable.

The Threat

Intentional damage to an electric power system can be caused by a wide variety of actors. Most common are ordinary vandals, typically hunters who shoot at transmission lines or the insulators attaching them to towers. Utilities are experienced with handling vandalism, which is very unlikely to cause massive damage. Hence this report is not concerned with vandalism except to the extent that remedial measures for more serious attacks might have an incidental value in reducing it.

The Single Saboteur

Most of the U.S. incidents noted above could have been caused by one person. The fact that most have been relatively minor suggests that either the saboteurs did not know how to cause greater damage or they did not want to. In sabotage initiated over labor disputes, the perpetrators usually are trying to hurt the utility or their suppliers, not to cause widespread blackouts. The dispute would have to get extraordinarily bitter before anyone would risk antagonizing a large part of the public. A personal grievance might be a more probable motivation for an individual to try to cause widespread damage. A utility employee who felt misused might want to use his expertise to retaliate in a spectacular fashion. Alternatively, any of the motivations of a group, discussed below, might apply to an individual who decides to take matters into his own hands.

The primary difficulty faced by a single saboteur intent on causing a devastating blackout would be to assemble all the necessary information and supplies. He would have to get the idea in the first place; research how electric power systems work and what the vulnerable points are; determine the layout of his target system; physically locate the actual targets; plan the attack in considerable detail; procure explosives; rehearse; and carry out the actual attack. If any of these steps were deficient, the attack would lose effectiveness.

It is unlikely, though not impossible, that an independent individual will combine the motivation, expertise, contacts to procure explosives, tenacity, and nerve to disable as many as eight facilities simultaneously. This would require visiting all the sites over several days and would entail a significant risk of detection. A more probable scenario for the independent saboteur is a one-night series of assaults on as many facilities as he can reach. Such an attack can still cause major problems for a utility, but far fewer than would more widespread damage. Theoretically, the saboteur could continue his attacks, but once utilities are alerted they can post guards to deter an immediate reoccurrence of the rampage.

Terrorist Groups

Organizations initiating terrorist attacks in other countries include separatists, political radicals, and anti-technology and/or anti-nuclear extremists. The only significant separatist movement in the United States in the past 125 years has been in Puerto Rico, and none seems likely to develop. Nor do the anti-technology or anti-nuclear movements seem likely to turn to large-scale, violent extremes, in part because people have peaceful ways to try to implement their views.

This country has had more experience with politically oriented extremism, particularly in the sixties and seventies. The Weathermen and other groups did bomb some transmission towers and might well have wanted to cause more damage. Much of this violence was in reaction to the war in Vietnam It should be noted that current trends, if anything, indicate a lessening of terrorist attacks.

[28] Ibid.

However, under some conditions, this threat might reemerge, possibly by environmental extremists. Electric power systems probably are not the most obvious targets but could become fashionable if terrorists choose to inflict great inconvenience and economic cost on society instead of more dramatic acts such as assassinations or destruction of symbolic targets. The Evan Mecham Eco-Terrorist International Conspiracy (EMETIC) targeted electric system facilities in 1987 -89.[29] Even extortion on a gigantic scale might be considered to raise funds and shake confidence in existing institutions.

Foreign groups could also import violence. American property and individuals abroad have been the targets of attack in many countries. It is not clear why some of the groups hostile to the United States have not carried their struggles here, and therefore it cannot be guaranteed that they won't. Groups in volatile areas such as the Middle East and Central America might want to hurt the United States directly. Separatists might want to pressure this country to influence events in their country, even if they have no direct conflict with us. Drug cartels in Colombia could hope to make our drug wars too costly. Environmental extremists concerned over potential global climate change might see the U.S. electric power system as symbolic of the refusal to curb production of carbon dioxide. The logic does not have to be sound for an attack to be damaging.

A group is much more likely than an individual to be able to mount a major assault on sufficient facilities to cripple a power system. A group combines all its members' skills and contacts and can share tasks. In particular, international contacts among terrorist groups multiply the expertise and resources available to any group. The knowledge gained by destroying substations and power lines in Germany and El Salvador is available in the United States. In fact several "how-to" sabotage manuals are available for sale here. Weapons and explosives are also widely available here and abroad. If foreign terrorist groups wish to attack the United States, they can probably find assistance herein obtaining target information and in camouflaging their activities.[30] However, a group is also much more likely to be detected than an individual.

Military Attacks

Commandos with special training and essentially unlimited resources and support could mount a far stronger attack than could even the most sophisticated subnational terrorist group that has yet emerged. The Soviet Union is reported to have such forces, called spetsnaz, available for operations in the United States.[31] The object would be to create havoc and demoralization before overt hostilities commence. While this risk is diminishing, it has not disappeared. Alternatively, a hostile country might take this approach if it were unable or unwilling to declare war but wanted to take some military action against the United States.

The ultimate attack would be an overt military operation. The vulnerability of electric power systems can have serious national security implications. For example, in World War II, Germany's highly centralized electric system was not attacked until late in the war. German officials, surprised at this omission, commented after the war that ''The war would have finished two years sooner if you (the Allies) had concentrated on the bombing of our powerplants earlier. . . " When the Allies finally did destroy Germany's electric generating and synthetic fuel facilities, the German economy was crippled.[32] This experience will not be ignored in any future hostilities.

For defenses to be effective against military assault, either commando or overt, they would have to be extraordinarily strong and expensive, well beyond anything that might be justified against subnational terrorists. Since even a limited terrorist attack could have extremely serious consequences, this report focuses on responses to that threat. Actions necessary only to counter military threats are beyond the scope of this report, but it notes potential benefits of a few of the counterterrorism steps.

---

[29]Robert K. Mullen, *personal* communication Apr. 2, 1990.

[30]Yonah Alexander, "International Network of Terrorism," *Political Terrorism and Energy,* Yonah Alexander and Charles K. Ebinger (eds.) (New York, NY: Praeger Publishers, 1982).

[31]Victor Suvorov, *SPETSNAZ, The Inside Story of the Soviet Special Forces* (New York, NY: W.W. Norton & Co., 1987) and as partially reprinted *in the* Hearings Record of the Senate Committee on Governmental Affairs, "Vulnerability of Telecommunications and Energy Resources to Terrorism," Feb. 7 and 8, 1989.

[32]Federal Emergency Management Agency, ''Dispersed, Decentralized and Renewable Energy Sources: Alternatives to National Vulnerability and War," December 1980.

Chapter 3
Impacts of Blackouts

The United States has had little experience with blackouts that last more than a few days. The only major blackouts over the past 25 years have been the 1965 Northeast blackout, the 1977 New York City blackout, the August 1988 downtown Seattle blackout, and the 1989 blackout in the Carolinas. Most of what we know is anecdotal evidence, drawn primarily from the well-documented 1965 Northeast and 1977 New York City blackouts. The lessons learned from the recent Hurricane Hugo experience should provide additional information on the impacts of blackouts. This is particularly important in light of the technological changes that have occurred in the last decade-especially the proliferation of computers and automation in all sectors and the advances in telecommunications which require a reliable supply of power.

This chapter provides an overview of costs and reviews the quantitative estimates for both actual and hypothetical outages. The remainder of the chapter discusses the impacts of blackouts on the industrial, commercial, and residential sectors and on essential services and infrastructure.

OVERVIEW OF COSTS OF BLACKOUTS

Blackouts have impacts that are both direct (the interruption of an activity, function, or service that requires electricity) and indirect (due to the interrupted activities or services). Examples of direct impacts include food spoilage, damage to electronic data, and the inoperability of life-support systems in hospitals and homes. Indirect impacts include property losses resulting from arson and looting, overtime payments to police and fire personnel, and potential increases in insurance rates. Direct and indirect impacts can be characterized by whether they are quantifiable in monetary terms (economic impacts); relate to the interruption of leisure or occupational activities (social impacts); or result in organizational, procedural, and other changes in response to blackout conditions (organizational impacts).[1]

Direct impacts can be avoided if the end-user has backup systems, but these have often proved unreliable. Indirect impacts may be partially mitigated through contingency planning, improved communications, customer education, social programs, and other planning approaches.[2]

Estimating the costs of electric power outages is difficult and imprecise because the economic value of electric reliability to different customers is not well-understood. Only recently has much progress been made in developing economic values for reliability, including the development of analytical techniques for measuring or estimating the direct and indirect costs of actual and hypothetical outages.

To estimate costs, utilities and public utility commissions (PUCs) rely on either hypothetical cost analysis or reconstruct the level of economic activity that might have occurred had there been no blackout. Both of these methods have inherent uncertainties, and theoretical models have their own shortcomings. Also, indirect and social costs often cannot be quantified but only enumerated.[3]

Types of Costs

The kinds of costs considered in value of reliability estimations include both short-term outage and long-term coping or adaptive response costs.

The true economic cost of any outage is the opportunity value of profit, earnings, leisure, etc. that would have been produced but for the loss. Therefore, one must ascertain what the lost opportunities were and how they would have been valued by those who suffered the loss. The short-term outage costs are incurred during and shortly afterward, and include product spoilage, lost sales, foregone leisure, and other opportunity costs. Long-term coping costs are incurred when customers invest in equipment to mitigate the effects of a shortfall. Investment in backup generators, for example, is clearly made to mitigate the impact of future outages. Historically, mitigation costs have been relatively insignificant in

[1]William T. Miles, Jane Corwin, and Peter D. Blair, "Cost of power Outages—The 1977 New York City Blackout," paper presented at the IEEE Industrial and Commercial Power System Technical Conference, Seattle, WA, May 14-17, 1979, pp. 65-66.

[2]Ibid.

[3]Ibid., p. 66.

Table 3—Direct and Indirect Costs

Primary electricity user	Direct cost components (costs to household, firm, institution, etc.)	Indirect rests	Remarks
Residential	a. Inconvenience, lost leisure, stress b. Out-of-pocket costs —spoilage -property damage c. Health and safety	a. Costs on other households and firms b. Cancellation of activities c. Looting/vandalism	Indirect costs are a minimal, if not negligible, fraction of total (direct and indirect) costs of a curtailment.
Industrial, commercial, and agricultural firms	a. Opportunity costs of idle resources —labor —land -capital —profits b. Shutdown and restart costs c. Spoilage and damage d. Health and safety effects	a. Cost on other firms that are supplied by impacted firms (multiplier effect) b. Costs on consumers if impacted firm supplies a final good c. Health and safety-related externalities	Indirect effects are likely to be minimal for most capacity-related interruptions, but can be significant component of total costs for longer duration energy shortfalls.
Infrastructure and public service	a. Opportunity cost of idle resources b. Spoilage and damage	a. Costs to public users of impacted services and institutions b. Health and safety effects c. Potential for social costs stemming from Looting and vandalism	Indirect costs constitute a major portion of total costs of curtailment.

SOURCE: M. Munasinghe and A. Sanghvi, "Reliability of Electricity supply, Outage Costs and Value of Service: An Overview," *The Energy Journal,* vol. 9, 19s8, p. 5.

most parts of the United States due to the high standard of reliability.[4]

Short- and long-term costs may have both direct and indirect elements (see table 3). Direct costs are those suffered by the direct customer, such as spoilage or lost production. Indirect costs include those realized by customers of an impacted firm; they may have to purchase higher cost substitutes, incur additional production costs, or have unrecovered costs. Indirect costs can be several times as large as direct costs because the loss of a single input may retard an entire production process. Other components of indirect costs include the multiplier effect from lost wages and other factors of production[5] and potential social costs stemming from looting and vandalism. Social costs are difficult to quantify and have been generally neglected in estimations. For example, while losses resulting from looting and arson can be identified and assigned dollar values, the secondary or ripple effects often cannot be enumerated. These secondary effects, such as a potential increase in insurance rates, represent long-term and far-reaching economic implications.[6]

Hypothetical Outage Cost Estimates

Numerous analyses have estimated the costs of unserved electricity for various consumer sectors. Most of these are based on survey data from particular utility service areas. They vary substantially among classes of customers and among customers within each class.

Table 4 shows some estimates of the costs of power outages. The more recent estimates, based on survey data, reflect the value of service reliability in terms of the average dollar change in a consumer's monthly bill that would offset a change in service reliability. These estimates cannot be compared directly because of differing methodologies, as-

[4]Frank J. Alessio, Peter Lewin, and Steve G. Parsons, "The Layman's Guide to the Value of Service Reliability to Consurners," in Criterion, Inc., *The Value of Service Reliability to Consumers* (Palo Alto, CA: Electric Power Research Institute, EPRI-EA-4494, May 1986).

[5]Ibid.

[6]Arun P. Sanghvi, ''Economic Costa of Electricity Supply Interruptions: U.S. and Foreign Experience, "in Criterion, Inc., op. cit., footnote4, p. 8-45.

sumptions, economic and demographic mixes, and other conditions.

In general, the consensus among utility analysts is that system outage costs can be valued at something between $1 and $5 per kilowatt-hour (kWh) for the types of outages commonly experienced. However, they vary considerably by type of customer, the condition of the outage, the length of the outage, etc.[7]

Actual Outage Cost Estimates

***The* costs** of the 1977 New York City blackout have been studied more extensively than other outages. (Box C provides a description of the sequence of events that led to the blackout.)

Table 5 summarizes the estimated costs of the blackout. Based on these figures, the direct cost of unserved energy was $0.66/kWh and the indirect cost was $3.45/kWh. For the most part, the costs in table 5 are based on secondary data sources provided by numerous public and private organizations. Significant impacts include losses in securities and banking, restoration costs, and capital equipment for Con Ed,[8] and losses to the small business community. Levels of inconvenience appear to have been substantial. These figures should be considered as lower bounds for the total costs.[9]

Damages from looting and arson totaled around $155 million, or about 50 percent of the total economic costs associated with the blackout. The social impacts were sensitive to the unique circumstances of the event and the socioeconomic conditions, including weather, time-of-day, duration, local income distribution and employment, political climate, and availability of contingency plans.[10]

Economic impacts of the 4-day 1988 Seattle blackout were very sensitive to its timing and duration. For restaurants and stores, the timing of the blackout was particularly bad, covering a regular downtown event—the First Thursday Gallery Walk-and the beginning of the Labor Day weekend. Department and clothing stores also missed out on last-minute school shopping. The Bon Marché ` department store estimated its unrecoverable losses at about $500,000. Restaurants in the area estimated lost business at $10,000 to $45,000 for the 4 days. The costs at one hotel included lost revenues from the 75 percent of reserved guests who went to other

Table 4—Comparison of Cost Estimates for Power Outagesl

Date	Geographic scope	Estimated cost
1971	New York State	$2.17 million/hr[a]
1971	New York City	$2.5 million/hr[a]
1971	United States	$0.60/kWh[b]
1973	New York State	$0.33/kWh[c]
1976	United States	$1Ikwhd
1976	United States	$2.68/kWh (industrial) $7.21/ kwh (commercial)
1977	Canada	$15/kW (15-minute outage) $91/kW (1 -hour outage)
1978	New York City	$4.1 Ilkwh
1983 [2]. . . .	PG&E service area	$14.87 to reduce outages to a minimum[e] -$26.41 to tolerate 1,400 hours additional outages
1983 [3]. . . .	PG&E service area	$6.72/kWh (one 1-hr outage, summer afternoon)[f] $2,126/kWh (eight 48-hr outages, summerafternoon)
1986 [4]. . . .	PG&E service area	$1.35/outage/year (momentary)[g] $39/outage/year (12 hrs, winter morning)
1986 [5]. . . .	PG&E service area	$2.93/kWh (4hrs, winter morning, 3.15 kWh unserved)[h] $14.61/kWh (1 hr, winter evening. 0.75 kwh unserved)

[a]Based on wages paid.
[b]Based on GNP/kWh ratio.
[c]Based on GRP/kWh ratio.
[d]Based on cost-benefit analysis.
presidential, based on market research data.
[f]Commercial, based on survey data. Reflects total direct cost range of $3.51 *5to$1,112,092.*
[g]Residential, based on customer survey data.
presidential, based on contingent valuation data.

SOURCES:
1 Unless otherwise noted, the material in this table is from William T. Miles, Jane Corwin, and Peter D. Blair, "Cost of Power Outages-The 1977 New York City Blackout," paper presented at the IEEE 1979 Annual Meeting, Seattle, WA, May 14-17, 1979, and sources cited therein.
2 Andrew A. Goett, Daniel L. McFadden, and Chi-Keung Woo, "Estimating Household Value of Electrical Service Reliability With Market Research Data." The *Energy Journal*, vol. 9, 1988, p. 105.
3 Chi-Keung Woo and Kenneth Train, "The Cost Of Electric Power Interruptions to Commercial Firms," *The Energy Journal, vol.* 9, 1988, p. 161.
4 Michael J. Deane, Raymond S. Hartman, and Chi-Keung Woo, "Household Preference for Interruptible Rate Options and the Revealed Value of Service Reliability," *The Energy Journal, vol.* 9, 1988, p. 121.
5 Michael J. Deane, Raymond S. Hartman, and Chi-Keung Woo, "Households' Perceived Value of Service Reliability: An Analysis of Contingent Valuation Data," *The Energy Journal, vol. 9, 1988,* p. 135.

[7]Rene H. Males, "Reface: Value of Reliability, the Undefined Issues, " in Criterion, Inc., op. cit., footnote 4, p. viii.

[8]In addition to operating revenue losses of $5.7 million reflecting approximately 84,000 MWh of unserved energy, Con ~'S steps to upgrade system reliability will probably cost more than $65 million.

[9]Miles et al., op. cit., footnote 1, p. 66.

[10]Ibid.

