14

ELECTRICITY: PROTECTING ESSENTIAL SERVICES

Jay Apt, M. Granger Morgan, and Lester B. Lave

The record of the past 40 years shows that in the nation's system for generating, transmitting, and distributing electricity, some blackouts are inevitable. Natural hazards produce many local and regional blackouts (Table 14.1), and society has learned to cope with them. Power outages occur more frequently than theory predicts, however, and despite years of promises and technology development, the frequency of large blackouts has not decreased over time (Figure 14.1). Making cost-effective improvements in control and operation of the grid[1] is important; however, data suggest that reducing the frequency of these low-probability, high-consequence events will become increasingly expensive.[2]

The U.S. and Canada blackout on August 14, 2003, revealed that many private institutions are far ahead of the public sector in defining their critical missions and taking steps to protect them when the lights go out. During the one-day blackout, some hospitals and television stations in New York City, Toronto, Cleveland, and Detroit were able to stay open because they had backup generators. Services in other sectors, however, could not be delivered. Elevators in office buildings were stuck between floors, trains stopped between stations, traffic signals went dark, cell phones lost reception, and, in Cleveland, water ceased to flow and sewers overflowed when the electric-powered pumps stopped functioning. If the blackout had persisted for longer than a day, the

Portions of this work have appeared in the following publications: S. Talukdar, J. Apt, M. Ilic, L. Lave, and M. G. Morgan (2003). "Cascading Failures: Survival vs. Prevention." *The Electricity Journal* 16(9): 25–31. J. Apt, L. B. Lave, S. Talukdar, M. G. Morgan, and M. Ilic (2004). "Electrical Blackouts: A Systemic Problem." *Issues in Science & Technology* 20(4): 55–61. J. Apt and M. G. Morgan (2005). "Critical Electric Power Issues in Pennsylvania: Transmission, Distributed Generation, and Continuing Services when the Grid Fails," Pennsylvania Department of Environmental Protection.

Table 14.1. Blackouts affecting many customers, 1965–2004

Date	Location	Number of customers affected (millions)
November 9, 1965	Northeastern United States	30
June 5, 1967	Eastern United States	4
May 17, 1977	Miami	1
July 13, 1977	New York City	9
January 1, 1981	Idaho, Utah, Wyoming	1.5
March 27, 1982	Western United States	1
December 14, 1994	Western United States	2
August 24, 1992	Florida (Hurricane Andrew)	1
July 2, 1996	Western United States	2
August 10, 1996	Western United States	7.5
January 1998	Québec (ice storm)	2.3
February to April 1998	Auckland	1.3
December 8, 1998	San Francisco	0.5
December 26–28, 1999	France (wind storms)	3.5
August 14, 2003	Great Lakes region, New York	50
August 30, 2003	London	0.5
September 2003	Atlantic region of United States (Hurricane Isabel)	4
September 23, 2003	Denmark, Sweden	4
September 28, 2003	Italy	57
November 7, 2003	Chile	15
July 12, 2004	Athens	3
September 5, 2004	Florida (Hurricane Frances)	2.8
August 31, 2005	Gulf coast of United States (Hurricane Katrina)	2.3
September 12, 2005	Los Angeles	1
October 25, 2005	Florida (Hurricane Wilma)	3.3

Source: Data on the U.S. and Canadian outages between 1984 and 2000 are from the North American Electric Reliability Council (NERC); data on other outages are from press reports.

region's public health and welfare would have begun to suffer from the failures of more and more socially critical missions (see Appendix 14.A for the effects of blackouts on an array of critical services).

Before the next blackout strikes, whether caused by natural elements or human sabotage, private and public institutions need to decide which of their missions (of those requiring electricity) are critical, and then protect them. In this chapter, we review the vulnerabilities of many critical systems and discuss cost-effective ways to reduce their vulnerability. Throughout our discussion, we approach the challenge of reducing vulnerability from the perspective of not simply protection of the electrical grid, but protection of the social services that rely on the grid.

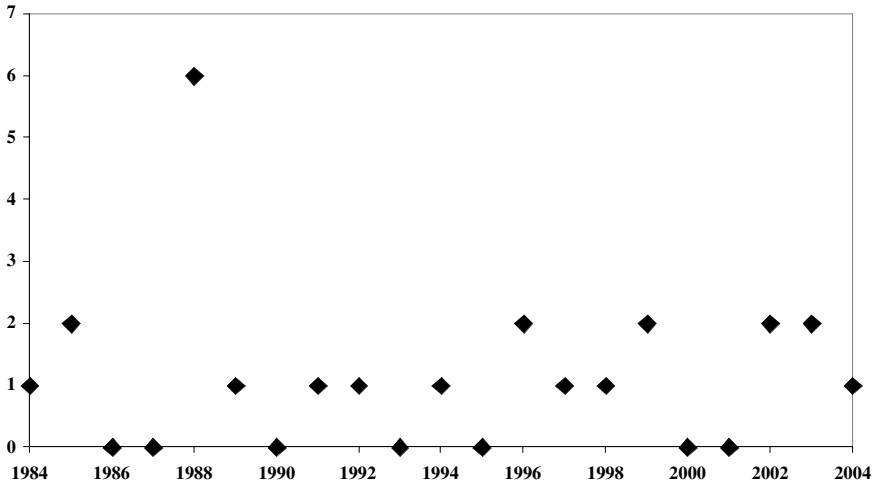

Figure 14.1. Number of blackouts in North America affecting 1 million or more customers, 1984–2004. No statistically significant trend showing improvement or worsening with time is evident in the data. Analysis is based on North American Electric Reliability Council Disturbances Analysis Working Group database and public reports.

Private institutions delivering critical services face additional challenges in that while the social benefits of keeping services running during an outage are large, these benefits are dispersed among society as a whole. The capital costs, however, are concentrated in the hands of the service providers. Therefore, there is little incentive for the private service providers to change. We discuss public policy measures that could alleviate this benefit–cost dilemma.

CRITICAL SERVICES: A CASE STUDY

To develop specific data on the fate of critical social services when the electric grid fails, the Carnegie Mellon Electricity Industry Center assigned students in a 2004 engineering project course the task of assessing the vulnerability of such services in the Pittsburgh area. Students also developed options and benefit–cost ratios for sustaining those critical services during grid power unavailability.

The case study found that while some important services in Pittsburgh, such as hospitals and the 911 emergency response system, have taken measures to ensure continued service during a blackout, several other vital services would lose power. These vulnerable services include both privately and publicly owned assets. For example, important private services such as grocery stores, gas stations, and cellular phone service are vulnerable. Traffic networks are also vulnerable, because Pittsburgh's traffic signals would fail during a blackout, and

many tunnel ventilation fans would become inoperable. The study also found that three of the five Pittsburgh police zone stations do not have on-site backup generation. In addition, liquid fuel storage tanks, which rely on electricity to pump fuel, generally have no electric backup. Some fuel can be released from storage tanks via gravity flow, but the switchover from pump to gravity flow can be time-consuming.