Box C—New York City Blackout

On July 13, 1977, at approximately 9:41 p.m., New York City plunged into total darkness. The blackout was caused by a series of lightning strokes compounded by improperly operating protective devices, **inadequate presentation** of data to system dispatcher, and communication difficulties. These combined factors created conditions that cascaded to the point of total collapse of the Consolidated Edison (Con Ed) system.[1]

On this day, Con Ed was providing approximately 5,860 MW of electricity to its New York City customers over 345- and 138-kV transmission lines and cables. Approximately half of the electricity was being generated by plants located in Brooklyn, Manhattan, Queens, and Staten Island; the remaining load was supplied by Con Ed generators outside the city, and purchased from utilities in upper New York State and Canada. Con Ed also was wheeling 240 MW to the Long Island Lighting Co. (LILCO) and approximately 200 MW of emergency power to the Pennsylvania-Jersey-Maryland Pool.

At 8:37 p.m. lightning hit two 345-kV lines supplying 1,200 MW of electricity from the Indian Point No. 3 and the Bowline and Roseton generating units to the City. The resulting short circuit caused the protective relays, located at the Millwood West and Buchanan South substations, to open the circuit breakers and disconnect the lines. This interrupted the supply (870 MW) from Indian Point No. 3, which then shut down automatically. Isolating the generator at Indian Point No. 3 caused one of the 345-kV transmission lines between Pleasant Valley and Millwood West to increase load above its normal capacity rating (825 MW), although it remained within its long-term emergency rating (860 MW). This caused operators to reduce voltage by 8 percent. The Con Ed system operator requested all generators within the city to increase power production to replace the loss and relieve loading on the 345-kV line. However, by 8:55 p.m. the in-city generation had increased (550 MW) only enough to compensate for the two-thirds of the power lost.

Nineteen minutes later, another bolt of lightning hit with a devastating effect. This bolt hit one of the remaining large, heavily loaded 345-kV lines bringing power to the city. Normally, the strike should have caused relays to temporarily isolate the line for mere moments-just long enough to dissipate the lightning's energy. However, one circuit breaker failed to operate properly, causing other relays to isolate the line entirely. This loss of transmission capacity overloaded remaining lines, resulting in their isolation.

With the now inadequate supply of power, Con Ed had no choice but to shed load, blacking out parts of Westchester County. Simultaneously, LILCO's spinning reserves automatically increased output. However, the cables connecting LILCO and Con Ed were overloaded as a result, and LILCO disconnected itself from Con Ed, eliminating a further source of power.

At 9:27 p.m., still another lightning bolt struck a power line. When this happened, the remaining Con Ed generators could not maintain the load and were shut off automatically. At the same time, Public Service Electric & Gas Co. disconnected from the Con Ed system severing Con Ed's remaining ties to the north. At approximately 9:41 p.m. the 1977 New York City blackout began.

Full power was restored in about 25 hours. Many protective circuit breakers had to be individually examined and reset. The city was powered up one section at a time, carefully balancing the added loads with supply, as described in chapter 5.

[1]Systems Control, Inc., *Impact Assessment of the 1977 New York City Blackout,* prepared for the U.S. Department of Energy, July 1978, p. 13.

hotels, plus expenses for hiring additional security guards.[11]

One industry that profited from the Seattle blackout had electrical generators for rent. One company received 50 to 60 phone calls for 2 generators; another only had 3 available.[12]

Another actual cost analysis was based on a utility-imposed 25 percent curtailment during peak hours for 25 consecutive days in Key West, Florida in July-August 1978. The Key West system experienced a generating equipment breakdown that reduced electric supply to 80 to 90 percent of peak demand. Total electric shortage impact costs in Key

[11]Addy Hatch, "Businesses Assessing Losses From the Blackout," *The Seattle Times,* vol.111, No. 215, sec. C, p. 4, Sept. 7, 1988.

[12]Ibid.

Table 5-Cost of the New York City Blackout—1977[a]

Impact areas	Direct ($M)		Indirect ($M)	
Businesses	Food spoilage	$1.0	Small businesses	$155.4
	Wages lost	5.0	Emergency aid	
	Securities industry	15.0	(private sector)	5.0
	Banking industry	13.0		
Government			Federal Assistance	
(Non-public services)			Programs	11.5
			New York State	
			Assistance Program	1.0
Consolidated Edison	Restoration costs	10.0	New capital equipment	
	Overtime payments	2.0	(program and installation)	65.0
Insurance[b]			Federal crime insurance	3.5
			Fire insurance	19.5
			Private property insurance	10.5
Public Health Services			Public hospitals-	
			overtime, emergency	
			room charges	1.5
Other public services	Metropolitan Transportation		MTA vandalism	0.2
	Authority (MTA) revenue:		MTA new capital	
	Losses	2.6	equipment required	11.0
	MTA overtime and		Red Cross	0.01
	unearned wages	6.5	Fire Department	
			overtime and damaged	
			equipment	0.5
			Police Department	
			overtime	4.4
			State Courts	
			overtime	0.5
			Prosecution and	
			correction	1.1
Westchester County	Food spoilage	0.25[c]		
	Public services:			
	equipment damage,			
	overtime payments	0.19		
Totals		$55.54		$290.16

[a]Based on aggregate data collected as of May 1,1978.
[b]Overlap with business losses might occur sines some are recovered by insurance.
[c]Looting was included in this estimate but reported to be minimal.

NOTE: These data are derivative, and are neither comprehensive nor definitive

SOURCE: Systems Control, Inc., *Impact Assessment of the 1977 New York City Blackout*, prepared for the U.S. Department of Energy, July 1978, p. 3

West were $2.30 kWh average for all non-residential users. The breakdown is $2.00 to producers (e.g., auto repair, stores, schools), $0.10 to employees (wage loss), and $0.20 to consumers. The cost is approximately 50 times the then $0.05/kWh price of electric power in Key West.[13]

In addition, several empirical studies on user loss from power shortages were conducted. These studies examined two electric power shortages of several hours in San Diego, the Key West curtailment, and natural gas shortages in Alabama, Kentucky, Ohio, and Tennessee. The findings concluded that the extra cost to make up interrupted production comprised 60 percent of the loss to both commercial and industrial users. Unrecovered costs totaled 20 and 30 percent for commercial and industrial users, respectively. The inconvenience from postponing appliance use comprised 36 percent of the cost to residential users.[14]

SECTORAL IMPACTS

Industrial

Many industrial processes are highly sensitive to power disruptions. An interruption of less than 1 second can shut plant equipment down for several hours. Outages can spoil raw materials, work-in-

[13]Jack Faucett Associates, *Analytical Framework for Evaluating Energy and Capacity Shortages* (Palo Alto, CA: Electric Power Research Institute, EPRI-EA-1215, April 1980), vol. 2, pp. 1,5-1.7.

[14]Ernest Mosback, "Shortage Costs: Results of Empirical Studies, " in Criterion, Inc., op. cit., footnote 4, pp. 3-3, 3-11.

progress, and finished goods. Spoilage is a significant problem in chemical processes, steel manufacture, food products, and other industries.[15] Blackouts also pose opportunity costs from idle factors of production. Human health and safety effects are another major concern in industrial outages. Not only are the workers exposed to possible injury or health hazard from the power interruption, the neighboring population also could be exposed to risk from hazardous spills or releases due to the loss of environmental or safety equipment.[16]

costs

Industrial-sector costs are more directly measurable in terms of equipment damage, loss of materials, cost of idle resources, and human health and safety effects. Lost output is the primary cost. One approach is to take the classic economic factors of production—land, labor, capital, profit, and entrepreneurship-and identify the value of the foregone opportunities for each of them for various industrial processes. Those opportunities can be evaluated using some measure of excess capacity of each of the factors of production. When all resources are idle (have excess capacity), the opportunity cost is estimated at the value of wages. When all resources are fully employed, the loss includes the value that would have been added in production. One may need to add the costs of spoilage and other damage, long-term adaptive costs, indirect costs, and consumer surplus if final demand is left unserved.

For example, in 1965 Dunlop Tire's Buffalo plant lost 1,700 tires (worth $50,000) when power failed during the critical curing process. The Tonawanda, New York Chevrolet plant had to junk 350 engine blocks because high-speed drills froze while boring piston holes. Ford's huge Mahwah, New Jersey assembly plant had to wait for standby power when Orange & Rockland Utilities, Inc. gave West Point priority because "the cadets need to study tonight. ' '17

Commercial

For many commercial customers, any outage of **a** duration of more than 1 or 2 seconds has a significant cost due to computer problems, equipment jamming, or ruined product. For these firms a l-hour outage is not substantially more costly than a 10-second outage.

With the increasing pervasiveness of computers and communications systems in all economic activity-commercial sales, offices, industrial process control, finance, communications, public works control, government-their performance in a blackout affects all impact sectors. The major consequences include costs associated with the inability of the computer to perform critical functions, loss of data, and possible damage to the computer and peripheral equipment. Degradation of storage media is a major concern if the room temperature strays too far from the norm.[18] Critical systems usually have backup power sources, although most are not designed for an extended blackout, when the operating environment becomes more of a concern.

An entirely new industry has grownup around the need for backup systems and recovery services for heavily computer-dependent activities. Computer security companies take over computer functions, such as payroll, inventory, and records maintenance, when disasters tempera.riiy or permanently disable corporate computers.[19]

costs

The commercial sector is the most difficult of the three sectors to analyze and has been studied the least. Its boundaries and components are ill-defined, and it incorporates a very wide variety of products and services. In many areas, the commercial sector is the most rapidly growing customer class, and the costs of outages may average the highest.[20]

Some utilities define the commercial sector as what is left over after accounting for residential and large industrial customers. Using this definition, large apartment buildings, small grocers, and moder-

[15] M. Munasinghe and A. Sanghvi, "Reliability of Electricity Supply, Outage Costs and Value of Service: An Overview," *The Energy Journal,* vol. 9, 1988.

[16] Mosbaek, op, cit., fOOtnote 14.

[17] ''The Disaster That Wasn't,'' *Time,* Nov. 19, 1965, p. 36.

[18] Systems Control, Inc., "Impact Assessment of the 1977 New York City Blackout' prepared for the U.S. Department of Energy, July 1978, p. 46.

[19] Tyson Greer, "Weyerhaeuser Division Waits for Data Disasters," *Puget Sound Business Journal,* vol. 9, No. 21, sec. 2, p. 5A, Oct. 3, 1988.

[20] Sanghvi, op. cit., footnote 6, p. *-26.

ate-sized manufacturing firms would all fall in the commercial class. Another classification is based on SIC (Standards of Industrial Classification) codes. Still others are based on peak demand levels, a kWh rule, or the voltage of service.[21]

For those parts of the commercial sector where the principal activity is production that can be made up after an outage without substantial cost (e.g., laundries, drycleaners, bakeries, etc.), the idle resource cost approach used in the industrial sector probably is most appropriate. At the other extreme, large apartment buildings can be viewed as a concentration of households, and analyzed using one of the residential-sector outage cost methods.[22]

Between these two extremes are commercial establishments that sell products and those that provide services. The potential for product damage and the ability to makeup lost production are critical here. Food stores and warehouses, for example, can have significant spoilage costs. Similarly, fast-food outlets not only can have high spoilage costs, but also service immediate demand and usually cannot make up lost business.[23]

Agriculture

An Ontario Hydro survey conducted between 1976 and 1979 indicates there can be significant hazards to livestock and produce during a blackout. Sensitive processes include incubation, milking, pumping, heating, air-conditioning, and refrigeration. Of the larger-than-average farms included in the survey, 26 percent had standby generation. About 60 percent had facilities to shut off a portion of their load in an emergency.[24] In 1965, farmers deprived of power for their milking machines hooked them up to generators operated by tractor motors.[25]

Residential

Never are Americans more aware of their dependence on electricity and the machines it drives than during a blackout. Without electricity, air-conditioning is off, and many people do not have heat or hot water. In high-rise buildings, people must use stairwells. Senior citizens and the disabled are at an extreme disadvantage in outages. Consumers do not have lights, refrigerators and freezers, stoves and microwave ovens, toasters, dishwashers, intercoms, televisions, clocks, home computers, elevators and escalators, doorbells, hair dryers, heated blankets, can openers, food processors, carving knives, toothbrushes, razors, and garage door openers. With the advent of high-tech electronics, most people have battery-operated radios or TVs, but few keep enough batteries on hand **to** last more than a few hours.

If a blackout occurs during the winter, as did the 1965 outage, those with yards or balconies **can** put food outside. In the 1989 summer blackout in Washington, DC, PEPCO distributed dry ice. For those with fireplaces or barbecues, cooking is still possible; others must resort to cold food or restaurants. Illness from food spoilage can be **a** significant problem.

One of the more sociologically interesting impacts of the 1965 outage was the fact **that** without access to their normal forms of entertainment, people turned to each other; 9 months after the blackout, the birthrate increased from 50 to 200 percent at New York hospitals.[26]

costs

Electricity permits activities whose value varies with time of day, week, or year. The short-term opportunity **cost is the** degree of disruption of the household's preferred consumption pattern. Some activities, such **as** cleaning, can be deferred without significant loss (and in many **cases** might be considered an emotional benefit). Others can be deferred or relocated (e.g., washing clothes, eating dinner). Still others can only be relocated (e.g., watching **a** particular TV program). At some times of the day/year and/or for particular groups, there can be health and safety implications (e.g., lack of heat/AC, elevators, life-support systems, hot water, and refrigeration). Costs also vary by household income, type of appliance stock, preferred leisure activities, and other household characteristics.

---

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Len Skott, "Ontario Hydro Surveys on Power System Reliability: Summary of Customer Viewpoints," in Criterion, Inc., op. cit., footnote 4.

[25] "The Disaster That Wasn't," op. cit., footnote 17.

[26] "Blackout Fallout," *Time,* Aug. 19, 1966, p. 40.

In addition to deferring or relocating activities, households may experience out-of-pocket expenses for mitigating responses such as using block or dry ice to preserve food, firewood for heat or cooking, candles and batteries for lighting, batteries for radio/television, etc.[27]

Two equivalent measures of loss are the dollar amount the household would accept as compensation for the disrupted consumption pattern, and the amount the household would be willing to pay not to have its preferred consumption pattern disrupted.

Transportation

A blackout affects virtually every mode of transportation (box D). Subways, elevators, and escalators stop running, and corridor and stairwell **lights** usually are out. Street traffic becomes snarled without traffic lights. Gasoline pumps do not work, and the availability of taxis and buses declines over time. Parking lot gates and toll booths will not operate. Pedestrians are perhaps the least affected, although their danger increases without traffic signals and after dark with the loss of street lighting. Trains can still function, but doing so can prove hazardous without signal lights. Airports are powered by auxiliary generators that enable aircraft to land and take off in an emergency. However, considerable delays can be expected. In high-density areas where most people are dependent on public transportation, economic and other impacts are increased by the inability to get to work. Other transportation effects result from the inability to deliver goods.

Telecommunications

There is a growing reliance on telecommunications networks in all sectors of the U.S. economy. Businesses and government depend on reliable communications to perform routine tasks. Also, businesses are using their communications systems and the information stored in them to achieve a competitive advantage and to restructure their organizations on a regional or global basis. Thus, the failure of a communications system can lead not only to market losses but also to the failure of the business itself.[28]

The functioning of all crucial municipal public services, such as police, fire, etc., will also depend on telecommunications. A recent study by the National Research Council noted that our public communications networks are becoming increasingly vulnerable to widespread damage from natural disasters or malicious attacks.[29]

Extended power outages can affect telecommunications networks and lead to economic disruption. The extent of the disruption will depend on whether telecommunications networks, both public and private, have emergency backup power systems and how reliable the backup systems are. Today, many networks have their own dedicated emergency backup system. The importance of backup power systems was evidenced during Hurricane Hugo and the recent San Francisco earthquake. At the height of Hurricane Hugo, 39 central offices and 450 digital loop carrier facilities were operating on backup power. Southern Bell indicated that the facilities could operate on battery power for about 8 to 10 hours before gas or diesel generators take over.[30] With the commercial power turned off in San Francisco because of the risk of free, central offices operated on diesel generators. These diesel generators could operate for up to 7 days, according to PacBell. The earthquake did little damage to the network.[31]

In an emergency, commercial satellites could also be used to augment or restore a public network. Currently, only the American Telephone & Telegraph Co.'s interexchange carrier network is augmented by the Commercial Satellite Interconnectivity program, which uses surviving C-band commercial satellite resources.[32]

The impact of a disruption will depend on how crucial communications equipment is to a particular

---

[27]Sanghvi, op. cit., footnote 6.

[28]U.S. Congress, Office of Technology Assessment, *Critical Connections: Communication for the Future*, OTA-CIT-407 (Washington, DC: U.S. Government Printing Office, January 1990).

[29]National Research Council, *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness* (Washington, DC: National Academy Press, 1989).

[30]*Telephony*, "Survival of the Network," Oct. 23, 1989, p. 42, and "Hugo No Match for So. Bell," Sept. 25, 1989, p. 3.

[31]"PacBell Network Survives Quake," *Telephony*, Oct. 23, 1989, p. 14.

[32]Ibid., p. 18.

Box D—Transportation Impacts—Northeast and New York City Blackouts

The 1965 Northeast blackout occurred at 5:30 p.m.—a peak period for most modes of transportation-and lasted for up to 13 hours. The worst potential hazard was in the air, where at peak hours between 5:00 and 9:00 p.m. some 200 planes from all over the world were headed to New York's Kennedy Airport. Logan Airport in Boston, as well as numerous smaller airports, also were blacked out. Inbound flights lost visual contact as the ground lights went out. Luckily, it was a clear night, and pilots could seethe other planes over the darkened cities. Planes bound for New York were diverted as close as Newark and as far as Cleveland and Bermuda. Philadelphia received 40 NY-bound airliners carrying some 4,500 passengers. Kennedy was shut down for 12 hours.[1]

In 1965,630 subway trains in transit ground to a halt, trapping 800,000 passengers. Under the East River, 350 passengers had to slog to safety through mud, water, and rats. In the middle of the Williamsburg Bridge, 1,700 passengers were suspended in two trains swaying in the wind. It took police 5 hours to help everyone across a precarious 1 l-inch wide catwalk running 35 feet from the tracks to the bridge's roadway. A total of 2,000 trapped passengers preferred to wait it out, including 60 who spent 14 hours in a stalled train under the East River.[2]

Thousands of people were trapped in stalled elevators. In at least three skyscrapers, rescue workers had to break through walls to get to elevator shafts and release 75 passengers. Elevator failure resulted in the only two deaths attributable to the 1965 blackout: one person fell down a flight of stairs and hit his head, and another died of a heart attack after climbing 10 flights of stairs.[3]

Traffic lights failed and main arteries snarled. At unlighted intersections, countless volunteers took over the job of directing traffic. Hundreds of drivers ran out of gas as they waited for traffic to clear, only to find that service station pumps cannot work without electricity.[4]

In 1977, the New York airports were ordered closed at 9:57 p.m. on July 13, only minutes after the power failure. At Kennedy, 108 airline operations were scheduled between 9:00 p.m. and midnight July 13; 37 operated before the airport was closed. LaGuardia had scheduled a shutdown at midnight July 13 for runway construction, and disruption was much less significant (39 of 60 scheduled operations). Newark Airport handled 32 diverted aircraft from Kennedy and LaGuardia. Auxiliary generators supplied emergency power to the terminals, in which more than 15,000 passengers remained through the night. At Kennedy International Airport, some power returned at 3:30 a.m. on July 14, but the first authorized takeoff was not until 5:34 a.m. At both Kennedy and LaGuardia, parking lot gates and payment systems were out, and parking area employees computed fees manually. This resulted in severe traffic jams and long delays.[5]

The subway system fared a little better in 1977. The blackout occurred around 9:40 p.m., after most commuters were home. Also, the storm activity and brownouts offered some warning. Dispatchers running the subway system noticed power surges on the line before the blackout and radioed motormen to go to the nearest station and remain there.[6] Thus, only seven trains in the entire system were in transit when the power went off. Emergency evacuation problems were most severe for a train stuck on the Manhattan Bridge. Even buses could not run the next day, however, because of the unavailability of fuel from electric pumps. Moreover, Grand Central Terminal was forced to close when drainage pumps lost power. Even after power was restored, flooded converters prevented electrically powered trains from using the station during the morning rush-hour on July 15, thus delaying about 75,000 daily commuters.[7]

The train stations in New York City halted operations during the 1977 blackout. The main inter-urban train line, AMTRAK, stopped service from the south in Newark. Going north, AMTRAK provided buses to New Haven, where trains from Boston turned around. Conrail trains serving Trenton, New Brunswick, and South Amboy experienced delays up to several hours.[8]

After the 1977 blackout, the Metropolitan Transportation Authority initiated an$11 million program to install new equipment to ensure against massive disruption of the transit system in the event of a future blackout.[9]

---

1 "The Disaster That Wasn't," *Time, Nov.* 19, 1965, p. 36.
2 Ibid.
3 Ibid.
4 Ibid.
5 Systems Control, Inc., *Impact Assessment of the 1977 New York City Blackout,* prepared for DOE, July 1978, pp. 16, 89-$@.
6 Alan McGowan, "The New York Blackout," *Environment, vol.* 19, No. 6, August/September 1977, p. 48.
7 Systems Control, Inc., op. cit., footnote 5.
8 Ibid.
9 Ibid.

industry/business. Medium- and large-size businesses that use integrated information systems to link operational processes—i.e., order entry, scheduling, etc.—will experience economic damage shortly after a power failure. While many business use a number of interconnected networks, supplied by a variety of sources (including local area networks and private and public networks), most private networks depend on public networks for transmission and switching capabilities. The Federal Government, for example, uses a number of private networks to communicate within a particular department or agency, but uses public networks to communicate outside.[33]

OTA has found that, in general, businesses have been slow to prepare for emergencies or adopt security measures, often postponing action until after a problem has occurred. One major reason cited is cost. Moreover, the value of communication security has to be traded off not only against cost, but also against system access and interoperability .[34]

Emergency Services

Emergency services include police and fire and their communications and transport, as well as hospitals. Power outages can also affect these services. All hospitals have emergency power systems to support the most critical activities, such as operating rooms, intensive-care units, emergency services, etc. Depending on the facility, auxiliary power systems may not be able to support some other activities, including x-ray, air-conditioning, refrigeration, elevators, etc. Moreover, technical problems may arise with the auxiliary generators, as evidenced in the 1977 New York blackout. In some instances, hospitals had difficulty bringing generators on-line, and were faced with generators overheating and inoperable transfer switches for connecting loads to emergency circuits.

Fire-fighting and police communications could be severely disrupted by the loss of power. Fire alarm systems may be inoperable and fire-fighting maybe hampered in those areas where some power is required for pumping water.

Moreover, the indirect impacts of a blackout, such as looting and arson, can severely strain fire-fighting and police services. For example, during the New York City blackout, 70,680 calls were made to911, compared with the 17,700 made in a normal 24-hour period. Also, during the 1977 blackout, there were 1,037 fires (primarily arson) with over 6 large-scale frees, requiring 5 companies. More than 80 injuries were reported due to the abnormal fire activity. Exhaustion was common due to the high heat and humidity and the lack of food supplies and rest areas.[35]

Public Utilities and Services

Public utilities include electric, water, gas, sewage, garbage, and related services (e.g., public health inspection).

Water supply systems generally rely on gravity to move water from reservoirs through the mains and to maintain pressure throughout the system. Some power may be required at pumping stations and reservoirs. Loss of pressure in mains hampers free-fighting and hospitals, and may permit contaminants to seep into the water supply. Typical system pressure will supply buildings up to five or six stories tall. High-rise buildings use electric pumps to provide adequate supply on upper stories, or have roof tanks with 24- to 48-hour storage capacity. If electric pumps in high-rise buildings do not work, residents would have to go without water or get it from neighbors below.[36]

Electricity is needed in treatment and pumping of sewage. An outage at a treatment plant causes raw sewage to bypass the treatment process and flow into the waterways. Lack of pumping station power prevents sewage flow and ultimately causes a backup at the lowest points of input (usually basements in low-lying areas). During the 1977 New York City blackout, many of the sewage treatment plants and pumping stations in Westchester County and New York City had standby power supplies, but only for short durations. After the standby power was exhausted, untreated sewage flowed continu-

[33] **Ibid., pp. 82-84.**

[34] Office of Technology **Assessment, op. cit., footnote 28,** ch. 10.

[35] Systems Control, Inc., **op. cit.,** footnote 18.

[36] Ibid.

ously into the harbors. Signs were posted on all neighboring beaches prohibiting use.[37]

costs

Outage costs attributable to essential services and infrastructure, including street and traffic lights, public transport, telecommunications, hospitals, airports, sewage and sanitation, fire and police protection, etc., are difficult to measure. For many of the essential functions, backup emergency generation already exists, although it maybe unreliable or only designed to be operated for a few hours at a time. For some infrastructure services, the cost of installing standby generation should provide a reasonable order-of-magnitude estimate of outage costs. However, the costs of public transportation and lighting outages are more difficult to estimate.[38]

In a blackout, electric utilities have revenue losses from unserved energy, expenses for equipment and overtime personnel to restore power, plus any capital investments needed to ensure that particular type of blackout does not occur again.[39]

Consolidated Edison suffered more than bad press in 1977. In addition to operating revenue losses from 84,000 MWh of unserved energy, and the cost of restoring power, Con Ed had to make capital and other investments (e.g., operator training programs) to upgrade system reliability .40 Moreover, Con Ed stock experienced increased trading on July 14, and closed at its lowest value for some time. The stock had a closing loss of 1.25 at the end of a week that had begun with increasing values.[41]

Following the 1965 blackout, utilities across the country changed their operating procedures and made capital investments in relays and circuit breakers to ensure that no single failure would again result in a cascading outage. (See ch. 4.)

[37]Ibid.
[38]Sanghvi, op. cit., footnote 6.
[39]"The Diaster That Wasn't," op. cit., footnote 17.
[40]Miles et al., op. cit., footnote 1.
[41]Systems Control, Inc., op. cit., footnote 18.

Chapter 4

System Impact of the Loss of Major Components

A sophisticated saboteur or major natural disaster can readily cause widespread power outages. The time and effort needed for a system to recover could range from seconds to months, depending on which components are damaged, the system's basic characteristics, and the availability of spare parts. Even if a power failure is avoided or lasts only seconds, costs may be high as less efficient reserve generating capacity replaces low cost units, and sensitive consumer equipment such as computers are disabled. This chapter addresses the resilience of current bulk power systems to equipment outages, examining both reliability and economic impacts.

U.S. utilities have been highly successful in maintaining very high levels of bulk power system[1] reliability. Bulk power systems in the United States are designed and operated to be reliable and economical in the face of normal events including occasional equipment failure. Utilities are also prepared to minimize the impact of some highly unlikely events such as multiple simultaneous equipment failures at a single site. However, sabotage or major natural disaster can inflict damage well beyond what utilities plan for. Because U.S. utilities have performed so reliably and have only rarely faced widespread and multiple equipment failures, there is uncertainty about how bulk systems will actually behave in extreme circumstances.

One factor leading to reliability and resilience is the highly interconnected network common to modern power systems (see box E). Because of the vast size of most power systems, no individual powerplant or transmission component is critical to the operation of any power system. An electric system typically has many powerplants, in some cases several dozen. An individual powerplant, even a large multi-unit one, supplies only a small fraction of the total demand of most control areas. There are some very small control areas in the Midwest, but each powerplant provides only a small fraction of the total capacity in the interconnection.

Distribution systems are not designed to have such a high level of reliability as the bulk system. In fact, the great majority of outages that customers experience result from distribution system problems, not from the bulk system (around 80 percent by one estimate).[2] However, unlike bulk system failures, distribution-caused outages are localized, and utilities have considerable experience in responding to them.

SHORT-TERM BULK POWER SYSTEM IMPACTS

The Importance of Any One Component: Preparing for Normal Failure[3]

Some of the thousands of components in any system occasionally fail or operate improperly, or are disabled by natural events such as lightning strikes. Because these events are common and inevitable, utilities consider them to be normal. Most bulk power systems in the United States are designed and operated to continue operation following the failure of any one device without interrupting customer service or overloading other equipment.[4] This is commonly referred to as the "n-1 operating criterion. Some utilities prepare for two such contingencies (called the n-2 operating criterion). Systems west of the Rockies make some exceptions to the n-1 criterion for certain major facilities. In those systems, some customers may be briefly interrupted following certain outages, but with no overloading of other equipment leading to uncontrolled or cascading outages.

Preparing for equipment failure involves two main functions. These are: 1) holding sufficient generation and transmission capacity in reserve to

[1]Bulk power systems include the generation and transmission, but not distribution (see U.S. Congress, Office of Technology Assessment, *Electric Power Wheeling and Dealing*, OZ4-E-41O (Washington, DC: U.S. Government Printing Office, May 1989), ch 4). This chapter focuses on bulk systems since damage to them may be far more widespread and difficult to repair than distribution damage.

[2]U.S. Department of Energy, "The National Electric Reliability Study: Executive Summary," DOE/EP-0003, April 1981, as cited in: *Power System Reliability Evaluation,* Institute of Electrical and Electronics Engineers, 1982, p. 42.

[3]See Office of Technology Assessment, op. cit., footnote 1.

[4]North American Electric Reliability Council, *Overview of Planning and Reliability Criteria of the Regional Reliability Councils of NERC* (Princeton, NJ: April 1988).

[5]See Office of Technology Assessment, op. cit., footnote 1.

Box E—The Organization of Electric Systems: Utilities, Control Areas, Power Pools, and Interconnections

The electric power industry today is a diverse and heterogeneous amalgamation of investor and publicly owned utilities, government agencies, cogenerators, and independent power producers.[2] In most of the country, individual utilities are highly interconnected and operate under a variety of formal or informal coordination agreements. The level of power transfers and coordination between utilities is determined largely by control areas, power pooling arrangements, and physical interconnections.

Control Areas

Responsibility for the operation of the Nation's generating facilities and transmission networks is divided among more than 140 ''control areas. In an operational sense, control areas are the smallest units of the interconnected power system. A control area can consist of a single utility, or two or more utilities tied together by contractual arrangements. The key characteristic is that all generating utilities within the control area operate and control their combined resources to meet their loads as if they were one system. Control areas coordinate transmission transactions among electric power systems through neighboring control areas. Control areas maintain frequent communications about operating conditions, incremental costs, and transmission line loadings.

Power Pools

There are two types of power pool arrangements-tight power pools, which include holding company power pools; and loose power pools. Tight power pools are highly interconnected, centrally dispatched, and have established arrangements for joint planning on a single-system basis. Four of these tight pools consist of utility holding companies with operations in more than one State; the others are mostly multi-utility pools. Together, the tight power pools account for about a quarter of the industry's total generating capacity. Arrangements among utilities in loose power pools are quite varied and range from generalized agreements that coordinate generation and transmission planning to accommodate overall needs to more structured arrangements for interchanges, shared reserve capacity, and transmission services.

Interconnections

North America's interconnected utilities create four physically separate, synchronously operated transmission networks: the Eastern Interconnection (or Seven Council Interconnection); the Texas Interconnection; the Western Systems Coordinating Council (WSCC); and the Hydro Quebec System. DC and AC transmission interties between the networks are limited in location and capacity, with the result that the transmission systems in the United States do not forma single national grid, but rather form three huge, separate grids. However, even the smallest one, the Texas Interconnection, is very large with installed generating capacity of over 50,000 MW comprised of scores of generating units.

---

[1] See U.S. Congress, Office of Technology Assessment, *Electric Power Wheeling and Dealing*, OTA-E-410 (Washington, DC: U.S. Government Printing Office, May 1989, ch. 4.

[2] At present, the Nation's utility industry includes 203 investor-owned operating companies; 1,988 local publicly owned systems; 994 rural electric cooperatives; 59 public joint-action agencies, and 6 Federal power agencies, In addition, there are several hundred cogeneration and small power producers selling power to utilities.

respond immediately; and 2) designing circuit breakers and relays to protect and isolate equipment in a controlled manner.

Reserve Generation and Transmission

Utilities keep enough generation, transmission and substation capacity on-line and ready for operation to replace any operating components that fail. Generating units must be warmed up and rotating in synchronism with the 60 Hz of the power system before operating. Generating units which are synchronized and ready to serve additional demand immediately are called spinning reserves. Utilities select "unit commitment plans" specifying which units will be warmed up and cooled down to follow the cycle of loads over the course of a day, week or season. Unit commitment schedules are chosen which minimize the total expected costs of operation and Spinning reserves required to maintain reliability and meet expected changes in demand.

Unlike generating units, transmission circuits and substations don't require any warm-up time and are instantly available as long as they are connected to the system. The flow of power in a transmission network is dictated by the laws of physics. One of the key laws is that power flows on all available paths

between a generator and a load. This is called parallel path flow. After a generator or transmission circuit fails, the power flow on the remaining circuits responds immediately. To ensure that resulting flows don't exceed emergency ratings, "security-constrained dispatch' techniques are used to ensure sufficient transmission reserves. Control center operators typicallyexamine a series of contingency cases to determine the most severe contingency and the resulting transmission loadings. When they find a contingency would create unacceptably high loadings, the generation dispatch is adjusted to reduce the resulting flows to acceptable levels.

Circuit Breakers and Relay System Design

Relaying techniques and circuit breakers to isolate and protect equipment are essential to maintaining reliable service. Circuit breakers are installed at each end of every circuit and transformer in the system to provide protection in the event of a short circuit. Under normal conditions the breakers perform routine switching operations such as disconnecting and isolating equipment for maintenance or inspection, transferring loads among circuits and disconnecting generators when not needed. When relays sense a short circuit, they cause the circuit breakers to operate, isolating the faulted component. Most breakers on the bulk power system operate in no more than five cycles (1/12 second in the U.S. 60-Hz system), and three cycle (1/20 second) operation is common. Prompt isolation of faulted components is critical to ensuring that the remaining equipment is not damaged and is able to continue operation.

Increasingly, many power systems are using elaborate relaying schemes for protection.[6] These involve coordinated operation of multiple circuit breakers simultaneously in different locations rather than merely isolating individual failed components. For example, in the Pacific Intertie, which connects the Pacific Northwest with southern California, a complex scheme is employed which isolates generation in Oregon and transmission circuits in Arizona when certain circuits in California fail. This system, which enables California to reliably import large amounts of power, ensures that a transmission failure in California will not cause damaging imbalances in neighboring States.

Impacts of Multiple Failures: Islands and Cascading Outages

While the failure of any single generating unit, transmission line or substation normally should not cause significant outages, simultaneous failure of more than one major component generally will result in interruption of service.[7] When abnormal, multiple failures occur, a power system typically undergoes ''system separation, " in which portions of the system disconnect from each other.[8] Some of these isolated portions, called "electrical islands," may have an imbalance of supply and loads. Those islands have either more generation than load or more load than generation, causing the system frequency to deviate from its normal value of 60 Hz and transmission voltages to exceed design limits. In turn, protective relays would cause several generators and transmission circuits to disconnect from the island, resulting in a blackout. Other islands may have a balance of supply and demand, allowing continued operation even though disconnected from the rest of the system.

"Cascading outages" occur when the failure of one or more components causes the overloading and failure of other equipment and breakup of the system into islands in an uncontrolled fashion. It is not possible to accurately predict the way a system will break up after a major disturbance-there are too many variable factors.[9] Utilities do analyze their systems and implement plans to help anticipate and control the likely pattern of islands. Their analyses show that the pattern of islands will vary depending on the location of loads, which units are operating, how much each unit is generating, the configuration of the transmission network, and the specific second-by-second sequence of events causing the disturbance. However, one can predict that cascad-

---

[6]North American Electric Reliability Council, *1987 Reliability Assessment—The Future of Bulk Electric System Reliability in North America, 1987-1996* (Princeton NJ: October 1987).