The study found that Pittsburgh's natural gas system is highly reliable; possibly more so than the diesel supply chain. Although natural gas backup generators are typically more expensive than those powered by diesel, natural gas powered backup is a viable option for high value services, especially if the generators are used to produce electricity and heat during normal operating conditions. However, local law specifies in some cases that backup systems be fueled by diesel. Furthermore, critical service providers such as financial institutions prefer diesel – they can control their own fuel storage supply, independent of the natural gas supply. However, only a few days of diesel is usually on hand even in the best facilities. Propane can be used for backup fuel in certain locations.

As proven in the Paris heatwave of 2003 and the Quebec ice storm in 1999, an outage during extreme hot or cold weather could significantly damage health and the economy. If an outage were to occur during hot weather, air conditioners would fail. In very cold weather, forced-air heaters and electronic ignition boilers would not operate. In addition, an extended outage during the winter could cause pipes in homes to freeze and burst, putting more stress on emergency management personnel. In either hot or cold weather, some people would be at risk for health problems, and emergency shelters would need to be available. An effective information campaign (which takes into account that television sets would not be working) would need to disseminate information about the availability of emergency services. While plans do exist for handling weather-related emergencies in some cities, it is important that such plans be regularly reviewed and updated to ensure that regions are well prepared for an extended power outage.

RE-FRAMING THE PROBLEM: WHAT SERVICES MUST BE CONTINUED?

While much of the government and the research community, including many of those concerned with the electric power industry, have focused on the protection of networked infrastructure, what really matters is the social services that those networks provide. Three strategies can be pursued to assure that critical social services are maintained: (1) harden the network to make it less vulnerable to disruption; (2) make the network more robust so it can survive

disruptions and continue to operate (perhaps at a reduced level of service); and (3) pursue alternative strategies to keep services operating when power from the network is no longer available.

Because networked infrastructures are physically dispersed, there is no way to harden every piece against accidental or intentional disruptions, although increased protection for some system components would make sense.[3] Researchers in cyber security understood the limits to system hardening many years ago. Indeed, it was the desire to produce a computer communication system that could continue to operate when parts of it were disrupted that led to the architecture of ARPAnet, the forerunner of today's Internet. Computer security theorists have therefore largely abandoned the model of a computer system as an impenetrable fortress. Rather, they seek to design a "survivable" system – that is, one that can fulfill its mission in a timely manner, even in the presence of attacks, failures, or accidents.[4] Making the electric infrastructure similarly more robust is feasible, and many improvements are possible in operations and standards.

A focus on survival of missions stands in contrast to survival of the generation and transmission grid through approaches such as "islanding" (separating the survivable parts of a grid from those that are critically wounded), which have long been used. These are good tools, but their implementation over the past two decades has failed to eliminate low-probability, high-consequence outages, nor are they likely to do so in the future.

Ensuring the fulfillment of critical missions is also different from either a traditional vulnerability assessment approach or the approach of making the electricity delivery system 100 percent reliable.[5] Invulnerability is not only very expensive, but it is also impossible to test and probably impossible to achieve for a complicated system like the electric grid. Rather, a fresh approach is needed to prevent society from incurring large costs during the inevitable next blackout or from attempting to entirely prevent such a blackout.

SEVEN STEPS TO ASSESSING READINESS

The goal of a socially oriented approach is to lower the social costs of grid failures, rather than preventing all of them. More specifically, the goal is to reduce the costs of the inevitable grid failures by assuring the continued availability of critical services and subsystems, such as traffic signals in urban cores, pumps for water and sewer systems, urban mass transit, emergency service systems, subway and elevator egress, and crucial economic functions.[6] Verification could be accomplished in a number of ways, including actual tests conducted on the services and subsystems (something that cannot be done on the full grid).

The first step in defining and verifying solutions to the survivability of critical missions would be to determine a set of design reference events that

Table 14.2. Three representative blackout events

	Temporal duration	Spatial extent	Reference frequency	Likely causes
Reference event 1	4 hours	1 circuit (about 1,000 people)	1 in 22 months	Load shedding, weather
Reference event 2	2.5 days	400,000 people	1 in 6 years	Weather, disruption of transmission or generation
Reference event 3	2 weeks	All of a region	1 in 50–100 years	Weather, terrorism

would mimic outages of varying lengths and geographical locations. The system would be evaluated on the basis of whether it fulfills critical missions during these design events. An example of a set of design reference events is given in Table 14.2.

The second step would be to define the missions that must be fulfilled. This step would results in enumeration of life-critical and economically important missions that are provided by electric power, together with a list of missions which, if unfulfilled, would have important socio-economic consequences (such as reducing gross domestic product or inducing terror).

The third step would be to prioritize the missions. The priority list would be different for different design reference events. For example, a 12-hour outage from a cascading grid failure would have different priorities than would a month-long blackout from a severe ice storm or human attack on system components. Similarly, some services, such as delivering potable water, could carry on uninterrupted for a day or more because of water stored in the system. Thereafter, however, water delivery would be far more problematic. Others services, such as sewage treatment and disposal, might be an immediate problem.

The fourth step would be to determine which missions are already protected (e.g., hospitals and navigation aids for air traffic). Weak links in the chain would be identified at this step. For example, while the New York City area's Newark and Kennedy airports quickly restored power for passenger screening and other boarding functions the day after the 2003 blackout, LaGuardia could not because it had insufficient backup power, and its grid power was slow to be restored. As a consequence, East Coast air traffic was snarled by the closing of a busy hub.

The fifth step would be to determine which missions require procedural changes or new hardware.

The sixth step would focus on the missions in step five that require new hardware. This step would seek cost-effective technologies that could fulfill critical missions during the design reference events. For example, light-emitting

diodes (LEDs) could produce traffic signals with only a small fraction of the energy required to light the incandescent bulbs currently housed in traffic lights. Inexpensive batteries and trickle chargers of LED traffic signals could ensure that lights could continue to operate without additional electricity for days during a power outage. Other cost-effective devices might include those that make elevators return to the ground floor or allow subways and elevated trains to creep to the next station. Some devices would be attractive for private investment (for example, tenants may be willing to pay higher rent for a building that has its own micro-grid with backup power). For public goods at this stage, the costs of fulfilling the missions would be compared with the value of the missions, and alternative methods of fulfilling the missions could be evaluated. Effects of the candidate solutions on the nominal and recovering grid would be assessed and verified during this step by building and testing prototypes where necessary. For example, loads would be tested for their smooth transfers from distributed power systems to and from the grid to ensure that the transfer would not affect grid stability – this could require hardware and operations changes and would certainly require tariff changes.[7]

The seventh step would be to build a system for allocating competing resources required for these missions during an extended blackout. This is often the first step considered by managers trained in emergency response, but it would be much more effective if preceded by steps one through six.

Performing the tasks outlined in these steps can yield an up-to-date assessment of the readiness of the system to respond to challenges. Knowing the available hardware and procedures, governing authorities can estimate which missions could be accomplished and where the greatest trouble spots are likely to be.

PRIVATE AND PUBLIC INVESTMENTS IN SOCIALLY CRITICAL MISSIONS

During a large power outage such as one caused by a hurricane or ice storm, the best that government agencies can do by way of social services is to provide a limited number of shelters and very limited distribution of water. Most of the organizations in a position to assure that important social services continue during a power outage are private companies. While it might be to the collective benefit of society for these organizations to make investments that will make services more robust, it is often not in their private interest to do so. In other cases, the investments may be in the interest of private entities but not properly identified as an opportunity. Or it might be possible to provide incentives or information to make these investments more attractive to private entities.

Private entities such as supermarkets and gas stations have no responsibility to secure their operations to make them more robust to blackouts – they are responsible only for their owners. If it is possible to avoid loss or increase profits during a blackout, a profit-maximizing firm will do so. For example, the decision for a private company to install a backup system involves the calculation of the cost of a backup system, how often it would be needed, and whether it would generate net benefits.

Most backup systems required to provide services independent of grid power have associated capital and maintenance costs. When a purchase of a given capital expense is contemplated, the decision maker estimates the frequency of power outages at the location being considered, and the cost of the power outage. If a 100-kilowatt generator (appropriate for a heat treating furnace, for example) costs $76,000 and is financed over its 12-year lifetime, the annual cost of capital to purchase the generator at an interest rate of 7 percent is $9,400. Operations and maintenance costs for this size a generator, if properly maintained and operated at full load once a month, are approximately $1,900 annually, for a total yearly backup cost of $11,300. If the generator is used during a power outage to back up a service that incurs losses of $25,000 (perhaps in lost product during a furnace heat-treating cycle), then the generator would be a sensible purchase if the company expects the power to fail long enough to ruin production more frequently than once every two years. Figure 14.2 illustrates the decision process.

As another example, a multi-story apartment building owner with a typical small traction elevator faces a product differentiation backup decision. The elevator would be backed up by a 12-kilowatt generator, with capital cost of $13,200 and annual maintenance cost of $240. Using a discount rate of 7 percent and a 12-year equipment lifetime, the amortized monthly cost of the backup would be $160. For a five-floor apartment building with six apartments per floor, a monthly rent increase of less than $5 would pay for the backup. While some tenants might not value this service, others might seek out such a building and willingly pay the increase.

SUGGESTED POLICY CHANGES TO ASSIST INVESTMENT

Policies to encourage survivable services can be win–win situations. At present, however, institutional or informational barriers inhibit more widespread installation of backup systems, even when they generate net benefits. State and local governments could encourage or require private parties to improve the reliability of important social services in a number of ways. For example, governments could modify electricity tariffs to permit load serving entities to recover costs associated with designing, installing, testing, and maintaining backup on-site power systems for individual customers who sign up for this service.

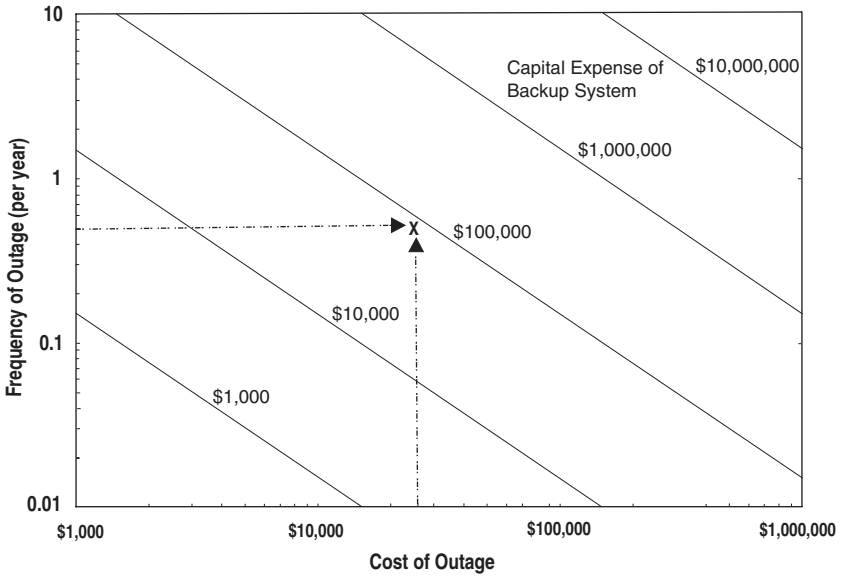

Figure 14.2. Decision support tool for backup systems. Example analysis for backup systems with 12-year depreciation at 7 percent discount rate and annual operations and maintenance costs equal to 2.5 percent of capital cost. If the capital cost of the backup system is lower than the point at the intersection of the assumed cost and frequency of a power outage, the purchase of a backup provides greater benefit than cost.

State and local governments could also provide information and suggestions to private parties to help them see how they might benefit from strategies that would make their services more robust in the face of power outages. A prime candidate might be a multi-story retirement home that installs backup power for its elevator and then finds that advertising this fact provides it with a competitive advantage.

Governments could encourage firms to offer "preferred customer" services that would assure continued availability of services, such as access to gasoline and ATM machines, to customers who have paid a fee that allows the companies to make the necessary additional investments. Preferred customers would be offered special service during an emergency. Alternatively, government might approve a special surcharge for businesses during blackouts, analogous to the surcharge collected by taxicabs during a snow emergency. The surcharge would enable a service provider to recover the cost of an already installed backup system. In addition, states should study whether barriers exist to fostering backup power installations funded through surcharges.

States or localities could require businesses to post publicly accessible information on the presence or absence of back-up devices. In much the same way that the publication of the U.S. Environmental Protection Agency's toxic

release inventory has induced many companies to cut emissions, such postings might induce companies to take steps to make their critical services more robust.

Changes to building codes and other legal requirements could also change business practices. For example, a decade ago some U.S. cities adopted a building code that requires elevators in newly constructed buildings of more than seven stories to have backup power. Similarly, a community could require, as a condition of doing business, that firms operating gasoline pumps, ATM machines, or similar devices must work together to arrange for a percentage of these services to remain operational in the event of a power outage.

Governments could also provide tax incentives, subsidies, or grant programs to support the development of needed facilities. Given limited resources, this option should be used sparingly. Some circumstances, however, such as certain upgrades to emergency rooms of private hospitals, may warrant modest assistance.

Finally, communities could facilitate the construction, interconnection, and operation of distributed generation systems, and the operation of competitive micro-grid systems. In much of the United States today, rules granting utilities exclusive service territories make such micro-grids illegal; these rules could be changed.[8]

State and local governments could also encourage or require public and non-profit parties to improve the reliability of important social services. For example, information and suggestions to local governments and non-profit organizations could help them see how they might benefit from strategies that would make their services more robust in the face of power outages.