[7]This assumes that the system is operated for n-l contingencies. A system operated for n-2 should be expected to have significant impacts only when more than two major components fail.

[8]Westinghouse Electric Corp., *Utility Survey of Methods for Minimizing the Number and Severity of System Separations,* EPRI EL-3437 (Palo Alto, CA: Electric Power Research Institute, March 1984).

[9]Ibid.

ing failures will extend over large areas, in some cases over a multistate region.

Preparing for Extreme Contingencies

Because uncontrolled, cascading outages can be so widespread and difficult to recover from, U.S. utilities have made special provisions to avoid them even though the circumstances leading to them are viewed as highly unlikely. In addition to planning for 'normal" contingencies, U.S. utilities also plan for 'extreme' contingencies.[10] The reliability criteria of each of the NERC regional reliability councils specify that bulk power systems shall be planned and operated in a reamer to avoid uncontrolled, area-wide interruptions under certain extreme contingencies. Under extreme contingencies, substantial outages will occur, but should not extend across an entire system.

Typical extreme contingencies examined include the loss of an entire multi-unit generating station, multi-circuit transmission substation, or loss of all circuits on a common right-of-way. Thus, the failure of all units in a large multiple-unit plant would cause serious, although perhaps temporary, blackouts in most systems. While customer interruptions would be expected in the immediate area, cascading failures resulting from overloading of remaining equipment should not occur if the extreme contingency planning has been performed properly.

The types of equipment failure that a terrorist attack or major natural disaster may cause are far more severe than those considered by utilities as extreme contingencies. The extreme contingencies planned for by utilities today are limited to failures at a single site. However, natural disaster or attack could well affect two or more major sites. The simultaneous failure of any combination of two or more large multi-unit powerplants, or multi-circuit transmission corridors or substations may well lead to cascading failures. While the extent of the impact (e.g., the characteristics of the electrical islands) can't be accurately predicted, it can be very large.

LONG-TERM BULK SYSTEM IMPACTS

The Importance of Any Few Components: Large Reserves and Peak Capacity

Most of the time, U.S. utilities have large amounts of generating capacity in excess of demand. Anything less than the failure of much of this generation reserve should cause outages lasting no longer than the few hours required to start idle capacity and restart the system. However, there may be a daily cycle of shortages or rotating outages during hours of peak demand. The large surplus of generating capacity over demand results from two factors: 1) installing sufficient capacity to meet peak loads; and 2) planned reserve margins in excess of peak demand.

Power systems are designed to meet widely fluctuating loads which reach their peak for only a few hours in any year. Peaks usually occur in the late afternoons of hot summer days when air-conditioners add to normal loads, or on very cold winter days when space heating is uncommonly high. Because capacity is installed to meet the peak demand, a large amount of capacity operates at partial output or is idle except during those peak periods. Off-peak-period loads may be as little as one-third of daily peak. On average, demand throughout a year is around 60 percent of peak demand.[11] Thus, on average, the power plants in a system operate at no more than around 60 percent of capacity.

Furthermore, even at peak periods, there is generally a large amount of reserve generating capacity. Most utilities plan to install generation reserve margins of 15 to 20 percent.[12] Utilities install reserve capacity in order to accommodate both planned and unplanned needs such as scheduled maintenance, unexpectedly high load growth and equipment outages. Because loads grew much slower than anticipated during much of the 1970s and 1980s, many areas of the country now have far higher reserves than planned, too, with over 35 percent in some NERC regional reliability councils.

[10] North American Electric Reliability Council, *Overview of Planning and Reliability Criteria of the Regional Reliability Councils of NERC* (Princeton, NJ: April 1988).

[11] U.S. Department of Energy, *Electric Power Supply and Demand for the Contiguous* United States *1988-1997*, DOE/IIE-0013, January 1989, tables C1-C9.

[12] U.S. Congress, Library of Congress, Congressional Research Service "Do We Really Need All Those Electric Plants?" August 1982.

As loads continue to grow, however, this excess capacity gradually is being reduced. Other regions of the country, on the other hand, are beginning to experience relatively small reserve margins.[13]

Transmission systems are planned to accommodate both the geographical distribution of powerplants as well as the changing patterns of loads. Thus, the reserves of generation are necessarily accompanied by similar reserves of transmission. Transmission networks also link the many utilities in the Nation's three interconnections (see box E). NERC reports that some transmission systems are heavily loaded by economy energy transfers both within and among regions, and will continue to be during the 1988-97 forecast period. These transfers are driven by fuel price differentials rather than reliability requirements. For example, the Pacific Intertie carries low-cost hydroelectricity from the Pacific Northwest to displace expensive natural gas-or oil-fired generation in California. However, on some occasions, large, long-distance transmission lines carry power which is essential for reliability, not just for minimizing electricity costs.

Because there generally are large reserves of transmission just as there are of generation, it would take the destruction of the transmission capacity associated with several powerplants to keep any system down for an extended period of time over a wide area. However, at certain times such as extreme peak periods or when scheduled maintenance or unplanned outages have reduced actual reserve margins, failure of only a few key generation or transmission components units could significantly disrupt service.

System Impact When No Outages Occur: Higher Costs and Lower Reliability

Even if a blackout is brief or avoided altogether, the loss of damaged or destroyed base-load generating units is very expensive for the duration of the outage. Base-load units, fueled by uranium, coal, or hydropower, have the lowest operating costs of any units in a power system and are typically the largest units. If they are damaged, the energy they would have produced must be replaced by other more expensive units such as inefficient peaking units using natural gas or oil. In the case of a large nuclear unit replaced by natural gas-fired turbines, the additional cost can be well over one-half million dollars daily .14

The lost use of the transmission capacity necessary to deliver the power from a generating unit to consumers is similarly costly. The capacity to transfer power while remaining within voltage and load flow limits on the system is a constraint on economic dispatch. When sufficient transmission is not available to deliver power from the lowest cost generators to loads, other generators must be operated instead.

Any loss of generation and transmission capacity reduces the reliability of a system somewhat. The destruction of one or more major generating or transmission components reduces a system's reserves, leading to fewer options and less resilience for any further component outages. The degree to which reliability is reduced depends on the level of installed reserve margins.

BULK SYSTEM RECOVERY FROM OUTAGES

There has been little experience with the types of widespread, carefully planned and executed acts of aggression addressed in this report. However, the utility industry has a long history of responding to various kinds of emergencies, whether they are relatively small, such as an outage of a transmission circuit or a generator unit, or more serious, due to tornado damage, hurricanes or earthquakes. Most utilities have some plans in place for restoring service after a total shutdown. However, few have had to test those plans recently—in the 1980s, Florida, Texas, South Carolina, and California provide the notable examples.

Restoring service involves starting generation or reclosing circuit breakers and adding load in small increments, slowly piecing the system back together. For customers in small islands adjacent to an area that remains interconnected, power may be restored in a few minutes. Isolated islands will take

[13] U.S. Department Of Energy, *Electric Power Supply and Demand for the* Contiguous *United States* 19&1997, DOE/IIE-0013, January 1989, tables C1-C9.

[14] This estimate is based on a 1,000-MW unit outage and the average operating costs of nuclear units and gas turbines reported in U.S. Department of Energy, *Historical Plant Cost and Annual Production Expenses for Selected Electric Plants 1987,* DOE/EIA-0455(87) (Washington, DC: U.S. Government Printing Office, May 1989), figure 1. The costs are, respectively, 2.1 and 4.7 cents/kWh.

longer, especially those that were completely blacked out.

Restarting Generating Capacity

If an external source of power is available, restarting a unit is not a problem. However, if no external power sources can be used, the powerplant must have "black start" capability. Black start capability can be provided from a diesel or a self-starting gas turbine unit in the plant. It is also possible to provide black start capability from the interconnections of a system. This is done by disconnecting the interconnections from the load-serving circuits (to avoid overloading the lines) while keeping the generator connected. The interconnections can then be energized to import power from the neighboring system to use in starting the unit.

Restoring Transmission

As generating units are restarted, portions of the transmission system can be energized. The segments energized must be carefully selected to avoid building up excessive voltages due to the capacitive effects of the high-voltage lines. This requires that load be added as line segments are energized. Care must be exercised not to overload the small amount of generation connected.

A power system is restored by successively restarting generators, connecting transmission lines, and connecting load until significant islands of operating load and capacity are available. Then the separate portions of the system are connected to each other. In this way, the portions of the system that are operable can be completely restored and returned to as near normal operation as feasible. Restoration of an outage should begin within minutes of an outage. The length of time to restore full service depends on the design of the system, the severity of the blackout, and the components damaged.

SPECIFIC EXAMPLES OF ATTACKS

To evaluate the impact of sabotage on electric power systems, postulated attacks were developed and reviewed for their effect on six areas in the United States. The impact of these attacks is described below, beginning with the simplest attacks that are most applicable nationwide. Most of the attacks involve transmission circuits (whether at substations or along transmission lines).

The components attacked could be identified by someone generally familiar with power systems, either using published transmission maps or from direct observation. Physically locating the targets would involve modest effort and planning, since they are generally large and highly visible. Anyone familiar with power systems could readily identify the particular transmission facilities that need to be attacked for effective disruption. However, it is possible for unsophisticated saboteurs to mistakenly target small or relatively unimportant facilities.

These cases assume that the attack occurs at a load level of about 80 percent of annual peak load. It is also assumed that about 20 percent of the total generating capacity is undergoing maintenance or forced outage. In all of the cases, the extent of the initial interruption would not be affected by the time of day or load level. That is because the amount of reserves which are warmed up and ready to operate is sufficient to handle only one (or in some cases two) contingencies, as is standard utility practice. The near- and long-term impacts would be lessened, however, if the attacks occurred during the spring or fall when system loads are lower. In most cases, rolling blackouts would be necessary only during certain hours, e.g., between 10 a.m. and 6 p.m. on weekdays, when loads are typically their highest.

Destruction of Any One Generator, Transmission Circuit, or Transformer

As has been noted above, U.S. power systems are operated to withstand the loss of any single piece of equipment without interrupting customer load. Therefore, the destruction of any one of these would not cause a blackout. The loss of any of these may signtificantly increase a utility's operating costs, if it made replacement of low-cost baseload generators with high-cost peaking units necessary.

Destruction of One Major Multi-Circuit Transmission Substation or Multi-Unit Powerplant

As noted above, U.S. utilities generally plan for the loss of an entire multi-circuit transmission corridor, substation, or multi-unit powerplant. For such a loss, the system should not experience cascading outages. However, customer interruptions should be expected. No case was found in which

such an attack would seriously disrupt the bulk power system or affect more than a subarea of a utility.

Immediately after the loss of a transmission substation (or of the multi-circuit corridor supplying it), the customers served directly and some others would be interrupted. Some more distant customers might be affected by the operation of protective relays as a result of power transients. The more distant customers interrupted would be restored in several minutes as the operators reconnected the circuit breakers and adjusted generation output. Customers in the immediate **area** of the failed substation would experience a longer power outage, lasting on the order of one day. Customers served by a distribution circuit powered directly from a destroyed substation might not return **to service** for several days or even weeks.

If a powerplant **was taken out** of service (whether by attacking the generating **units** themselves, the generation substation, or the transmission circuits leading from it to the network), the impacts would be less severe. While the outages could cover large areas, service should be restored in several minutes as operators reconnected the circuit breakers and adjusted generation output. Costs of replacement power could be high, particularly if the plant was a large, low-cost baseload unit replaced by inefficient peaking units.

Destruction of Two or Three Major Transmission Substations

Inmost cases, the nearly simultaneous destruction of two or three transmission substations would cause a serious blackout of a region or utility, although of short duration where there is an approximate balance of load and supply in the isolated areas. It is almost certain that the transmission system would have too little capacity to continue operation after the second loss, resulting in separation of the system and the interruption of customer load in several areas. Most customers would be restored within 30 minutes, after undamaged interconnections were restored. For most systems, there would be a sufficient balance of generation and load to restore all customers as soon as generation could be warmed up and brought on-line.

There are some areas of the country where failure of key substations could cause long-term disruptions. Two particularly vulnerable cities would be isolated by the loss of two or three substations, because of a serious shortage of generation. Rolling blackouts during high-load times (e.g., daytime) would occur for several weeks until temporary repairs were made.

Destruction of Four or More Major Transmission Substations

The destruction of more than three transmission substations would cause long-term blackouts in many areas of the country. Only a few areas have a good enough geographic balance of load and generation to survive this very severe test. For example, one city is served by a ring of nine evenly spaced transmission substations. Nearly all the interconnections serving this major metropolitan area would be destroyed by attacking the seven largest and easiest to identify transmission substations. The other two are smaller and of little importance during normal conditions. There is enough local generation in this case to restore service to most customers quickly, although it is considerably more expensive than the imported power. This case represents the best case of a multiple-substation attack.

A final example is a city served by eight transmission substations spread along a 250-mile line and located in five States. A knowledgeable saboteur would be needed to identify and find the eight transmission substations. A highly organized attack would also be required. However, the damage would be enormous, blacking out a four-State region, with severe degradation of both reliability and economy for months.

Chapter 5

Current Efforts To Reduce Energy Systems Vulnerability

Since the late 1970s national emergency preparedness initiatives have focused primarily on developing programs within appropriate government agencies. The National Security Council (NSC) has played a central role in directing this effort. About 20 Federal departments/agencies are involved with emergency preparedness. The Department of Energy (DOE), through its Office of Energy Emergencies, is the lead agency for energy-related issues. Other involved agencies include the Departments of Defense, Interior, and State, the Federal Bureau of Investigation, the Federal Emergency Management Agency, and the Nuclear Regulatory Commission.

In the early 1980s, the General Accounting Office criticized Federal Government agencies for inadequate energy emergency preparedness planning and coordination. Since then, improvements have been made in developing comprehensive plans and programs, streamlining coordination, and eliminating duplication. However, because of the number of Federal agencies involved in energy emergency planning, uncertainties about authority, responsibilities, and activities are bound to exist. These same uncertainties may be magnified during a national emergency and thus hamper efforts to ensure adequate energy supplies and distribution to essential facilities.

The Federal Government has limited authority or responsibility to provide physical protection for energy systems. Individual utilities are responsible for protecting their physical plants and ensuring reliability. Utilities routinely build redundancy and plan for inevitable but occasional equipment failure but do not consider multi-site sabotage when designing the system. That is not to say that utilities are not concerned about energy systems vulnerability. The North American Electric Reliability Council (NERC) has been working quietly on vulnerability issues for several years. Recently, NERC developed recommendations and guidelines to mitigate electric power systems vulnerability. Utilities generally follow NERC guidelines on such matters. NERC often acts as a clearinghouse for the electric utility industry-developing and disseminating resource materials and information on vulnerability. It also has encouraged member utilities to establish liaisons with government agencies and other industry groups. To a large extent, NERC facilitates communication and coordination among its members-an activity that would be essential during an emergency situation.

State efforts in energy emergency preparedness peaked in the early 1980s in response to the oil disruptions of the 1970s. Funding and staffing levels have since declined. This decrease in funding and staffing could affect the States' ability to respond to an energy emergency. In addition, most of the States' plans and organizational structure were developed in response to a particular crisis-an oil supply disruption-and may not be relevant to other situations. Plans need to be revised to reflect other potential disruptions, including natural disasters and sabotage.

Furthermore, interstate and intergovernmental communication and coordination may be inadequate. According to DOE, only 9 States have developed routine communication systems with surrounding States. Based on an energy emergency simulation, a Federal interagency group concluded that existing Federal and State crisis management plans were not well-coordinated and may beat cross purposes.[1]

This chapter provides an overview of current efforts and responsibilities of various institutions, including the utility industry, Federal agencies, States, and public utility commissions. Also, the current status of the U.S. electrical equipment manufacturing industry is discussed.

CURRENT EFFORTS

Private Industry

Utilities

In the United States the physical protection of electric power facilities does not appear to be a high-priority item for utility management. Historically, deliberate attacks on electric power facilities have not resulted in power or financial losses significant enough to justify a major investment in

[1] *Report of the Interagency Group on Energy Vulnerability, November 1986-November* 1988, prepared for the Senior Interagency Group for National Security Emergency Preparedness, January 1989.

physical security. However, it is important to note that the utility industry is concerned about vulnerability and has been working quietly on security issues for some time.

Utilities recognize that communication is an important part of any security plan. Under emergency conditions, including sabotage, the ability to communicate is even more critical. Thus, utilities place a high priority on the restoration of communication networks during emergencies.

Utilities also recognize the need for improved communication with law enforcement officials and other utilities. Virtually all utilities with key facilities have established contact with the local FBI office. The FBI can assist utilities in evaluating threats, inspecting facilities, and planning emergency responses. In addition, utilities have encouraged additional information exchanges between operating personnel and security managers to ensure adequate emergency preparedness.

North American Electric Reliability Council (NERC)

NERC and its nine regional councils were established in the late 1960s to assist utilities in providing for the reliability and adequacy of electric generation, transmission, and distribution systems. Formation of the organizations was aided by Federal legislation following the Northeast blackout of 1965.

At NSC's direction, DOE requested NERC to address electric power systems vulnerability issues. In 1987, NERC established the National Electric Security Committee (NESC) to assess the degree of vulnerability of U.S. electric power systems and develop a program to mitigate vulnerability to sabotage and terrorism. The Security Committee established three working groups which dealt with physical security enhancements, operating strategies, and design and restoration improvements. In July 1988, the NESC presented its report and recommendations to the NERC Board of Trustees. The report with its recommendations was approved in October 1988. Most of the recommendations have been implemented while a few are still under review.

NERC's program includes a close-working relationship with the Federal Bureau of Investigation. Also, NERC has identilfied utilities where spare transformers are located.

A small number of agencies have been briefed on the NERC report and recommendations. These agencies include the National Security Council, the Department of Energy, the President's Science Adviser, and the Federal Emergency Management Agency.

The NESC, having completed its mission, has been disbanded and related activities assigned to NERC's Engineering and Operating Committees or to the Regional councils or the utilities.

Edison Electric Institute (EEI)

EEI has established a security committee, which consists of 70 members who are responsible for physical protection of utilities' facilities. According to EEI, more than half of the committee's members are ex-FBI agents or members of other law enforcement agencies. EEI's security committee facilitates security information exchange among its members, NERC, and government agencies.

Federal Government

National Security Council **(NSC)**

The NSC is the lead agency for national security emergency preparedness policy. In 1988, NSC defined the government's approach to emergency preparedness. It grouped government agencies by particular areas such as economics, energy, human services, law enforcement, telecommunications, and transportation. One department/agency is the lead agency within each group and is responsible for identifying responsibilities and operating procedures and coordinating activities with other groups. For example, DOE is the lead agency for the energy group. Also, NSC is the principal liaison with Congress and the Federal judiciary on national security matters.

Federal Emergency Management Agency (FEMA)

FEMA serves **as** adviser to NSC on national security emergency preparedness, which includes mobilization[2] preparedness, civil defense, technological disasters, etc. FEMA also provides guidance to other Federal agencies in developing and implementing emergency preparedness plans. More spe-

[2]Mobilization is defined as the marshalling of resources, both civil and military, to respond to and manage a national security emergency.

cifically, FEMA is responsible for developing plans for the conversion of industrial capacity and supply during a national emergency. This effort involves identifying industrial facilities that are essential to national mobilization and developing mechanisms, including standby agreements, to allocate facilities when production capacity is in short supply. During a national mobilization, FEMA would likewise be involved in coordinating and facilitating emergency supply imports. In addition, FEMA authorizes government agencies to establish National Defense Executive Reserve programs (discussed in a later section) and provides guidance in this regard.

Recently, FEMA prepared a prototype national plan for graduated mobilization response (GMR) options. This process provides a framework for mobilization planning in three incremental steps: planning and preparation, crisis management, and national emergency/war. Eight Federal departments and three agencies were considered in the process. As a result of this effort, a Defense Mobilization Order was issued in January 1990. The order defines GMR, provides policy guidance, and further establishes a system for developing and implementing mobilization actions that are responsive to a wide range of national security threats and warnings. FEMA expects that a final document, which will institutionalize the process, will be available in 1990.

Another ongoing FEMA activity is the preparation of Major Emergency Action papers. These papers are intended to provide information to decisionmakers on response options, costs and benefits, and the implementation process during a wide spectrum of emergencies.[3]

FEMA also published a Defense Mobilization Order, which provides criteria and guidance for Federal departments/agencies to develop strategies, plans, and programs for the security of essential facilities and resources. Responsibility for protecting essential facilities rests with appropriate Federal departments/agencies. FEMA monitors compliance and reports its findings to the NSC.

FEMA's disaster relief activities are the most visible. The most recent examples are FEMA's efforts to assist South Carolina, Puerto Rico, and the Virgin Islands in the wake of Hurricane Hugo and victims of the Loma Prieta earthquake.

Department of Energy (DOE)

DOE is the lead government agency for energy emergency preparedness. Its mission is to ensure that adequate energy supplies are available to support the Nation's infrastructure during a national emergency. In this regard, DOE's Office of Energy Emergencies (OEE), created in 1981 in response to Executive order 11490, is responsible for dealing with energy system vulnerability concerns.

OEE's FY89 program budget totals about $6.2 million, the bulk of which is used for staff salaries. The budget has remained essentially the same over the past 5 years. OEE consists of 71 professional and support staff.[4]

Vulnerability Program—Recently, the OEE developed a Vulnerability Program whose purpose is to reduce the risks of energy system interruption. The Program consists of four phases: Phase I included case studies to determine the nature of vulnerabilities in the electric power, petroleum, and natural gas industries. This effort included considerable input from industry, Federal, State, and local governments and is essentially completed. The results of the studies are classified. Phase II establishes an industry outreach program which provides information and solicits industry/government joint cooperation. DOE cites the NERC/DOE initiative, noted earlier, as an example of Phase II activity. According to DOE, the first phase has been completed and the second is progressing.

Phase 111 of the program includes additional case study exercises and other industry outreach efforts. DOE expects industry to respond to the concerns raised by these exercises. However, there appears to be no provision for follow-up activities under this phase. Phase IV will identify national security vulnerabilities which cannot be addressed by the respective industries. This phase may include federally funded programs to remedy energy system vulnerability concerns. Other OEE efforts have included updating the State emergency contracts directory, reviewing legislation and contingency

[3]Federal Emergency Management Agency, National Preparedness Directorate, Office of Mobilization Preparedness, Mobilization *Preparedness—An Overview*, March 1989.

[4]Edward v. Badolato, Deputy Assistant Secretary for Energy Emergencies, U.S. Department of Energy, testimony at hearings before the Senate Governmental Affairs Committee, Feb. 8, 1989, pp. 4,6.

plans, and disseminating information to States via an electronic mail system called DIALCOM. OEE has also conducted regional seminars and simulations to provide assistance to State energy planners.[5] An overview of the results of the regional seminars is given in the "State Efforts" section.

DOE has established a threat notification system to alert energy industries. Notification consists of a message describing a threat that could lead to aggressive actions. For example, notification of Iran's reaction to the reflagging of Persian Gulf vessels was sent to NERC, the American Petroleum Institute, the National Gas Association, the Interstate Natural Gas Association of American, and the National Coal Association. These organizations in turn notify their respective industry members.

Interagency Group on Energy Vulnerability/ Policy Coordinating Committee on Emergency Preparedness and Mobilization Preparedness— Because of a growing concern about international terrorism, the NSC directed DOE to establish the Interagency Group on Energy Vulnerability (IGEV). It focused on national security issues relating to the vulnerability of U.S. energy systems. The Group was charged with developing initiatives to decrease vulnerability and mitigate the impact on national security of any disruptions.[6] In late 1988, IGEV was terminated and its concerns and functions merged into a new interagency group, the Policy Coordinating Committee on Emergency Preparedness and Mobilization Preparedness, Standing Committee on Energy. Committee members include the Departments of Energy, Defense, Justice, Interior, State, Transportation, and Treasury; the Central Intelligence Agency; the Federal Bureau of Investigation; the Federal Emergency Management Agency; National Communications System; National Security Council; and the Nuclear Regulatory Commission.

National Defense Executive Reserve (NDER) Program

Authorized by Congress, the NDER is a collection of civilian executives recruited from various industries. When authorized by the President, the industry executives, called reservists, would provide information and assistance in their areas of expertise to Federal authorities. Reservists would also help coordinate industry efforts in meeting national needs. FEMA authorizes government agencies to establish NDER units and provides overall policy guidance. The Office of Energy Emergencies within DOE administers three NDER units: the Emergency Petroleum and Gas Executive Reserve, the Emergency Electric Power Executive Reserve, and the Emergency Solid Fuels Executive Reserve.

DOE indicates that these industry executives could provide invaluable assistance in assessing damage, evaluating supply capability, and coordinating repair and restoration efforts. DOE plans to have about 400 industry representatives involved in the NDER program. The reserve staff for the Electric Power unit is at 50 percent of the staffing goal and Solid Fuels is up to 80 percent, according to DOE.[7]

Since its birth in 1964, the NDER program has not been without criticism. It has been administered by several government agencies, including the Defense Electric Power Administration within the Department of the Interior, the Economic Regulatory Commission, and finally the Office of Energy Emergencies within DOE. Questions have been raised about training and recruitment, and antitrust concerns have been raised by petroleum industry officials. Consequently, the petroleum executive reserve unit has not been fully developed. Over the last few years, however, DOE has been aggressively recruiting reservists and facilitating training sessions for new reservists.

The Federal Bureau of Investigation (FBI)

The FBI is responsible for counterterrorism programs in this country. Its authority extends to dealing with terrorists attacks against energy facilities. The Bureau recently proposed a counterterrorist program that would focus on the vulnerability of the Nation's infrastructure to sabotage. The program was designed to place **70** additional agents in field offices to identify key infrastructure facilities, develop contingency response plans, disseminate information, and provide assistance to private industry. Funding for the $17 million program has not

[5]National Research Council, **Committee on State and Federal Roles in Energy Emergency Preparedness,** *State and Federal Roles in Energy Emergency Preparedness,* **prepared for the U.S. Department of Energy (Washington, DC: National Academy Press, January 1989), pp. 15-18; Badolato Testimony, op. cit., footnote 4, p. 10.**

[6]Charter of the **Interagency Group on Energy Vulnerability of the Senior Interagency Group for National Security Emergency Preparedness.**

[7]Badolato **Testimony, op. cit., footnote 4, p. 15.**

been approved. A second proposal, now under review, will use existing resources within the Bureau to develop liaisons with private industry and disseminate threat information.[8] Currently, the FBI maintains a liaison with the Department of Energy. Threat warnings are disseminated to DOE, which in turn notifies private industry.

Department of Defense (DoD)

DoD administers the Key Assets Protection Program (KAPP), whose purpose is to protect selected civilian industrial assets from sabotage during a national emergency. Selected industries are those that are deemed essential to national defense and include some industry-owned energy facilities. Key assets are not owned or controlled by DoD. The program identifies which electric power systems provide energy to vital military installations and defense manufacturing areas. In addition, critical nodes on each power system are identified in order to facilitate defense planning.

As administrator of the KAPP, the Commander in Chief, Forces Command, develops and maintains a classified Key Assets List (KAL). Facilities that are included on the list must be nominated by DoD and meet stringent criteria, which includes onsite inspections and the approval of owners. DoD also solicits nominations of infrastructure assets from other Federal department and agencies. Responsibility for ensuring the security of a facility rests with the owner/operator initially.

In the mid-1970s, the electric utility industry participated in the Defense Industrial Facilities Protection program (now KAPP). At DOE's insistence, DoD discontinued the "utility list" in 1980. The utility industry and DOE objected to DoD's need to conduct onsite physical security surveys, particularly by Defense agency personnel unfamiliar with electric power systems, and the arbitrary nature of the selection process.[9] The utility industry has not rejoined KAPP. Since then, DoD, with an initial grant from FEMA, is again attempting to identify electric ***utility critical*** nodes that support key defense facilities. Once identified, DoD will not@ owners and solicit their cooperation in improving reliability and/or security of the critical nodes. The identified nodes will not be placed on the KAL.

States

States' efforts to plan for energy emergencies vary considerably. This assessment is based on a 1988 DOE survey of State energy emergency preparedness and information collected by DOE in 1985 and 1986.[10] According to DOE, most energy emergency plans were developed under the Energy Emergency Conservation Act, which no longer exists.

DOE found that most States had established a formal authority to deal with energy emergencies and developed plans that delineate responsibilities and provide guidance. DOE noted that almost all of the plans were developed in response to the 1979 oil disruption, and only three plans have been updated since 1983. Many of the plans focus on educating the public and on conservation programs. Fewer than one-third address the social impacts of energy supply disruptions.[11]

While some authority and organizational system is in place, staffing and funding levels have decreased over the past few years. About one-third of the responding States have at most one full-time professional staff person working on energy preparedness; 58 percent have two or fewer. Most States indicated that staff are not full time. The majority of respondents noted that the decline in funding has reduced some States' response capability .12 And, in terms of intergovernmental coordination, some respondents expressed a need for more information and communication between their States and DOE.

On a regional level, energy emergency planning and preparedness varies as well. In 1988, DOE's Office of Energy Emergencies conducted four regional seminars, which included a simulation of an energy emergency. From these seminars, DOE found that energy emergency planning was just getting off the ground in the Southeastern States.[13]

---

[8]Bill McGrath, Federal Bureau of Investigation, personal communication% Dec. 11, 1989.

[9]U.S. congress, General Accounting Office, *Federal Electrical Emergency Preparedness Is Inadequate,* EMD-81-50, *May 12, 1981,* p. 19.

[10]National Research Council, op. cit., footnote 5.

[11]Ibid., p. 24.

[12]Ibid., pp. 23-24.

[13]For purposes of these seminars, the Southeastern region includes: Texas, Oklahoma, Arkansas, Louisiana, Mississippi, Alabama, Florida, Georgia, South Carolina, North Carolina, and Tennessee.

The Southern States Energy Board is a central player in this region, encouraging cooperation and coordination among State and regional energy officials. The Western States[14] had the best integrated emergency planning of all the regions, according to DOE. Emphasis is placed on interstate and regional planning, and many States conduct energy emergency exercises. Perhaps because of the danger of earthquakes, California has one of most coordinated and knowledgeable emergency planning offices in the country. California has a large staff and one member of the Energy Commission assigned to energy emergency preparedness. The State's plans are updated and tested regularly.[15] It does not appear that the inland Western States are as highly coordinated as the Pacific Coast States. The Northeast/Mid-Atlantic region[16] is the most vulnerable to energy emergencies because of its dependence on fuels produced in other regions or countries. DOE did not report on the status of emergency planning in this region. And, in the Middle West region,[17] responsibility for dealing with energy emergencies is left to the industrial sector.[18]

Public Utility Commissions

Public utility commissions normally allow utilities to recover security costs. For example, security fences and guards, and monitoring and surveillance equipment are included in the overall cost of operating a nuclear power facility. Also, spare components are typically held as an essential part of the operation and are included in the rate base. Utilities have expressed reluctance to employ additional security measures. Among the arguments they have raised is a concern that utility commissions would disallow any related expenditures. This concern is as yet untested. It is possible that utility commissions may find that no need exists for additional security against very low-probability events (e.g., concerted aggression against utility systems). If so, they would be unlikely to allow utilities to charge for such expenditures. However, if utility activities are in response to Federal emergency preparedness policy or guidelines, approval of expenditures is more likely.

STATUS OF THE U.S. ELECTRICAL EQUIPMENT MANUFACTURING INDUSTRY

The heavy electrical equipment manufacturing industry has been undergoing restructuring in recent years, resulting largely from the drastic slowdown in electric power capacity expansion and new equipment orders. Atone time, U.S. companies dominated the heavy electrical equipment manufacturing industry. Today, there are only a handful of U.S. companies. Some companies have entered into joint ventures, while others have exited the business altogether. Still others have negotiated mergers and buyouts. For example, General Electric sold its extra-high-voltage (EHV) transformer manufacturing technology to Westinghouse, which in turn formed a joint venture with ASEA Brown Boveri (ABB) in 1989.[19] Recently ABB, itself a merger of Swedish and Swiss companies, exercised its option to buy out Westinghouse. Manufacturing facilities will remain in the United States.

Currently, Westinghouse and Cooper Power Systems, a wholly owned subsidiary of Cooper Industries, are the only domestic manufacturers of very large Generation Step Up transformers (GSUs). Transformers manufactured overseas by a number of foreign companies, including Siemens of West Germany and Hitachi, are also sold here. The Westinghouse ABB facility, located in Muncie, Indiana is operating at about 50 percent capacity and has not been profitable in the last few years. However, the plant is active, with over two shifts continuing production at reduced throughput.[20] Drexel Burnham Lambert estimated that capacity utilization in the U.S. electrical equipment industry

[14] The Western region includes: Washington, Oregon, California, Nevada, New Mexico, Nevada, Arizona, Colorado, Wyoming, Montana, and Idaho.

[15] *Inside Energy/With Federal Lands*, "DOE Working With States To Improve Responses to Energy Emergencies," Oct. 30, 1989, p. 7.

[16] The Northeast/Mid-Atlantic region includes: Virginia, West Virginia, Maryland, Delaware, Pennsylvania, New Jersey, New York, Connecticut, Massachusetts, Vermont, New Hampshire, Rhode Island, and Maine.

[17] The Middle West region includes: North Dakota, South Dakota, Nebraska, Kansas, Minnesota, Iowa, Missouri, Michigan, Wisconsin, Indiana, Illinois, Ohio, and Kentucky.

[18] The Strom Thurmond Institute, *Regional* Differences, *Common Concerns—Federal-State-Industry Roles* in *Energy Emergency Preparedness*, Regional Seminars Conference Report, Summer 1988, pp. 11-14.

[19] Meeting with Westinghouse transformer plant personnel, Muncie, IN, July 27, 1989.

[20] Ibid.

ranges from 50 to 80 percent, depending on the product line.[21]

Furthermore, EHV circuit breakers are no longer manufactured by American-owned companies, although they are produced domestically. General Electric sells Hitachi-made circuit breakers and Westinghouse markets Mitsubishi-made models. Two foreign suppliers-Siemens of West Germany and ABB—manufacture circuit breakers in U.S. factories.[22]

The restructuring trends are influenced by the declining market for electrical power equipment and subsequent profitability and the presence of foreign manufacturers. The power transformer industry, for example, has significant overcapacity because of the decline in demand, according to the Department of Commerce. Moreover, nearly 40 percent of U.S. EHV transformer production capacity has been removed in the last 3 years. At the same time, foreign manufacturers' share of the U.S. power equipment market has increased to about 20 percent and is expected to continue to rise.[23] Foreign-controlled companies have been predicted to account for about 60 to 75 percent of the market for all core electrical equipment products (distribution transformers, switchgear, transmission, construction equipment, and power generation) by 1990.[24] However, it is important to note that a larger fraction of these products will be manufactured domestically. Because of the decline in the U.S. dollar, foreign companies have found serving U.S. markets very expensive and one solution to this situation is to establish facilities in the United States.[25]

In contrast, U.S. participation in foreign markets is minimal. One reason is that electrical equipment has been excluded from GATT (General Agreement on Tariffs and Trade) jurisdiction, resulting in limited U.S. access to foreign markets. This exclusion from GATT was influenced by the close relationships among utilities, electrical equipment manufacturers and the government in European countries. Most foreign utilities are State-owned or subsidized. This government stakeholder position has made penetration of some European markets difficult. According to the National Electrical Manufacturing Association (NEMA), between 1975-88, U.S. manufacturers of large power transformers and steam turbine generators did not win a single order from a European Community (EC) purchaser with a domestic production base for these products.[26]

Recently, access to foreign markets has been the subject of discussion and negotiations among the Department of Commerce, the U.S. Trade Representative, and the EC Commission, which will control trade for its members, beginning in 1992. The EC, in late 1988, issued a directive that covers procurement in three previously excluded sectors: energy, water, and transport. The directive, which is currently under review by the European Parliament and Council of Ministers, proposes that utilities competitively procure purchases above a certain EC unit value (about $170,000 - U.S.). The utilities, however, will have considerable latitude in choosing tendering and procurement procedures, and will be allowed to exclude offers that have less than a 50 percent "EC content," which will be based on contract value.[27]

According to recent testimony by NEMA, the proposed directive provides no new right of access for non-EC suppliers. American electrical equipment manufacturers will continue to face closed utility markets in most EC member states, according to NEMA. On the other hand, U.S. markets are open to foreign suppliers.[28]

Proponents for maintaining U.S. electrical equipment manufacturing capability suggest that economic-jobs for U.S. workers—and national security considerations are two of the most compelling

[21]Drexel Burnham Lambert, "Current Perspectives on the Electrical Equipment Industry," December 1987, reported in *Electrical Marketing*, "Why Foreigners Will Control U.S. Electrical Equipment Market," vol. 13, No. 3, Feb. 5, 1988, p. 8.