However, because most power outages arise from failures in the local distribution system, some jurisdictions have adopted regulatory requirements to foster retail competition based on reliability. This is most prevalent in New Zealand and Australia, where up-to-date reliability indices are posted on utility and government websites.[9] Transparency of this sort aids consumers, but it is uncommon in the United States.

TEMPTING TARGETS

Electric infrastructures have been targeted for destruction by, for example, the North Atlantic Treaty Organization (NATO) in the southern Yugoslav province of Kosovo, the Farabundo Marti National Liberation (FMLN) in El Salvador, radical environmentalists in the United States and the Czech Republic, and labor movements and disgruntled landowners in several countries. They have also proven to be tempting targets to hunters practicing their sharp shooting. Iraqi insurgents have attacked European and U.S.-manufactured hardware in

Iraq, and presumably some information on vulnerable features has been shared with groups outside Iraq.

Several general areas of vulnerabilities may be tempting targets for sabotage. For example, often many of the main transmission lines feeding cities travel over a single corridor, providing a target for both natural hazards and human disruption. A 2002 study by the National Research Council identified large transformers as a critical area of vulnerability, because they are often unique and take many months to construct.[10] Spare relays and transformers are sometimes stored at substations.[11] Indeed, substations have been the subject of domestic attacks with some frequency. On the generation side, however, vulnerability due to a fuel shortage is now lower, because past labor actions in the coal mining industry were frequent enough that generators now have many weeks of coal on hand.

Several companies maintain large portable generators that can be brought in to provide power in emergencies. Analysis should be undertaken to examine whether the country has enough such capacity, and whether other portable equipment (such as transformers on rail flat cars) are needed. Navy and other ships are also a potential source of power during disruptions in coastal cites, and diesel locomotives can be used in inland locations, but all of these options require advanced preparation and planning.

Although a potential target of attack, the electric grid is not particularly effective for causing psychological disruptions. Because the average U.S. customer loses electricity for 2–8 hours one or two times per year,[12] it is difficult to incite terror by turning out the lights. There are conditions, however, under which a blackout can cause terror. For example, riots occurred during the 1977 New York City blackout (3,500 arrests were made amid widespread looting) but not during the 1965 or 2003 blackouts.[13]

On the other hand, the psychological value of attacking nuclear generation stations and their associated fuel storage facilities is substantial, and these installations have received additional physical security attention in recent years. An attack would not need to cause a core meltdown or the release of radioactivity to generate a public outcry. Public concern that leads to plant closures could quickly reduce generation margins in countries such as France, where nuclear power provides 85 percent of electricity, and the United States, where roughly one-third of all power in the eastern United States is generated by nuclear stations. The public's concerns may be especially important in nations that have experienced a nuclear power plant or fuel cycle mishap (the United States and Japan, for example). Continued attention to the physical and cyber security of these facilities, including personal reliability programs to reduce personnel vulnerabilities, is warranted.

A recent review by Farrell and colleagues identifies additional areas of vulnerability, such as tank farms associated with the U.S. Strategic Petroleum

Reserve.[14] While petroleum distillates fuel only 2 percent of U.S. generation, diesel (a petroleum distillate) provides much of the nation's emergency backup capability. The study points out that liquefied natural gas (LNG) storage facilities could be a target. LNG is stored at roughly 150 peaking generation facilities worldwide, and more than 100 LNG tankers ply the seas. An attack on an LNG terminal could leave the public much less likely to accept an increase in the number of LNG terminals, which are projected as trade in LNG becomes more global. One response to the risk of disruption of gas supply would be dual-fired generation units, which can burn whichever of two fuels costs less or is available if supply of the other is interrupted.

Computer-based failures or attacks on infrastructure have also become a concern. Farrell and colleagues describe the U.S.-led 1982 cyber attack on the Soviet Union's natural gas pipeline infrastructure as evidence of similar current vulnerabilities. More recently, consolidation in the power industry has increased the number of devices running the same computer software (making more systems vulnerable to a single attack), and pressures from competition leave little money for large expenditures for cyber security. The U.S.–Canadian commission investigating the 2003 blackout established a special task force to look into whether the blackout was caused by cyber attack. The task force concluded that it was not, but nonetheless significant architecture and operation vulnerabilities existed in the control software and hardware. Organizations such as the Computer Emergency Response Team Coordination Center may be able to work with vendors and operators to reduce such vulnerabilities, but the threat of insider action is significant.

A 2003 study by Watts describes instructive South American experiences in reinforcing their grids.[15] For example, Chile, which first deregulated electricity in 1982 and faced domestic attacks throughout that decade, constructed mobile substations, accompanied by transportation plans to move these large-wheeled units and coordinated in advance with urban law enforcement units. Some standardization of transformers at subtransmission voltages was made, with spare units stocked at low power levels. Substations were protected with double fences 4–5 meters high and solid steel doors with sensors to detect intruders. Transmission tower bases were protected with fences. However, Watts notes that "after more than two decades of deregulation in Chile and in absence of terrorist attacks, some secure physical policies have been forgotten in order to reduce 'unnecessary' costs." Watts notes that Brazil has established a monitoring and control network based on power line communication, which can isolate some locations to reduce the extent of cascading outages. This system uses an automated protection scheme based on both central and distributed agents to control generation and load, and is said to achieve stable operation within seconds of loss of a major substation.

RECOMMENDATIONS FOR GRID IMPROVEMENTS

While completely eliminating blackouts is an unrealistic (and expensive) goal, it is quite possible to improve upon the current record of blackouts while at the same time decreasing the extent of cascades caused by deliberate human actions.

Investigations of blackouts such as those listed in Table 14.1 reveal a number of common problems that need to be addressed.[16] Significant improvements can be made within the next few years. We recommend a near-term plan based on our analysis of what has worked in other interconnected systems. These proposed improvements recognize that real people make mistakes, and that the system should be designed to reduce both the number and effect of those mistakes. Some of these recommendations are hardware-related, but all are designed to reduce both accidental and deliberate large blackouts.

MONITORING AND DATA COLLECTION

Ineffective monitoring, or lack of monitoring, comes up regularly as a problem leading to blackouts. While there is great variability in the quality of system monitoring across the country, monitoring of the power system overall is more sparse than it should be, both within regions and between them. Market pressures are not likely to improve matters.

Systems to display these data to operators vary as well, and most control centers ignore decades-old recommendations to display the information in a format that enables operators to identify the extent of a disturbance. The present representations of system state, particularly indicators of danger, are too complex. They stress accuracy over clarity. And even the limited and poorly displayed monitoring data that are collected are not shared among power companies.

National standards for telemetry data on power flows and transmission system components must be established and enforced. Operators can no longer be expected to make the right decisions without good data. Control centers must have displays and tools that allow operators to make good decisions and to communicate easily with operators in different control areas. There must be backups for power and data, and clear indications to all operators that data are fresh and accurate. The emphasis should be on data and presentations that support decisions.

Grid operators also need much clearer metrics of danger and suggestions for action (similar to collision avoidance alarms in aircraft and in air traffic control centers). A better warning system does not have to be expensive, however. For example, if the existing 157,000 miles of transmission lines in the United States were fitted with $25,000 sensors every 10 miles, and if each sensor were replaced

every five years, the annual cost would be $100 million, or roughly one-tenth the lower bound of the estimated annual cost of blackouts. From a consumer's standpoint, the cost would increase the average residential electricity bill (now approximately 10 cents per kilowatt-hour) to 10.004 cents per kWh.

As described in more detail in Chapter 13, the data systems that monitor and control the grid in most large utilities formerly were proprietary systems with limited or no connections to the rest of the world. However, partly in response to cost pressures, some system functions in some utilities are no longer isolated. This leaves these systems vulnerable to cyber attack. Because the arcane nature of proprietary systems no longer protects utilities that adopt a common system, they must pay much more attention to the threats posed by hackers who can develop one exploit and use it on many power systems.

TRAINING

Another issue to address is operator training. Training, as with monitoring, varies widely between power companies. Most operators are not trained routinely with realistic simulations that would enable them to practice dealing with the precursors to cascading failures and the management of large-scale emergencies.

All grid operators must be trained periodically in contingency recognition and response using realistic simulations. These simulations must include all operations personnel in a way that exposes structural deficiencies such as poor lines of authority and insufficient staffing. The goal should be to recognize and act upon signs of extreme system stress that may be well outside daily operations experience. The description of piloting an aircraft as "years of boredom interrupted by moments of stark terror" applies also to grid operations, and training should be as rigorous as that undergone by pilots. Grid operators must have the systems and training that only realistic simulation, using their specific control center configuration, can provide. Federal standards for training, licensing, and certification of grid operators and control centers are warranted to ensure against a single weak control center bringing down a large area. No federal entity mandates such realistic training for grid operators, but the owners of nuclear generation plants proved (after Three Mile Island) that it can be done.

EQUIPMENT

Power companies widely vary in their system abilities and equipment sophistication. Some companies can interrupt power to customers quickly during an emergency, whereas others are nearly helpless. This patchwork ability to shed load is not appropriate to the current interdependent transmission grid.

Some systems can interrupt power automatically, but some cannot even do it manually from the control center. Operation control centers must be able to actually control.

Shedding of load in the near term would probably take the form of preemptively blacking out large areas. Some power companies have customers who have agreed to be blacked out in emergencies, but this practice is not uniform. In a future decade, it may be possible on a large scale to provide signals to consumers to shed parts of their load in exchange for lower tariffs, but this partial load reduction solution has not been economically feasible with current systems in the United States.

Sensors, load-shedding devices, and other system components must be checked on a more systematic basis than they are at present. The August 30, 2003, London blackout resulted from an undersized component that had not been checked. Five hundred thousand people were stranded during rush hour. In today's highly competitive environment, chief financial officers may frown upon periodic checking and testing – it should therefore be mandated by national standards.

INDUSTRY STANDARDS

Industry standards are lax across the grid, and this also can lead to outages. For example, in many systems vegetation under transmission lines is trimmed only every five years, instead of more frequently. As was recorded in the 2003 U.S.–Canada blackout, lines sagging into untrimmed trees contribute to blackouts. Industry standards for tree-trimming under transmission lines must be set with the costs of failures in mind, not just by the competitive constraints of the immediate marketplace. Companies that do not comply should be penalized. These standards could vary by region and should be set by regional bodies such as the regional transmission operators.

NATIONAL COORDINATION

A national grid coordination center should be established and run as a national asset by a private body. It would stimulate research and development to support the data needed for grid monitoring. A national center would also monitor the grid at regional and larger levels, provide national flow control, and perhaps act as a backup for computer failures in individual control regions. As with air traffic control, the roles and responsibilities of the local and national centers would be neither perfect nor without infighting, but they would complement each other to avoid the complete lack of "big picture" awareness seen in so many blackouts.

In addition to the national coordination center, a permanent government investigation body should be appointed, including professional accident investigators who are trained to look for systemic as well as discipline-related causes. This body should be an entity separate from the operators or regulators of the grid.

INNOVATIVE THINKING

In the longer term, more serious consideration should be given to changing the basic geometry and operation of the transmission system. For example, advanced power electronics could be use to control exactly where power flows through the lines.[17] Advanced systems could also be used to better compensate when industrial customers add or drop very large loads. In addition, direct current transmission lines could reduce the loss of energy that occurs in transmitting alternating current power long distances. Other technologies, such as robust automatic control systems to reduce dependence on human operators, might be feasible in a decade.

If properly implemented with intelligent controls, generating electricity in relatively small plants located close to consumers, rather than in large central generation plants, could reduce blackouts.[18] Such distributed generation could also lead to dramatic increases in overall system efficiency because excess heat need not be thrown away, as it is in large central plants, but could be used for space conditioning or process heat. Such distributed generation now accounts for 7 percent of the United States' capacity, and the Energy Information Administration calculates that a three-fold expansion is possible. This distribution could dramatically increase reliability, if local fuel storage is used (to avoid reliance on the natural gas network). However, while distributed generation holds promise, for the foreseeable future the U.S. power system will primarily rely on centrally generated power sent over the existing transmission grid.

The need for innovative thinking suggests that an expert commission should be created to advise the body setting mandatory standards. The commission should have experts from operating companies, systems operators, the Federal Energy Regulatory Commission (FERC), and academia to take a fresh look at how to design both engineering and operation standards to satisfy the goals of the system.

INFORMATION SHARING

Information is required to convince decision makers to invest in survivability. However, organizations that hold important information about survivability and the power network are highly protective of their information.

The sort of information needed to assist governments in the decision-making process can be summarized in three groups: (1) models of the storage, transportation, and consumption of fuel and other goods during a blackout; (2) catalogs of the electrical needs and generating abilities of facilities, agencies, businesses, and communities; and (3) quantification of the criticality of different services during design reference power interruptions.

Obtaining the information necessary to assess the vulnerability of important services in the face of power outages and proposing solutions may be at odds with the desire of many organizations, especially those involved with homeland security, to keep information about vulnerabilities out of the public domain so that pernicious persons or groups cannot exploit those vulnerabilities. The problem is that if groups performing system-level analysis for state or local governments cannot access important information, it is extremely difficult for policymakers to develop rational policies to reduce future vulnerabilities. We encountered such difficulties when we performed a preliminary analysis for one agency of the state of Pennsylvania and found that even with the state's assistance it was impossible to obtain important data from other state agencies.