[22]"The Rise of International Suppliers,' *EPRI Journal*, *vol. 13, No. 8,* December 1988, p. 7.

[23]Charles H. White, National Electrical Manufacturers Association testimony at hearings before the Senate Committee on Governmental Affairs, On Vulnerability of Telecommunications and Energy Resources to Terrorism, Feb. 7 and 8, 1989, p. 65.

[24]Drexel Burnham Lambert, op. Cit., footnote 21.

[25]Ibid.

[26]Bernard H. Falk, President, National Electrical Manufacturers Association, testimony at hearings before the House Committee on Foreign Affairs, Subcommittee on Europe and the Middle East and Subcommittee on International Economic Policy and Trade, Apr. 5, 1989, p. 2.

[27]Ibid., pp. 4-5.

[28]Ibid., p. 5.

arguments. Others maintain that without an adequate number of companies in the industry, competition will erode and a sellers market will prevail. Still others believe that the transportation of foreign-made equipment will take longer to reach the United States, which may be critical in a crisis. Some question whether standard American spares would be readily available from foreign manufacturers and wonder whether foreign manufacturers will give U.S. companies priority during a crisis. NEMA argues that an adequate domestic manufacturing capacity is needed to support a surge in demand for equipment or respond to a crisis.[29]

Others see no compelling reason for maintaining U.S. capability. Foreign companies make quality electrical products and do it in a timely manner. Many feel that foreign suppliers are committed to meeting U.S. needs. One utility executive noted that the global market is already part of the business environment, and procurement policies can address spare parts availability and other issues.[30]

[29] White, op. cit., footnote 23, p. 65.

[30] "The Rise of International Suppliers," op. cit., footnote 22.

Options To Reduce Vulnerability

The preceding chapters have established that U.S. electric power systems, while capable of absorbing considerable damage without interrupting service, are vulnerable to attacks by saboteurs and, to a lesser extent, to massive natural disasters. Damage could occur that exceeds normal utility contingency planning, resulting in widespread, severe power shortages and rolling blackouts that would be extremely expensive and disruptive, and could continue for many months.

The risk that massive damage will occur is not high, but neither is it negligible. International terrorist groups appear to have the capability of mounting a crippling assault, and at some point, they or domestic extremists may see a motivation. Earthquakes and hurricanes more severe than have yet been experienced in the United States are inevitable. Eventually one will cause unprecedented damage to an electric power system, although the random nature of such disasters makes the resulting disruption very uncertain.

Various measures can be taken to reduce vulnerability disruption if damage does occur. The North American Electric Reliability Council has recognized that threats exist, and some utilities have taken action, as discussed in the previous chapter. However, such actions are voluntary on the part of individual utilities. It can be easy to ignore low-risk events, even if they are of high consequence, especially when protective measures are costly.

Given the unpredictability of these types of disruptions and the uncertainty of their costs, it is not possible for a cost/benefit analysis to determine how much protection is worthwhile. The desirability of further measures is a matter of judgment more than analysis, as is the potential role of the government in stimulating greater protection.

This chapter describes the measures that could be useful in reducing the risk. This can be done by:

1. preventing or minimizing damage to the system;
2. minimizing the consequences of any damage that does occur; and
3. assuring that recovery can be accomplished as rapidly as possible.

In addition, the evolution of the electric power system can be guided toward inherently less vulnerable technologies and patterns. Table 6 lists the specific steps.

These measures are presented independently of how they would be implemented or who would pay for them. The following chapter discusses consistent policy packages of these measures that could be undertaken depending on the judgment of the decisionmaker as to the severity of the problem. The packages address the issues of implementation.

PREVENTING DAMAGE TO THE SYSTEM

While it is not possible to protect energy facilities completely, it is possible to deter attacks and limit damage. Measures to reduce vulnerability include both physical changes or additions to electric power facilities and institutional measures. Physical changes include constructing walls or berms around critical facilities and adding monitoring devices to detect unauthorized entry. Some changes may be prohibitively expensive, while others may involve minimal expense.

The transmission network is the part of the power system of greatest concern because it is highly vulnerable to attack, and the consequences can be great. The lines themselves are essentially impossible to protect because they extend over many thousands of miles, often in sparsely populated areas. However, lines can usually be repaired quickly with equipment and materials that utilities keep on hand.

Substations are the part of the transmission system with the most serious combination of vulnerability and potential consequences. Unguarded and unprotected substations in remote areas are as vulnerable as lines, but damaged equipment could take months to replace. The loss of even one key substation could effectively isolate a substantial part of the regional generation capacity from the load centers, posing the risk of long-term power shortages.

Table 6-Options To Reduce Vulnerability

A. Preventing damage
1. Harden key substations-protect critical equipment within walls or below grade, separate key peices of equipment such as transformers, toughen the equipment itself to resist damage, etc.
2. Surveillance (remote monitoring) around key facilities (coupled with rapid-response forces).
3. Maintain guards at key substations.
4. Improve coordination with law enforcement agencies to provide threat information and coordinate responses.
B. Limiting consequences
1. Improve emergency planning and procedures for handling power flow instability after major disasters and ensure that operators are trained to implement these contingency plans.
2. Modify the physical system-improve control centers and protective devices, greater redundancy of key equipment, increased reserve margin, etc.
3. Increase spinning reserves.
C. Speeding recovery
1. Contingency planning for restoration of service, including identification of potential spares and resolution of legal uncertainties.
2. Clarify legal/institutional framework for sharing reserve equipment.
3. Stockpile critical equipment (transformers) or any specialized material (e.g., various types of copper wire) needed to manufacture this equipment.
4. Assure availability of adequate transportation for a stockpile of very heavy equipment by maintaining database or rail/barge equipment and adapting Schnabel cars to fit all transformers if necessary.
5. Monitor domestic manufacturing capability to assure adequate repair and manufacture of key equipment in times of emergency.
D. General reduction of vulnerability
1. Emphasize inherently less vulnerable technologies and designs where practical, including pole-type transmission lines, underground transmission cables, and standardized equipment.
2. Move toward an inherently less vulnerable bulk power system (e.g., smaller generators near loads) as new facilities are planned and constructed.

SOURCE: Office of Technology Assessment, 1990.

Harden Key Facilities

Most substations are enclosed with nothing more formidable than a chain-link fence. Improved fences and gates could delay an attack while guards are summoned by perimeter monitoring systems. However, no fence will delay experienced, dedicated adversaries for more than a few seconds. Hence there seems little purpose in constructing very expensive perimeter barriers unless police or armed guards are stationed at or close to the site. Moderately reinforced fences, perhaps anchored at the bottom and incorporating rolls of barbed tape, would provide some protection against opportunistic saboteurs and vandals, especially if coupled with perimeter alarms.

Protective barriers-walls or berms-could be built around the transformers to preclude damage from off-site rifle fire. Barriers might be particularly valuable in substations at generating plants. Unsophisticated saboteurs might prefer to avoid approaching generating stations too closely because they are manned and often guarded, but appropriate walls would prevent easy attack from a distance. Walls would not stop a saboteur willing to climb the fence and attack from close range, but deterring less aggressive attacks could still prevent the loss of a billion-dollar generating station. Barriers would also limit the damage that could be caused by one large bomb, forcing the saboteurs to plan a more elaborate, risky attack.

The cost of hardening a particular facility depends on the site characteristics and the type of protection required. For example, a sheet metal wall (or building) will hide equipment from view. That might help against vandals, but it would provide no protection against a saboteur with a high-power rifle who knows the equipment is inside and will simply spray the wall with many bullets. A heavier wall, perhaps made of reinforced concrete that can stop rifle fire, would be considerably more expensive. If the surrounding terrain provides high-vantage points, the wall would have to be commensurately high. While no general rule is proposed, crash-resistant fences and a concrete wall would add perhaps $100,000 to $200,000,[1] a few percent of the multimillion-dollar facility cost. Some measures, such as walls, would make installation and maintenance of equipment more difficult. These costs should be included when evaluating the desirability of adding protection.

[1]Derived from The U.S. Army Corps of Engineers, "Security Engineering W@," August 1987, and Sandia National Laboratories, "Access Delay," Sand 87-1926,1989. App. A of the ACE manual lists several vehicle barriers including ditches (about $4/foot), concrete-filled posts ($50/foot), reinforced fences (about $40/foot), etc. For example, a 4-acre site would have a fence of about 2,000 feet. Assuming a ditch on 75 percent and filled posts on the rest, the cost would be $31,000, plus a crash gate at $13,000. In addition, a fence designed to delay attackers on foot, perhaps rolls of barbed tape attached to a standard chain-link fence, would cost about $6/foot, or $12,000. Such a fence would be little deterrence to a well-equipped adversary. More formidable barriers would cost over $20/foot. An 8-inch thick concrete wall around thtransformer would cost $13.50 per square foot. A three-phase transformer might involve a three-sided wall of about 25 feet per side plus an additional 75-foot straight wall to shield the opening while allowing access in case the transformer has to be removed. The wall might be 25 feet high, for a total of 3,750 square feet which would cost about $50,000. The grand total for the example is $106,000.

Utilities in most parts of the country generally have not designed their facilities to be earthquake-resistant, except for nuclear powerplants, yet several regions besides the west coast are vulnerable. Generating stations are particularly vulnerable to earthquakes unless adequately designed and constructed. The central Mississippi valley, the southern Appalachians, and an area centered around Indiana are particularly vulnerable to major earthquakes but are much less prepared than California. Review and appropriate upgrading of existing facilities, and application of appropriate seismic standards to new construction, could avert a major loss of generating capacity.

Surveillance

Equipment can be installed at unmanned, key facilities to detect intruders. Intrusion detection systems include sensors, alarm communication systems, and possibly video equipment to assess the cause of an alarm. Perimeter alarms and motion detectors would alert utility headquarters or police/military units which could instigate rapid, armed response. A rapid response could interrupt an attack and that possibility might deter an attack by a group sophisticated enough to recognize the problem. To be of greatest value, a detection system should be coupled with some sort of physical protection of the main substation components, to reduce the possibility of off-site attack.

A wide variety of intrusion sensors have been developed, ranging from buried pressure sensors to electric field disturbance detectors to fence-motion detectors. None is perfect. All sensors have some probability of failing to detect an intrusion, depending on such specific factors as the installation conditions, weather and geographic conditions. and sensitivity of the sensors. Sensors also may trigger nuisance alarms-i.e., alarms caused by spurious factors such as animals, weather (e.g., wind or rain), background noise, or failure of the sensor itself. Intrusion detection systems may include a closed-circuit television system for remote assessment of the cause of alarms. A detection intrusion system at a substation with a 2,000-foot perimeter would cost on the order of $125,000.[2]

At remote sites surveillance would be less useful because the response would take too long. Saboteurs can cross almost any barrier, leave explosives to destroy critical substation components, and depart within a few minutes. If several teams operate simultaneously at different sites, a utility may know a major attack is in progress but be helpless to do anything about it.

Even at remote sites, however, surveillance systems still would serve two major purposes. Detecting and monitoring unauthorized entry would permit the utility to investigate and presumably discover and disarm timed explosives. Thus the potential damage that one or a few saboteurs can accomplish would be limited to only one or two sites before utilities would have guards out. In addition, some forms of surveillance, such as remote TV cameras, may provide crucial evidence for an investigation even if an attack is successful.

A related issue is employee training to recognize and respond to sabotage threats. Reporting suspicious behavior near key facilities may uncover plans for an attack. **Alternatively,** recognition that sabotage and not natural causes has led to damage may lead to the preservation of evidence.

Guards

Detection and delay will do little to stop a serious saboteur if a human response is unavailable to intervene. A heavily armed response to an actual attack is most appropriate to police or military forces (see below), but private guards can deter some attacks.

Currently, armed guards are used at all nuclear powerplants. As a matter of routine, nuclear plant licensees must develop physical security plans, which include the training and use of guards. A well-trained, armed, and dedicated onsite security force is one of the major elements of a nuclear powerplant security system. Guards are also used at non-nuclear powerplants to monitor employees and visitors and vehicle traffic and for perimeter surveillance. The training and use of guards at powerplants vary by utility. Guards generally are not used at substations.

[2]Ibid. App. A of the ACE manual lists perimeter detector costs ranging from $20/foot for fence motion detectors to $40/foot for infrared systems. For a 2,000-foot perimeter this totals $40,000 to $80,000. A basic control panel would cost around $10,000, including the control unit, power supply, and communication module. AC(7I'V system costs around $30/foot adding another $60,000 to the surveillance package. Personnel to monitor the system would add an operating cost.

The deterrent value of guards depends on their numbers, training, capabilities, and orders as well as on the capabilities and motivations of their potential adversaries and the physical characteristics of the site. Opportunistic saboteurs and vandals may be deterred by even a single, unarmed guard. Ruthless terrorists with the resources to mount a well-planned, violent attack essentially could ignore any force less than a well-trained and motivated group of armed guards. Barriers and surveillance equipment can greatly increase the effectiveness of guards.

Guards are employed in different situations for a variety of reasons: to prevent or detect intrusion, vandalism, and theft; to control people and vehicle traffic; and to enforce rules, regulations, and policies. Although, private security guards perform some functions similar to public law enforcement officers, often wear uniforms and badges, and occasionally carry weapons,[3] their legal authority differs in many significant respects from that of public officers. In general, private security guards have no more formal authority than other civilians in the United States. A private security guard has only that authority which his employer possesses: the employer's basic right to protect persons and property is transferred to the security officer.[4]

Most guards are not armed and can do little directly to halt an attack in progress. Guards are in a much better position to detect suspicious behavior and report it to management or authorities. The ability of local law enforcement to mobilize rapidly in the event of an attack would be critical. In this situation, communication among local law enforcement officials, contract security firms, and the Federal Bureau of Investigation is essential.

The typical training period for most security guards is less than 2 working days. Many guards, including some who are armed, receive less than 2 hours of training. Most guard personnel aren't cognizant of their legal powers or authority. However, this situation may be changing. Because demands on security guards and the potential for legal liability have been increasing in recent years, a growing number of companies and schools are providing security training.[5] The extent and cost of training security personnel employed at electric utility facilities vary by company and by site depending on the degree of risk aversion acceptable to management.[6]

A utility's decision to use guards at a facility would have to address a number of issues: the kind of security coverage needed and costs; the effectiveness of guards in deterring different kinds of attacks; whether to employ in-house security personnel or contract out for guard services on a temporary or permanent basis.

Because many substations are located in remote areas, a related question is how long would it take for contract guards, if not stationed at the site, to arrive after a warning has been received. The rate of deployment would depend on a number of factors, including the circumstances of the event, and the location and resources of the contract security firm.

A utility's decision to employ guards as a security measure also raises a number of institutional issues. One issue is whether the government should grant police powers to utility security personnel. Advantages include increased authority and reduced liability risk. Potential disadvantages include abuse of authority (e.g., unnecessary arrests) and the legal implications of such abuse.[7]

Another issue is who should pay for the additional security. Normally, utility commissions allow utilities to recover security costs. Before additional security measures are taken, utilities and utility commissions will have to agree on what constitutes a valid need and is in the interest of the consumer.

Coordination With Law Enforcement Agencies

Ongoing communication among utilities and Federal, State, and local law enforcement agencies, is essential to reducing vulnerability. Clear lines of communication provide two main benefits. First, they enable law enforcement agencies to warn a

[3]Joseph Arwaddy, Burns International Security Services, Inc., personal communication Jan. 23, 1990. According to Arwaddy, less than 2 percent of security work involves armed personnel.

[4]Charles Schnabolk, *Physical Security: Practices and Technology* (Woburn, MA: Butterworth Publishers, 1983), p. 55.

[5]Ibid.

[6]Arwaddy, op. cit., footnote 3.

[7]Norman D. Bates, "Special Police Powers: Pros and Cons," *Security Management,* August 1989, vol. 33, No. 8, p. 54.

utility of a potential attack, should they learn of such circumstances. Second, they allow the utility and the law enforcement agencies to coordinate armed response plans when attacks occur or seem imminent. If utilities are forewarned that an attack is likely, they can take preventive measures such as temporarily increasing spinning reserves or stationing guards at important facilities.

The North American Electric Reliability Council (NERC) has recommended that utilities establish communications with the local FBI office. Regular information exchanges with local law enforcement agencies should also be pursued. These are steps that all utilities could employ at low cost. A utility's decision to establish a liaison with the FBI is purely voluntary, although most generally implement NERC's recommendations. The Federal Government might consider requiring the FBI to maintain communications with utilities.