Public utilities are particularly protective of information about their emergency preparedness. For example, community water systems have prepared vulnerability assessments and emergency response plans. When questioned about any aspect of emergency operations at water system facilities (including the number and size of generators, the amount of fuel stored at pumping stations, or the parts of the water system that will first lose service in a crisis), facility managers will most likely answer by saying that the information is contained in the emergency response plans. These documents are reviewed but not retained by the states before being sent to the federal level. They are not available to the public.

This lack of information sharing is a problem even for responsible government agencies: one county emergency management coordinator described hitting an information "roadblock" when requesting information from local utility companies in an attempt to develop a critical infrastructure plan. A 2003 survey of public utility commissioners found that 54 percent "believe that utilities are either somewhat or very reluctant to share their security information with the commission."[19] The purpose of protecting information about emergency preparedness is to assure the public that emergency plans will not be compromised. This must be balanced by releasing enough information to assure the public that emergency plans are effective.

At the moment, the pendulum appears to have swung too far in the direction of compartmentalized information. For example, certain actions by the Department of Homeland Security to centralize and then compartmentalize information about vulnerabilities are not conducive to developing corrective

action. For example, a 2004 Associated Press report describes the process by which landline phone networks must alert federal regulators of service outages and report how the problems will be avoided in the future, a process that Federal Communications Commission (FCC) asserts has improved the landline phone networks; however, attempts to apply the same process to the wireless and cable phone networks have met with opposition.[20] Neither the companies themselves nor the Department of Homeland Security want the information made available to the public for fear the information will provide "blueprints for terrorists bent on wrecking U.S. communications systems." Rather than filing with the FCC and allowing public access, the reports would be filed with the Department of Homeland Security.

The problem, of course, is that the Department of Homeland Security and other similar organizations have neither the resources nor the authority to develop and implement most of the changes that would be needed to make important social services less vulnerable. Those resources and responsibilities are widely distributed among state and local governments and in the private sector. It would help if the Department of Homeland Security and other similar organizations at sub-national levels could develop a greater ability to engage in system-level analysis that considers and balances a range of legitimate but perhaps conflicting social objectives. They would also need a greater ability to think about problems in terms of preserving social services as opposed to a unitary focus on protecting "critical network services." Furthermore, the department would benefit from having a greater ability to develop and promote a range of alternative polices that states and private entities might adopt to promote viable solutions to reduce vulnerabilities. Finally, the department would need to provide arrangements that allow informed independent analysis by academic and other groups following the lead of other agencies that deal with sensitive information, such as the Bureau of the Census (i.e., academics and others can become sworn Census Officers) and the Department of Defense (e.g., the JASONs, a rotating group of the nation's top scientists, have been providing classified analysis to the department since 1959).

In the meantime, the states would be well advised to develop an interagency arrangement, perhaps in the form of a standing interagency committee, which is charged with better balancing the conflict between the short-term need to protect information about vulnerabilities and the long-term need to encourage responsible parties to use such information to develop and implement solutions. Such an interagency committee should also have responsibility for exercising oversight to assure that solutions and systems developed by others would actually provide the protection they promise. Too often, entities provide assurances that everything is under control, only to find that back-up systems fail to operate when an actual outage occurs.[21]

Every organization faces a dilemma over releasing potentially harmful information. The more people who see the information, the more likely it will get into the hands of people who seek to harm the organization. But the more people with access to the information, the more likely that it will be thoroughly critiqued and that better plans will be developed.

The dilemma is particularly acute in a democratic nation under threat of terrorist attack. Not only is a great deal at stake in ensuring that proposed actions are efficient and cost effective, but the public has a stake in knowing what is to be done to protect them. A nation must strike a balance between open information (no one wants to tell terrorists how to do the most damage) and cost-effective actions. We know from published information on military programs that classified programs generally are not cost-effective and often are ineffective. Indeed, organizations often try to limit the release of data to shield themselves from scrutiny that might show that they are doing their job badly. In the United States at the moment, only a few individuals in the Department of Homeland Security have access to data, and there is little effective outside review of how their $41 billion is being spent.

Regardless of attempts to obscure it, however, much of the desired information can be obtained through other sources, from current employees to past computer postings. While publishing the information might make it easier for terrorists to disrupt society, it also is very likely to lead to improving the systems and possibly preventing or at least lessening the potential impact.

HOW MUCH PROTECTION?

The cost of failure of the grid can be substantial: the outage that affected 50 million people in August 2003 cost $4–6 billion. Given the high potential cost of a widespread outage due to a terrorist attack, government and private entities will face substantial pressure to encourage or require protection of a wide range of assets. However, no nation has unlimited resources to dedicate to countering the many threats that could be directed at symbolic targets and critical infrastructures.

How should a balance be struck between protecting assets and continuing robust economic activity? We can use the figure of cited above to estimate that attacks that black out 10 million people may take place every year in the absence of increased protection, costing $1 billion annually; if the system were up-graded at a cost of $100 million per year, the number of blackouts might be reduced to once every 10 years. With this assumption, we calculate that upgrading the system is worth $900 million in expected savings. In fact, this savings might justify an upgrade that cost $9 billion. Of course, different

assumptions of attack frequency will change these estimates greatly. If attacks on the grid succeeded in causing blackouts every three years (with no additional protection), then the justifiable expenditure for additional protection would be $300 million annually.

Whatever level of expenditure on new protection is agreed upon, mechanisms must be in place to decide on whether a particular expenditure should be made, and to allocate its costs. O'Hanlon and colleagues argue that the most efficient mechanism to allocate costs is "a combination of regulatory standards and antiterrorism insurance" whose premiums would be shared between the government and the users.[22] We note that the insurance industry is very slow to insure newly identified risks, so such insurance may be unavailable. We have also argued earlier in the chapter that national standards for grid operation and data can dramatically improve reliability. These will be viewed by industry as "unfunded mandates," but their cost may be viewed by society as justified.

In the energy sector, the FERC has indicated that it will approve applications to recover prudent costs for protection of electric power assets.[23] Burns and colleagues have discussed principles that state public utility commissions might use to determine whether protection-related expenses should be passed on to customers.[24] These authors conducted a survey of public utility commissioners in 2003, finding that 83 percent have no special guidelines for determining the acceptability of protection measures. They suggest that commissioners might use rules developed during the expenditures of funds to upgrade software to avoid the Y2K problem as a starting point. In any case, there should be enough flexibility to allocate some costs to protection for systems that have both public and private benefits. For example, the Department of Homeland Security could provide financial incentives to distributed generation systems that decrease the probability of grid failure.

We now consider the question of how to judge which expenditures to make, because the nation cannot afford to protect everything. If one target is hardened, an attacker will switch to a softer target. One way to study such interactions is through game theory. Another is through large-scale war gaming. Used together, both approaches have the potential to identify cost-effective areas for protection expenditures.