If an attack is detected, whether by guards or remote surveillance, very rapid, armed response may be required to prevent damage. Such responses must be planned and tested beforehand. Considerable coordination will be required to assure that the appropriate forces are available, know what is required, and will be alerted promptly. The forces could be local or State police, or, as is already being planned for facilities vital to national security, U.S. military forces. If no response forces are available in a useful time-frame (a matter of very few minutes), increased hardening and permanent armed guards are the only options for minimizing damage.

Under some conditions, it might be necessary to temporarily station armed guards, such as the National Guard, at electric power facilities. These troops could be deployed much faster and more effectively if contingency plans have been prepared and studied beforehand.

LIMITING THE CONSEQUENCES

If damage cannot be prevented, the next best thing is to ensure that impacts on customers are as low as possible. Utilities have already installed protective devices on the transmission networks such that it is unlikely that blackouts would cascade beyond the directly affected region. Other steps can be taken that would further reduce the extent of the impacts.

Improve Emergency Planning and Procedures

The behavior of a transmission system following simultaneous destruction of several key facilities cannot be predicted with complete accuracy. It depends on the circumstances on the system at the time as well as on the pattern of destruction. Considerable contingency planning under a variety of conditions is necessary to ensure that the best responses are identified. In cases where there is some warning, operators can revise the pattern of generation and transmission so that more failures can be accommodated. In addition, operators will be required to make quick judgments after damage occurs. Training in recognizing and responding to multiple, simultaneous losses, which no utility has yet experienced, will help operators control instabilities and keep as much power flowing as possible. The Pacific Gas & Electric Co. has credited its drills and planning with minimizing disruption after the 1989 Loma Prieta earthquake.

Modify the Physical System

Transmission networks are generally designed with reserve capacity to accommodate equipment failure and maintenance requirements, and allow for unpredictable developments in loads and resources. One or two equipment failures should cause no significant problems for the customers. Transmission networks could be designed to ride out virtually any conceivable attack, but that would require prohibitively expensive redundancy of equipment, including spare lines in separate corridors. However, some upgrading would limit the extent of the blackout in case of the loss of several key facilities. Analysis of the bulk power system following postulated severe damage can identify potential constraints to keeping at least some of the system operating. Some of the improvements that might prove worthwhile are upgraded control centers, greater redundancy at certain substations, more protection devices and interconnections, upgraded lines, improved communications, etc. The Electric Power Research Institute is developing highly sophisticated computer systems that could analyze and respond to abnormal fault conditions, thereby limiting disruption.

One counter trend should be noted. Loads on transmissions lines are increasing as utilities find opportunities for economic transfers of power.

Increasing competition in the electric power industry could further increase these loads.[8] Unless construction keeps pace with the increasing loads, the result will be smaller reserve margins. The greater the reserve margin, the more opportunities utilities would have to bypass damaged facilities. Thus increasing efficiency of use of the transmission system could conflict with reliability of service, especially under the kind of extraordinary conditions considered in this report.

Increase Spinning Reserves

When a major failure of generating or transmission capacity occurs, utilities must have replacement capacity available immediately. Since generators take some time to warm up before they can start delivering power, reserve capacity must be kept on-line. Usually this means several generators are operated sufficiently below full load so that any anticipated outage can be accommodated by an increase in their power level. The usual reserve is at least equivalent to the largest single unit or transmission line in operation, in accordance with customary planning for the possible loss of any one piece of equipment.

If multiple facilities are sabotaged simultaneously, the available spinning reserve is likely to be inadequate. Operators will not be able to find adequate replacements for the isolated generators, and many areas will lose power, at least until other units can be started which may require several hours. Under such conditions, increased spinning reserve levels could significantly reduce the disruption, depending on the patterns of damage and the remaining available capacity. Utilities are prepared to increase spinning reserves temporarily if they are aware of a specific threat against them such as sabotage or major storms. Maintaining higher levels routinely would protect against unexpected attacks.

If additional generating capacity is available, operating it as spinning reserve is not very expensive. The additional fuel and labor costs are modest. Some parts of the country currently have excess capacity which may be used for spinning reserves, although load growth is slowly reducing that surplus to historically normal levels. During certain periods, such as extreme peak hours or when multiple units are undergoing maintenance, surplus capacity is not available for increased spinning reserves. Increasing spinning reserves during those periods could require expensive new construction.

SPEEDING RECOVERY

Once the system has been stabilized, operators try to restore power as quickly as possible. Even after severe damage, power to parts of the system usually can be restored within a few hours by isolating the damage and resetting circuit breakers. Restoration to full service and reliability depends on at least temporary repair of the damage. The measures here are intended to eliminate constraints to both near- and long-term recovery.

The benefits of expedited restoration can be extremely large, even if no power outages occur. For example, for each day that a large coal-generating unit is idled, a utility must spend on the order of $1 million for replacement power.[9]

Contingency Planning

As in the two previous sections, advance planning and analysis is vital to minimizing problems. If utilities have already analyzed the problems, they should be able to act more efficiently. For instance, few operators have ever had to blackstart a generator or deal with an entire region of mismatched generation and transmission capacity and loads. Planning can also help with longer term problems such as where to get replacement transformers and how to get them to the site. NERC has started to inventory transformers in order to facilitate emergency borrowing. Completion of this task, such that the operators of all key facilities know where to look to borrow critical equipment, could save precious time in an emergency.

Clarify the Legal/Institutional Framework for Sharing

Utilities routinely loan equipment and crews to help restore another utility's power after an emergency, when this can be done without jeopardizing their own operations. However, utilities normally maintain spare large transformers only to the extent that they are needed to permit maintenance and

[8] U.S. Congress, Office of Technology Assessment, *Electric Power Wheeling and Dealing: Technological Considerations for Increasing Competition,* **OTA-E-409 (Washington, DC: U.S. Government Printing Office, May 1989).**

[9] See ch. 4 for a discussion of the cost of disabled units.

replace failures. If these spares are loaned, the owner is risking its own system reliability. From a national perspective, it is better to risk reliability in one area than to keep another area blacked out, but utilities cannot be expected to willingly sacrifice their own reliability for the national interest. In addition to their own economic interests, they may be concerned that they will be sued by their customers who suffer blackouts because backup equipment has been loaned out.

The Defense Production Act and other national emergency laws already permit the government to requisition equipment (with just compensation) needed in case of a threat to the national security, for instance if a key defense facility is blacked out in time of war. There is no general power to intervene in a major economic emergency that has no national security implications, but the legal situation that would pertain is complicated.[10] State governments can guarantee such transfers within their own boundaries, and utilities can make their own voluntary arrangements including indemnification. However, a national policy establishing a mechanism to determine priorities and protect economic interests may be needed to expedite action and in cases where the equipment would be shipped across jurisdictions.

Stockpile Critical Equipment

Rapid restoration of a system damaged by the loss of several large transformers requires finding and installing at least temporary replacements. Many utilities keep some spare transformers in case of equipment failure. At least one utility keeps spare Generation Step Up (GSU) transformers for each plant because of past problems with GSU reliability.[11] However, these spares are typically kept at the substation site, near the operating transformers, where a saboteur could readily destroy them along with the operating transformers. If a utility is unable to obtain spares, whether from its own system or from another utility, the only other option is to order a replacement from a manufacturer. Custom-designed units may require a year or more to manufacture.

A secure source of emergency transformers could cut many months off replacement time. Such a source could be a stockpile of the most commonly used types of transformers, available to any utility in an emergency, or it could be individual backup units for each vital substation. In either case, the units would have to be stored in a secure location, perhaps at military installations.

Backups for each substation would effectively solve the problem of long-term blackouts, but at a high price. The effectiveness of a common stockpile in reducing vulnerability depends on several factors relating to the nature of the destruction, the physical characteristics of the system, the availability of spares from other sources, and the number and type of spares in the stockpile.

The wide variety of transformers in use complicates the development of a stockpile. The major criteria are the input and output voltages and the power level. There is also a wide choice of less crucial factors such as insulation level and tolerable range of voltages.

Because voltages on transmission and distribution systems are standardized, there are only a few common and important combinations of step-down voltages. Six to eight key combinations of voltages could be identified for developing model transmission transformers. While there are many other voltage combinations and functions of transformers, those factors would not be the key consideration in an emergency.

GSU transformers present a more challenging stockpiling problem. Because generator output voltages are designed to maximize operating efficiency and not according to standardized values, voltages range from 12 to 30 kV.[12] A stockpile of GSU transformers would have to make use of the ability of generating units to produce a small range of output voltages (±5 percent of nominal), although with a slight loss of efficiency.[13] Also, ABB transformer engineers have suggested that it should be possible to design transformers to work with a variety of input voltages, in which case most 345-kV transformers could be backed up by two separate models and most 500-kV transformers by three to

[10] Robert Poling, Congressional Research Service, personal communication Feb. 12, 1990.

[11] Bernard Pasternack, American Electric Power, personal communication, October 1989.

[12] U.S. Congress, Office of Technology Assessment, op. cit., footnote 8, p. 91.

[13] D.G. Fink and H.W. Beatty (eds.), *Standard Handbook for Electrical Engineers* (New York, NY: McGraw-Hill, 1978), p. 7-34.

four common single-phase models.[14] Assuming similar numbers for 230- and 765-kV units, a stockpile of GSU transformers could be based on a total of around one dozen models. Another variable is the physical configuration. The bus from the generator carries an extremely high current so the losses can be high. Therefore, the substation and GSU are designed to minimize the distance this current has to travel, which may call for a custom-designed connector.

Power ratings, insulation levels, and impedances for both GSU and transmission transformers would have to be selected based on a trade-off of costs and expected application, and efficiencies would be suboptimal. Around 20 transformer models would cover most critical applications. However, a stockpile would almost certainly require more than one set (three single-phase or one three-phase transformer) of transformers of each model. For example, if saboteurs disabled four or more sets of transformers, it is probable that at least two of the sets would have the same voltage combinations and would be replaced by the same model. The number of units of each model would have to be selected based on an assessment of the likelihood of serious sabotage.

Stockpiling raw materials for the manufacture of transformers may be another way to reduce production time in case of an emergency. The customary practice is to design the transformers frost and then order the materials because of the customized nature of the product and costs. Copper, for example, is special-ordered for each transformer (the copper wire is rectangular, not cylindrical, with particular width and height) and takes about 10 to 16 weeks on order. Core steel, porcelain, load-tap-changers (LTCs) are similarly special-ordered. If existing designs and stockpiled materials are used, new transformers can be produced in less than 6 months (in contrast to normal procurement of over 12 months).

Additional spare transformers would be expensive. A set of extra-high-voltage transformers costs on the order of $2 to $5 million. If all important substations are to be backed by duplicate transformers, the capital cost could range up to many hundreds of millions of dollars, depending on the definition of important. Common transformers would have to be designed for use in a variety of applications, so they are unlikely to fall at the low end of the cost range. This is particularly true for the GSUs, which would require a mechanism to accommodate a range of input voltages. Assuming a stockpile of 40 transformer sets (two of each model), the capital cost would be on the order of $100 to $200 million. Building and maintaining storage facilities would add to the cost.

The suboptimal characteristics of common transformers would also result in substantial indirect costs. To match the voltage capability of a nonoptimized GSU, the generator would need to operate at other than its optimal voltage output, resulting in slightly degraded efficiency. Further, the transformer's generic characteristics could result in significant efficiency losses, for example if it is oversized for the generator and as a result operates at partial load. Assuming a combined efficiency loss of 1 percent, the cost at a 500-MW coal plant would be on the order of $2 million during the year required to obtain a custom-ordered replacement transformer. Presumably, however, this cost would be much less than the cost of not having a stockpiled transformer when it is needed.

There would also be costs associated with transporting the transformer from storage to the damaged site. Both the time required and the cost depend on the location of the stockpile and the damaged site. Also, because a common stockpiled transformer would not be perfectly matched to the specific site requirements, it would probably be replaced by a new or repaired transformer, and returned to the stockpile, doubling transport costs. Overall however, the cost of transport is a small fraction of the capital cost of a transformer.[15]

A decision to establish a stockpile would have to address issues of how many units and of what design, where to store them, under what conditions to release the equipment, and how to transport it. Priorities for the use of stockpiled equipment should more than one utility have a need may also need resolution.

Payment for the stockpile is another critical issue. Spares are typically held as an essential part of the

[14]Lex Curtis, Manager of Technical Support, Westinghouse/ABB (now ABB), personal communication, July 27, 1989.

[15]Hilton Peel, Manager of operations, Virginia Electric Power CO., personal communication% July 19, 1989.

operation of a system and are included in the rate base.[16] Currently, neither utilities nor State utility commissions have found compelling reasons to stockpile critical components beyond normal spares. To develop a stockpile paid for by utilities and their customers, both the utility and the utility commission must agree that the expenditures are a valid cost of business in the interest of consumers.

Assure Adequate Transportation Capability

Moving large transformers is difficult under any condition. Frequently, bridges have to be temporarily braced and overpasses removed. Under emergency conditions, transportation could be a serious constraint. The contingency planning discussed above should identify the transportation problems that could slow delivery of transformers to key facilities (or removal from other facilities for use as replacements). Utilities can move to eliminate as many of these problems as possible. For instance, if the rail lines that brought in the transformers have closed, alternative routes could be developed.

If transformers are stockpiled and many are required at once, transportation equipment itself may be a constraint. Large transformers are moved on specialized rail cars called Schnabel Cars. There are only 13 in the country (plus 1 in Canada), and some handle only one type of transformer or are limited in capacity. A serious stockpiling effort should be accompanied by a program to ensure that sufficient Schnabel Cars will be available. This might involve the production and stockpiling of the cars, or just the conversion of all existing cars to handle all transformers. If only single-phase transformers are stockpiled, conventional transportation equipment is probably adequate.

Monitor Domestic Manufacturing Capability

U.S. manufacturing capability of transmission equipment, particularly the large transformers, has declined and imports have risen. The use of imported equipment per se is not a problem if it is the least expensive, best quality equipment available. However, some utilities are concerned that in an emergency, they will have less leverage with foreign companies to assure expedited manufacture of critically needed transformers, and that equipment will take longer to deliver from abroad. Repair of damaged transformers also would be delayed if they had to be shipped abroad and back. At this time, it is not possible to determine what would have to be done to maintain the U.S. industry, or how great would be the value during emergencies. However, the situation would appear to warrant continued attention and analysis by the Department of Energy and the Department of Commerce. National security concerns may dictate the maintenance of some minimum capability even if it is not justified economically under normal conditions. Alternatively, the incentive for stockpiling may increase if supply from abroad can't be considered to be as expeditious.

GENERAL REDUCTION OF VULNERABILITY

The measures discussed above could be implemented specifically to reduce the vulnerability of existing bulk power systems. Other measures have not been listed because they would be far too expensive to retrofit. However, as the system grows, new construction is required that might emphasize different approaches. Vulnerability to massive destruction has never been a design parameter in electric power systems (except for nuclear powerplants). Making it a parameter could guide the evolution of future systems toward inherently less vulnerable technologies and configurations. Vulnerability is not likely to be the key factor in most cases, but it could swing an otherwise close decision.

Less *Vulnerable Technologies*

Existing equipment has not been designed to resist sabotage. It is possible that alternative transmission towers, insulators, transformers, etc., could be more resistant than current practice. The Electric Power Research Institute, equipment manufacturers, and DOE might be encouraged to study how to do this. In some cases, alternative designs may be available now that would be less vulnerable even though that was not one of the design criteria.

For example, underground cables are less noticeable and less accessible than overhead lines. Therefore they are less likely to be targets of casual saboteurs, and somewhat harder to attack for serious terrorists. They also avoid drawing attention to substations. Underground cables should also be more resistant to major natural disasters, since they

[16] Ibid.

are not exposed to wind, flying objects, or collapsing towers. However, underground cables are much more expensive to manufacture and install. Furthermore, maintenance and repair, though needed less frequently, are more difficult and expensive. If cables were destroyed, whether by saboteurs or earthquakes, replacement would take considerably longer than for overhead lines.

At present, underground cables usually are used only in heavily populated areas. In areas where land is very expensive, the narrower right-of-way needed by underground cables may more than makeup for the difference in equipment and installation cost. It is likely that there will be a growing trend toward underground cables because of increasing opposition to overhead lines, due in part to aesthetics (property values) and to increasing concern over the health effects of electric and magnetic fields associated with transmission lines.[17] Buried cables virtually eliminate electric fields and reduce magnetic fields. Reduced vulnerability could be an added incentive.

There would also be some advantages in moving toward greater standardization of key equipment, in particular the large transformers. Some of the potential benefits of standardization over the long term are increased opportunities for sharing during emergencies and some reduction in manufacturing time and cost. It would not be practical to retrofit existing facilities or change existing system voltages, but as new capacity is built, it could be guided toward a more limited family of voltages. However, some of the diversity found in our present system is a result of the diverse operating conditions that utilities face and their special needs. Each transformer carries a huge amount of power, and even a tiny loss of efficiency is very expensive. Hence standardization would impose serious additional operating costs if it sacrifices precise optimization for particular applications.

The transformers used in substations to reduce voltage from the transmission system to a distribution system are already standardized to a large extent in that there area limited number of combinations of voltages. If a stockpile were to be established (as discussed above), relatively few models would be required to backup most substations.

GSUs are less standardized than step-down transformers. They usually are designed, engineered, and manufactured to meet a utility's particular needs. It may be possible to design GSUs with multiple low-side voltage levels to fit a variety of generators, according to the National Electrical Manufacturers Association although that is not now done. These would cost more than standard transformers and probably result in less efficient generator and transformer operation.

Decentralized Generation

Until fairly recently, generating stations were growing in size and remoteness from the load centers because of economies of scale and difficulties in siting in densely populated areas. However, when large amounts of power are concentrated in a few generating and transmission facilities, the disruption that is caused by a few failures can be very large. Small generating plants are individually no less vulnerable than large plants (in fact they may be more so because fewer employees are stationed there), but the impact of their loss is less. Saboteurs would have to target more facilities to cause the same disruption. For example, destruction of electric power systems was never a major part of U.S. strategy in the Vietnam War, because most facilities were too small and scattered to be primary targets.[18] If, in addition, smaller plants can be sited close to load centers, the shorter transmission lines provide fewer opportunities for disruption.