Keith Florig examined whether the U.S. Postal Service should extend its existing program to irradiate mail bound for certain destinations in the wake of the anthrax attacks.[25] He estimates that irradiation of all mail would raise postage costs by 1–2 percent, delay delivery by several hours, and cause harm to some materials shipped by mail. He finds that mail sanitization "would have to avert at least a hundred casualties per year to be as cost-effective as most other societal investments in public and occupational health." But Florig then goes on to note the enormous disruptiveness of the anthrax scare, and that "society's

willingness to pay for preventing future incidents of terrorism through the mail should be based on the combined economic, institutional, psychological, and public health damage that such mischief can inflict. . . . Before committing billions of dollars to technologies for the long-term enhancement of mail safety, federal authorities would be wise to ask the public how they weigh these costs and benefits."

This formulation addresses a key point: protection expenditures can be large enough that the public, not just experts or lawmakers, should be involved in judging which systems should be protected. Risk communication is often thought of as a way to lessen the impact of a disaster on society but, as noted by Morgan and colleagues, it is a two-way street whereby the public and experts can jointly shape policy.[26]

In the United States, substantial roadblocks exist to both analysis and policy for protecting the electricity infrastructure. It is perfectly possible for any group isolated behind walls of secrecy to make enormous expenditures that are ineffective, directed at unimportant targets, and impose substantial penalties on individual liberties and the economy. Decisions must be made only after thorough examination of alternatives by a diverse range of analysts, and after wide-ranging and open discussion. Such a conversation is overdue.

In summary, the terrorist threat has prompted a more general examination of the reliability of the electricity system. The examination is welcome in that considerable costs inflicted on individuals and the economy could be lowered by focusing on ways to fulfill critical missions during a blackout. Because the costs of defending against both natural hazards and terrorists could be considerable, the public needs to be brought into the discussion to find out what interruptions they find most bothersome and what they are willing to pay – through higher taxes, higher product prices, or annual fees – for increased reliability.

ACKNOWLEDGMENTS

The authors thank the students of the Carnegie Mellon Electricity Industry Center 2004 engineering project course, who developed and assessed the data in the vulnerability study of the Pittsburgh area. The student members of the team were Benjamin Anderson, Erik Andreassen, Michell Birchak, Barbara Blackmore, Laura Cerully, Helen Davis, Jonathan Fasson, Dominic Fattore, Sandra Gani, Wenyao Ho, David Lagattuta, Emily Lauffer, Rachel Lin, Landon Lochrie, Nick McCullar, Ben Mosier, Jonathan Ng, Laura Sperduto, Marena Tiano, and Jennifer Wong. The Ph.D. candidate project managers were Kyle Meisterling and Paul Hines. Course faculty were Dmitri Perekhodtsev, Marija Ilic, Jay Apt, and M. Granger Morgan.

Appendix 14.A. Taxonomy of critical services

Service category	Specific service	Time, duration, and scope of outage during which service is critical	Typical existing backup	Health and safety risks	Economic risks
Emergency Services	911 and related dispatch centers	All outages	Most systems have comprehensive backup power systems	Risk of injury and fatality; inability to report and prioritize emergencies, potentially leading chaos	Indirect costs associated with increased chaos after an outage; businesses and stores may delay re-opening
	Police headquarters and station houses	All outages	Varies; some stations have backups; AC power is often required for recharging hand-held radios	Risk of injury and fatality; inability to report and prioritize emergencies, potentially leading to chaos	Indirect costs associated with increased chaos after an outage; businesses and stores may delay re-opening
	Fire protection services	All outages	Varies by location	High risk of injury and fatality	High risk to businesses and residences
Medical Services	Ambulance and other medical transport services	All outages	Limited; many require AC power to charge batteries for radios and cell phones, and to pump fuel at commercial gas stations	Risk of injury and fatality	Injury and fatality, loss of workforce
	Life-critical in-hospital care (e.g., life support systems, operating rooms)	All outages	Full, but some failed during the August 14, 2003 blackout; some systems have inadequate testing procedures	High risk of fatality	Fatality, loss of workforce
	Less-critical in-hospital services (e.g., refrigeration, heating and cooling, sanitation)	Medium and extended duration	Varies	Increased risk of infection	Indirect risk

Non-electric public utilities	Water treatment	Extended duration	Typically very limited	Risk of illness if system pumps untreated water	Incapacitation and workforce productivity
	Drinking water	Extended duration; immediately in areas with wells	Limited gravity-fed areas; some pumps have backup power	Risk of dehydration and/or disease, especially during hot weather	Incapacitation and workforce productivity
	Sewer treatment	Medium and extended duration	None in most areas	Risk of disease from untreated sewage in water supply	Incapacitation and workforce productivity
	Sewer pumping	Short duration, high use periods (morning, evening); long duration	Very limited	Risk of disease from sewage buildup in low elevation areas	Incapacitation and workforce productivity; damage to buildings in low-lying areas
	Natural gas	All outages (including some critical backup generation fueled with natural gas)	Most pipelines use the materials being transported as the pumps; in-home furnaces require power for pilot lights and fans	Significant health risk for customers using gas heat during cold weather	Pipes may burst in cold weather if homes/buildings are left without heat
Communications	Radio broadcast media	Medium and extended duration	Most stations have backup systems with several days of stored fuel	Radio is important for distributing emergency information; risk of chaos if stations fail to disseminate information	Increased chaos costs from decreased communications
	Television broadcast media	Medium and extended duration	Many stations have backup power systems with several days of stored fuel	Less vital than radio communications as most TV sets require electricity	Most risk is borne by broadcasters and advertisers
	Cable television and broadband services	Medium and extended duration	Minimal	Less vital than radio communications as most TV sets require electricity	Risk for businesses that rely on cable broadband services

(*continued*)

Appendix 14.A (*continued*)

Service category	Specific service	Time, duration, and scope of outage during which service is critical	Typical existing backup	Health and safety risks	Economic risks
	Wired telephone systems	All outages	Most systems have good backup power systems; some fiber optic systems depend on grid power, as do many new phones	High risk as many vital services rely on the wired telephone system	Very high economic costs; communications are vital to every sector in an emergency
	Wired data service	All outages	Varies	Minimal risk, unless used by medical or emergency services	Significant risk, as many business functions require broadband connectivity
	Wireless (cellular) telephone and data systems	All outages	Minimal; battery backup provides only 2–8 hours of service at most base stations	Possible risk to those unable to make emergency calls	Significant risk to customers who rely on cellular phones
	Computer services (on- and off-premise)	All outages	Data centers typically have good backups with several days of stored fuel and priority fuel contracts; on-site uninterruptible power supplies are typically limited to several minutes of computer backup power	Loss of data	Minimal risk, if computers use commercially available automatic shutdown software sensitive to power supply; significant for unprotected businesses
Non-emergency government services	Information service offices	Medium and extended duration	Varies with location and type of building	Important for distributing emergency information; risk of chaos if information is not available	Increased chaos costs from decreased accurate information

	Prisons and other detention facilities	All outages	Varies	Potential risk to prisoners, guards, and public if security systems fail	Indirect risk from increased chaos
Transport and mobility	Building elevators	All outages	Varies with local building codes, height, and age of building	Decreased mobility for elderly and disabled	Indirect risk from lost time
	Traffic signals	All outages, particularly in urban areas	Traffic police; a very few locations have battery backup	Risk of injury and fatality due to emergency vehicle delays; could be especially serious in conjunction with a terrorist attack	Large social costs associated with traffic delays
	Tunnels	All outages	Generally none for ventilation; lighting has limited backup	Accident risk if lighting fails; possible congestion disruption of emergency vehicles	High social cost resulting from traffic delays and closure if air quality becomes too bad
	Light rail systems and subways	All outages, evacuation immediately after event	None aside from emergency lighting	Some risk to elderly or disabled if adequate evacuation plans are not in place; high health risk if ventilation is inadequate	High social costs from workforce delays in urban areas
	Conventional rail systems including railroad crossings	Extended duration	Crossings have backup batteries	Some additional accident risk at busy intersections	Fatalities at rail crossings
	Air traffic control, navigation, and landing aids	All outages, immediately after event	Federal Aviation Administration requires backup power systems to be in place	Some risk of airplane accidents that would result in a large number of fatalities	High social costs resulting from air traffic delays and in-airport delays

(*continued*)

Appendix 14.A (*continued*)

Service category	Specific service	Time, duration, and scope of outage during which service is critical	Typical existing backup	Health and safety risks	Economic risks
	Airport operations including security and on-airport ramps, luggage systems, transportation, and food	All outages, immediately after event	Partial backup power is typical	Some health risk during extreme weather conditions	High social costs resulting from air traffic delays and local and system-level airport delays
	River lock and dam operations	Extended duration	Varies	Minimal risk, unless there is a diesel shortage and river transport is required	Significant costs if there is a diesel shortage; lost trade
	Buses	Medium and extended duration	Varies, but generally minimal; problems with fuel pumping and traffic congestion	Minimal risk	Significant social costs due to loss of access to gasoline for personal vehicles
	Drawbridge operations		Varies	Minimal risk, unless there is a diesel shortage and river transport is required	Significant costs if there is a diesel shortage; lost trade
Lighting	Building evacuation and stairwell lighting	All outages	Trickle charge battery lighting required by building codes	High risk of injury and fatality without emergency lighting, especially in densely populated locations	Injury and workforce incapacitation
	Residential lighting	All outages	Flashlights, candles, and lanterns	Some risk of injury in stairwells; risks due to makeshift lighting	Injury and fatality from fires due to candles and makeshift lighting
	Indoor commercial and industrial lighting	All outages	Varies	Varies	Varies

	Security lighting	All outages	Varies	Varies by location	Potential for high economic losses
	Street lighting	All outages	None typically	Increased accident risk when roads are unlit	Indirect costs
Retail grocery	Cash registers, lighting, refrigeration, security	Medium and extended duration	Varies with location and firm preferences	Risk of food and emergency supply shortage during an extended outage	Large social costs resulting from insufficient access to food and supplies
	Wholesale grocery distribution networks	Medium and extended duration	Generally minimal	Risk of food and emergency supply shortage during an extended outage	Large social costs resulting from insufficient access to food and supplies
Financial	Cash machines	Medium and extended duration	None typically	Minimal	Significant social costs resulting from inadequate access to cash
	Bank branches	Medium and extended duration	Only for security systems	Minimal	Minimal risk, if some other access to cash exists
Financial	Credit card systems	Extended duration	Some backup power typically	Minimal	High risk during an extended outage (if also a shortage of cash)
Fuel infrastructure	Pipeline and pumping systems	Medium and extended duration	Full for natural gas (because the system uses its own gas), typically none for other products	Indirect risk for vital services if fuel pumps fail to supply required fuel	High risk to services that rely on diesel to backup important systems
	Local storage infrastructure	All outages	Varies; many locations must switch from pump to gravity feed systems	Indirect risk for vital services if fuel cannot be distributed	High risk to services that rely on diesel to backup important systems
	Non-pipeline transport and distribution systems	All outages	Backup not required as long as truck fuel is available	Indirect risk for vital services if fuel cannot be distributed	High risk to services that rely on diesel to backup important systems or propane for heating and cooking
	Retail gasoline sales	Medium and extended duration	None (a few exceptions exist)	Significant risk if emergency services cannot obtain gasoline for vehicles	High social costs associated with lack of mobility if gasoline is unavailable

NOTES

1. Apt et al. 2004.
2. Talukdar et al. 2003.
3. High-voltage transformers are especially vulnerable – they are easy to incapacitate (e.g., some could be disabled with a single shot from a high-powered rifle) and very difficult to replace. Other elements of the power system, while not a risk to system reliability, could be used by terrorists as a vehicle for damage. For example, some cooling towers could be used to disperse chemical or biological warfare agents, and nuclear spent fuel storage facilities could be attacked in a way that dispersed waste. For more information, see Farrell et al. 2002.
4. Lipson and Fisher 1999.
5. Our proposal that in addition to addressing the security of the transmission system we should focus on sustaining critical social services when the transmission system fails has stimulated some allergic reactions among traditional power engineers. For a discussion, see Fairly 2004.
6. Farrell et al. 2002.
7. Morgan and Zerriffi 2002.
8. King and Morgan 2003.
9. New Zealand's reliability information is posted on the website of the Ministry of Economic Development; see "Electricity Information Disclosure Statistics," http://www.med.govt.nz/ers/inf_disc/disclosure-statistics/2003/2003-08.html, accessed July 14, 2004. Australian companies similarly posts information on the Internet; see http://www.qca.org.au/files/EnergexServiceQualityReportSeptQtr2004.pdf, accessed February 2, 2006.
10. National Research Council 2002b.
11. Farrell and Zerriffi 2004.
12. Short 2002.
13. For more information on the riots during the 1977 blackout, see *Time Magazine* 1977.
14. Farrell et al. 2005.
15. Watts 2003.
16. See also U.S.–Canada Power System Outage Task Force 2004; Western Systems Coordinating Council 1996; Energy Advisory Board Task Force on Electric System Reliability 1998.
17. At the moment, the United States and Canada are divided into just three synchronously interconnected regions in the east, west, and Texas. In principle the large eastern and western regions could be sub-divided to reduce system-wide vulnerability.
18. Zerriffi 2004.
19. NARUC/NRRI 2003.
20. *Wired* 2004.
21. Two notable recent examples are a large hospital in Cleveland that lost power during the U.S.–Canada blackout of August 14, 2003, and the air traffic control tower at Los Angeles International airport that experienced a power outage on April 12, 2004, and disrupted nearly 100 flights.
22. O'Hanlon et al. 2002.
23. 96 FERC ¶61,299, Docket PL01-6-000 (September 14, 2001).
24. Burns et al. 2003.
25. Florig 2002.
26. Morgan et al. 2001.