To some degree, the trend toward larger plants has been reversed. No very large (over 1,000 MW) plants, either nuclear or coal, have been ordered for over a decade. Many co-generation plants have been constructed that are directly at a load center. Smaller plants offer benefits such as shorter construction times, better matches with uncertain load growth and greater operating flexibility. Reduced vulnerability does not appear to have been a significant factor in the choices that have been made to date.

It is not clear how far this new trend can continue. That may depend in part on how competition

[17] U.S. Congress, Office of Technology Assessment, *Biological Effects of Power Frequency Electric and Magnetic Fields—Background Paper*, OTA-BP-E-53 (Springfield, VA: National Technical Information Service, May 1989).

[18] Federal Emergency Management Agency, "Dispersed, Decentralized and Renewable Energy Sources: Alternatives to National Vulnerability and War," December 1980, p. 28.

changes the institutional structure of the industry[19] and on the relative costs of fuels (natural gas is particularly suitable for small plants). Economies of scale have not disappeared. They merely have been overwhelmed by other factors, some of which, such as high inflation and construction stretchouts, would not be expected to recur in the future.

A related issue is the use of transmission corridors and substations for multiple circuits. Utilities often try to maximize the use of corridors because it is economical to do so and increasingly difficult to establish new corridors. However, this concentration increases vulnerability. Utilities plan for common failures of adjacent facilities (e.g., a plane crashing in the corridor could bring down all the lines) but saboteurs could attack several multi-circuit corridors simultaneously with very great impact. The use of single-circuit corridors and substations, wherever practical, would reduce the impact of each attack commensurately.

Vulnerability considerations are not likely to be dominant if traditional approaches prove much more economical. However, under some conditions, it may be worthwhile to include vulnerability as a factor when siting and sizing new facilities. Further study of the relationship between decentralization, economics, and vulnerability may be warranted.

[19]For an analysis of the effects of competition, see U.S. Congress, Office of Technology Assessment, op. cit., footnote 8.

All the measures discussed in the previous chapter would reduce the vulnerability of the electric power system. Some are already being implemented by the power industry, as utilities become more aware of the potential for major disasters. However, the level of implementation of these steps could be increased, and other effective measures are available which the industry is less likely to implement on its own initiative.

Some steps, such as planning, analysis, and legal arrangements, need not cost much, but could significantly increase preparedness in case of disaster. Others, such as stockpiling, would require considerable investment. The following analysis groups the specific measures according to whether they are likely to be implemented under present trends; or if they would require small expenditures; or whether they would be moderately to quite expensive. These groups are shown in table 7. Some of the measures are shown in more than one group, representing differing levels of implementation, or analysis in one and implementation in another.

The desirability of further government involvement in a largely private enterprise is a matter of opinion. There is a clear government role in handling emergencies and protecting the public health and safety (e.g., minimum standards for nuclear reactor safety, and direct implementation of airport security). It is less clear how far the government should go in preventing emergencies that have major indirect but little direct impact on the public. If, in the judgment of policymakers, the threat is greater than is being recognized by industry, and the consequences have grave ramifications for the public, then policy action may be justified. However, it should be noted that some of the initiatives discussed here will be controversial on ideological as well as practical grounds.

PRESENT TRENDS

Utilities are moving to reduce vulnerability through improved security and planning. The National Electric Security Committee of the North American Electric Reliability Council (NERC) has made a series of recommendations intended to reduce the risk of major damage occurring and to expedite restoration of service afterwards. The Edison Electric Institute has a security committee that coordinates information for physical protection for its member utilities. In addition, there are several government programs that analyze vulnerability and address weaknesses. These activities are described in chapter 5.

Collectively, these steps are reducing vulnerability, and should lead to further improvements. However, the improvements are unlikely to be as great as could be realized if Congress takes a more activist role. Furthermore, the generating and transmission overcapacity of the last 15 years is diminishing. This overcapacity was expensive, but it had the unintended effect of providing reserves that would have been highly beneficial if a major disaster had occurred. It is likely that the increase in vulnerability due to decreasing reserve margins outweighs the improvements in security underway. The advantages and disadvantages of leaving the decisions in the industry's hands follow.

Advantages

If decisionmakers see the threat of massive destruction as quite low, the measures already underway may be adequate. The design and operation of U.S. electric power systems are quite adequate for all emergencies except the loss of several key facilities at one time. Considerable damage can be accommodated without greatly affecting customers. Only extraordinary disasters would cause more than short-term, localized blackouts. The actions utilities are taking will further reduce the range of disasters that can have devastating consequences. With the additional attention being paid to earthquakes and hurricanes, preparation for natural disasters may be sufficient to handle all but very unlikely events.

Under most plausible sabotage or natural disaster scenarios, the utilities themselves would be big losers, from lost sales and damaged equipment. Therefore they also have incentive to achieve a reasonable level of defense. Leaving the decisionmaking to the utilities on investments to protect against disasters minimizes the risk of a commitment to expensive measures that prove ineffective.

Table 7—Policy Package Components

	Present trends	Low cost	Moderate to major investment
A. Preventing damage			X
1. Harden key substations.			
2. Surveillance			X
3. Guards			X
4. Improve coordination	X		
B. Limiting consequences			
1. Improve emergency plan/ procedure	X	X	
2. Modify the physical system. .			X
3. Spinning reserves		X	X
C. Speeding recovery			
1. Contingency planning	X	X	
2. Clarify legal framework	X		
3. Stockpile critical equipment. .			X
4. Assure adequate transportation	X	X	
5. Monitor domestic manufacturing		X	
D. General reduction of vulnerability			
1. Less vulnerable technologies.		X	
2. Decentralized generation . . .	X	X	

SOURCE: Office of Technology Assessment, 1990.

Disadvantages

Terrorist attacks are largely unpredictable. The lack of such attacks in recent years is no guarantee that there won't be an upsurge in the near future. Several international situations, including the Colombian drug wars, separatism in Puerto Rico, tensions in Central America and the Middle East, and even the shifting political climate in Eastern Europe could lead to efforts to cause harm to the United States by surreptitious means. Electric power systems could be a prime target for such attacks.

Even though some utilities are taking steps for protection, it is unlikely that all will implement even minimal measures. Some managers are bound to ignore low-risk, high-consequence events until they materialize, but by then it would be too late. Some areas could suffer extensive blackouts, at great economic and social cost, that might be averted or at least minimized if the government assures that the national interest is given due consideration.

LOW-COST GOVERNMENT INITIATIVES

Most of the measures in this package are already being addressed to some extent, and were included in the preceding section. The purpose of this package is to assure that these efforts are adequate, especially those that are voluntary for utilities. In addition, initiatives with potentially important long-term implications but which would not require large expenditures of government or private funds are included. This group of options is intended for those who conclude that electric power system vulnerability is a problem that requires greater attention, but does not justify major financial commitments.

Several of the steps discussed below suggest an approximate budget level for implementation by the Department of Energy (DOE) or other agency. This study has not analyzed the effectiveness or efficiency of any of the government agencies mentioned. Therefore it intends no suggestion as to whether the activity could be absorbed within the existing budget by simply increasing efficiency, or if less important activities could be cut back, or whether the overall budget would have to be increased.

Specific Initiatives

Planning for **Emergencies**

Most utilities with vital facilities appear to have established contact with the Federal Bureau of Investigation (FBI) to facilitate warnings that sabotage efforts are likely. DOE could perform a survey to confirm this coordination (which in itself would encourage utilities to establish and maintain these contacts) and perhaps sponsor regular meetings among utilities with critical facilities and the appropriate law enforcement agencies. This activity would require perhaps $100,000 in DOE's budget for the Office of Energy Emergencies (OEE).

DOE could also play an important *role in* coordinating utility emergency plans. Many of OEE's activities have been concerned with national security issues—assuring that vital military and industrial facilities will not be crippled by power shortages during an international crisis. Less attention has been paid to the economic damage that could be inflicted on the civilian economy. For instance, the Department of Defense (DoD) has a list of transmission substations that are vital to militarily important facilities, but DOE has no equivalent list for facilities vital to major civilian load centers. OEE could expand its cooperation with NERC, individual utilities, and State and local governments to analyze a wide range of disasters. OEE could then help the utilities and local police (or other agencies) plan

emergency responses. These same exercises could include emergency planning to limit the consequences of damage and speed recovery (e.g., contingency planning for locating and transporting spares). All these activities could require OEE expenditures of several hundred thousand dollars annually, depending on how rapidly the analyses and planning exercises are to be completed and how often they would have to be updated. The Federal Emergency Management Agency (FEMA) and other government agencies should also have a role in this emergency planning.

Increased Spinning Reserves

Increasing spinning reserves beyond present levels would have to be either mandated or paid for by the government. Additional equipment would have to be kept operating, which incurs manpower, fuel, and maintenance costs. In some cases, low-cost units would have to be operated at less than full load to supply spinning reserves because other units couldn't be operated at the necessary levels. Construction of new generating equipment would also be required if the installed capacity was inadequate to support higher reserves, as is becoming true in many parts of the country. Both the costs and the value of increased reserves are uncertain. Utilities have not yet determined the cost of spinning reserve as a separate, unbundled service to be purchased under competitive generation. A DOE study, possibly done in cooperation with NERC, could be of value to determine the costs of increased spinning reserve and the value if widespread damage does occur.

Increased Sharing of Spares

Congress can consider legislation to encourage the sharing of backup equipment, which utilities would otherwise consider necessary for their own system. This legislation would establish a forum for determining priorities in a national emergency and relieve lending utilities of liability for power outages in their own territory stemming from the absence of this equipment. The purpose would be to improve the chances that spare transformers and other key equipment are available where most critically needed. The first step would be to request a legal analysis, perhaps from the Congressional Research Service, to determine the applicability of existing legislation to a situation of a major, long-term power crisis that does not have great national security implications. It also could be beneficial to have DOE analyze how to include such sharing of otherwise unavailable equipment in the emergency planning discussed above.

Assuring Adequate Equipment Supply

The future of the electric equipment supply industry is of concern to both DOE and the Department of Commerce (DOC). A joint study of both its competitiveness and its role during emergencies would establish whether there is a government interest in maintaining particular capabilities. This study would not have to be very large. DOC already has studied the competitiveness of the industry. Utilities and the supply industry, both here and abroad, should cooperate in determining how equipment would be handled during an emergency.

Analyze Vulnerability Implications of Future Growth

DOE could also consider how the long-term evolution of the industry could be guided toward reduced vulnerability. Analysis of different technologies (e.g., underground cables) and configurations (e.g., small, dispersed generation) could determine the relative vulnerability, costs, operability, etc. In addition, the study would consider how to get the industry to give low-vulnerability options proper consideration. This would be a complex, demanding study with many different lines of analysis.

Advantages

This package of options would raise the visibility among utilities of the necessity of preparing for major attacks. Advance emergency planning should improve the handling of a disaster and the recovery afterwards, at least if the disaster conforms to anticipations. Few attacks would be deterred by this package, but the impact of some could be reduced. This package would also raise the priority given to such preparation by government agencies and provide the analytical basis for further steps. These options should lead to a useful reduction in vulnerability without requiring much investment by either government or industry.

Disadvantages

There are no real disadvantages to this package. The main question is whether the modest gains justify the modest costs. It is impossible to quantify the benefits of this package relative to present trends, but they are unlikely to be major, at least in regard

to terrorist attacks. There are too many different ways in which the system can be attacked to anticipate all of them. Advance planning by utilities has obvious value, but it would still be easy to overwhelm these preparations with a large-scale attack. Even routine vandalism, including shooting at transmission lines and substations, would not be greatly deterred. The studies proposed could be useful, but unless the results are implemented, they would provide no significant benefits.

MODERATE AND MAJOR INVESTMENTS TO REDUCE RISKS

If the initiatives discussed above are seen as inadequate, the next step is to ask what could be accomplished at higher cost. There are several options outlined in the previous chapter that entail considerable cost but promise significant reduction in vulnerability, at least under some conditions. Utilities are not likely to undertake these measures on their own. The measures are intended to address low-probability, high-consequence events that utilities do not consider sufficiently probable to include in their reliability considerations. If policymakers find that national interest considerations require that these investments be made, it is likely that the government will have to at least share expenses or coerce utilities. Sharing expenses will call for significant government expenditures at a time of considerable budget difficulty. One possibility would be a kind of users fee: a small, temporary tax on power sales. For instance, a tax of 0.01 cent per kilowatt-hour (raising an 8 cent/kilowatt-hour charge to 8.01 cents) would produce almost $300 million per year while remaining virtually invisible to all but the largest users. If imposed for a year or two, this tax would pay for most of the proposals discussed here. This approach is already used by some States to fired energy studies, for example. However, the fact **that** such a tax would not be obvious does not justify it if the need for government involvement is seen as very small.

Specific Initiatives

Protect Facilities

Protecting key facilities, particularly substations, would significantly reduce the risks of long-term damage, especially from low-level threats (unsophisticated saboteurs and vandals). The problem is to determine which facilities are worth protecting, what measures to take, and how to pay for them. DOE presumably would identify the most important facilities if the analyses of the previous section are performed. Depending on the decrease in vulnerability desired (i.e., how many areas are of concern, the acceptable duration of blackouts, and the level of reliability required after a disaster) there could be as few as 30 or as many as 150 facilities that would require protection to significantly limit the long-term disruption following a multi-site attack. The exact protection measures-hardening, surveillance, guards—for each facility would depend on its importance, physical characteristics and location as well as on the nature of the anticipated threat. Both DoD and DOE have extensive experience in protection design though they may not have applied it to many substations. These agencies could expand on DoD's Key Assets Protection Program to include designs for physical protection. The utility owner should also be involved in this exercise to ensure that the physical protection and its implementation would not interfere with the operability of the facility.

The cost of physical protection such as remote surveillance equipment and walls around the transformers would be highly variable, but the one-time total might be on the order of several hundred thousand dollars for each substation. This is only a few percentage of the cost of the facility, but it is still significant. Stationing a guard during off-hours (about 130 hours per week) would entail an annual cost that might be on the order of $50,000 to $100,000. It is likely that some utilities would be reluctant to make these changes voluntarily. The benefits (e.g., reduced threat of a major blackout) considered in arriving at the level of protection specified, accrue largely to the users of the power, not to the utility. Therefore it is likely that the government would have to mandate these improvements or pay for at least part.

Make Power Systems More Resilient

The analysis that identified key facilities presumably would also suggest opportunities for modifications (e.g., upgraded control centers, improved communications) to the physical system that would help maintain reliability following major damage to the system. However, getting these modifications implemented is likely to be difficult because no appropriate policy tools exist. Utilities build their

bulk power systems according to industry standards for reliability. Other than certain licensing procedures and interstate economic regulation, the Federal Government has little direct influence on how transmission systems are built and operated. The Federal Government does not tell utilities when to build more lines, how to operate them, or how to assure reliability. Unlike upgraded physical protection, which involves decisions on relatively few key facilities, system improvements are likely to entail many small modifications. Voluntary cooperation on the part of utilities would be essential.

One way would be for DOE to establish a program to help utilities identify weak points that would hamper recovery from a widespread attack, and at least share the costs of corrective action. Utilities would be particularly uninterested in extremely expensive physical modifications, such as increased generating and transmission reserves. Utilities are concerned with building new capacity to meet growing demand, but not to increase reserve margins above the levels they find prudent. Any estimate of the level of funding that would be required is highly speculative at this time because analyses showing what would be needed have not been conducted.

Stockpile Transformers

Stockpiling of transformers beyond the spares kept for customary reliability purposes is also of little interest to utilities, though there has been at least one case of the lack of a spare keeping a low-operating cost, nuclear powerplant inoperable for a considerable period. The total cost of establishing a stockpile would be large, perhaps $100 to $200 million. Requiring utilities to backup each important transformer would cost several times as much. However, the cost of either approach would be small compared to the benefits if several substations are destroyed simultaneously. A transformer stockpile would be needed only to counter terrorist threats since natural disasters (or even casual attacks) are very unlikely to damage more than one or two substations. The likelihood of a major assault is outside the scope of this analysis. If policymakers and the industry are convinced that the threat is sufficient, a government-industry cooperative venture might be possible. In addition to establishing the stockpile, decisions must be made on where to locate it, how to maintain it, how to allocate the transformers in case of a major emergency, and how to expedite their transport. Considerable advance planning and analysis must be conducted before implementation. DOE and FEMA might cooperate with the industry on these studies.

Advantages

Collectively, these steps would greatly reduce the vulnerability of the U.S. electric system to the kinds of attacks (see ch. 2) that have been experienced in the United States. The risk of major disruption from small-scale terrorist attacks would be virtually eliminated. In addition, normal operation should be more reliable because of greater reserve margins.

Disadvantages

Several of these steps could be very expensive (e.g., greater reserve margins, stockpiling). Apportioning these costs among utilities, rate-payers, and government will be difficult unless a general kilowatt-hour tax, as discussed above, is imposed. Furthermore, power systems would still be vulnerable to sophisticated saboteurs, including sophisticated terrorist groups as well as national commandos. These measures would make destruction more difficult and perhaps reduce the damage, but they won't eliminate the greatest concerns. Furthermore, even greatly enhanced resistance to sabotage is likely to simply move the problem somewhere else. For instance, small groups deterred from attacking substations could simply shoot transmission lines out. While the impact of a single incident would be much less dramatic and lasting than that of blowing up several substations, it could be repeated frequently over a wide geographic area, achieving much of the same disruption. Alternatively, the saboteurs could turn to telecommunications, water supplies, or other infrastructure elements. Thus, it is questionable how much protection would be purchased by these options for society as a whole.