ALEXANDER E. FARRELL
LESTER B. LAVE
GRANGER MORGAN

Bolstering the Security of the Electric Power System

The infrastructure cannot be made invulnerable, but the industry can improve its ability to provide service even when attacked.

The 2001 terrorist attacks made it clear that our airliners, tall buildings, water, and even our mail are potential targets. What will actually be attacked depends on the terrorists' goals, the damage that could be done, and our ability to protect each one. Terrorists attack highly visible, symbolic targets in order to make each of us fear that "this could happen to me." Although it is impossible to prevent terrorists from causing disruptions in a free society, much can be done to limit their ability to spread panic.

Energy, transportation, telecommunication, and water infrastructures are potentially attractive targets, because some elements of these complex systems are nearly impossible to protect and disruptions could impose large costs, threaten our well-being, and possibly cause thousands of deaths. In the wake of September 11, the electric power system in particular faces a number of important challenges—challenges that will require greater government involvement than has previously existed.

The need to protect power systems against ice storms, earthquakes, and other natural disasters has created a set of institutions and a physical system that can handle a wide range of physical insults. The current U.S. electric power system could likely handle all but the largest, best-organized physical attacks by terrorists. Experience demonstrates that even large-scale power outages would not create terror. However, the current system is not adequately managed to eliminate vulnerabilities at high-hazard facilities (such as nuclear reactors and spent nuclear fuel storage areas) or to deal with attack modes it was not designed to withstand (such as cyber-attack or exotic weaponry).

Further, vulnerabilities have been created by the increasing interdependence among complex networked systems supporting electricity service. More study is needed to understand these vulnerabilities and to determine the best ways of preventing loss. However, it is clear that "defense" is no longer the best strategy to pursue. Rather than attempting to develop an invulnerable fortress, it makes more sense to

Alexander E. Farrell (afarrell@cmu.edu) is a research engineer in the Department of Engineering and Public Policy at Carnegie Mellon University (CMU) and the executive director of the Carnegie Mellon Electricity Industry Center (CEIC). Lester B. Lave (lave@cmu.edu) is the Higgins Professor of Economics at CMU and codirector of CEIC. Granger Morgan is the Lord Professor, head of the Department of Engineering and Public Policy at CMU and codirector of CEIC.

improve the "survivability" of the system. No one can prevent a terrorist from taking down a transmission pole. However, the system can be configured so that although the failure of single elements may lead to discomfort, the electric power system will still be able to fulfill its mission in a timely manner even in the presence of attacks, failures, or accidents, and recover successfully.

The radical restructuring now taking place in the electric power system because of regulatory changes also threatens the system's robustness. Competitive markets will force the adoption of the lowest-cost solutions to providing electricity under the stipulated rules. If security is not an attractive investment above a minimal level, companies will not be able to make investments. Because security is a classic public good, our expectation is that it will not be an attractive investment. Thus, it is up to government to answer questions concerning how much the nation is willing to pay for additional security, what organizations will be charged with ensuring it, and who should pay for it. Currently, many different organizations inside and outside government, at the state and national levels, envision themselves as holding the primary authority and responsibility for governance over electric power system security. Congress must resolve this issue but do so carefully, because many tradeoffs are involved. It needs to decide both what sort of institutional arrangement to create and how to pay for improvements.

Turning out the lights

Many terrorism scenarios involve disruption of electric service, or "turning out the lights." Whether this would allow terrorists to create widespread fear and panic is open to question. In the United States, households lose power for an average of 90 minutes per year. For the most part, individuals and society cope with these outages well, and power companies respond rapidly to restore service. Facilities that have special needs for reliability, such as hospitals and airports, typically have backup generators.

The local distribution system is the source of most outages; these affect relatively small numbers of people. The bulk power (generation and transmission) system causes only a few outages each year. In its most recent report on failures in this part of the electric power system, the North American Electricity Reliability Council (NERC) identified 58 "interruptions, unusual occurrences, demand and voltage reductions, and public appeals" in 2000. Of these events, almost half (26) were due to weather, mostly thunderstorms. Operator or maintenance errors accounted for 12 events, another 12 were due to faulty equipment, and 2 (including the largest single event) were due to forest fires. Six outages occurred simply due to failure to have sufficient power to meet demand. Not all of these 58 events caused the lights to go out, but when they did, many customers were affected. Even so, recovery was typically swift. The largest single outage in 2000 affected more than 660,000 customers in New Mexico but lasted for less than four hours.

Natural challenges of even larger scale have been met. For example, in January 1998 an ice storm struck Southern Canada and New York State, felling 1,000 transmission towers and 30,000 distribution poles while sending thousands of tree branches into power lines. This event left 1.6 million people without power, some for more than a month. Almost a quarter-million people were forced to leave their homes. Insurance claims reached about $1 billion (Canadian). This event was disruptive and costly, but it did not create terror or significant loss of life.

However, critical points exist in the electricity infrastructure where attacks could cause more damage. Well-organized terrorists (no longer an oxymoron) could damage these choke points, because they are designed only to withstand natural hazards. Large transformers and substations constitute the bulk of these vulnerabilities, according to a 1990 Office of Technology Assessment report. These facilities are fenced off but typically are not armored or actively guarded. Some relatively low-cost security enhancements could help, from using bulletproof encasements to standardizing and stocking replacement parts (which today are rare and typically custom-made, especially for higher-voltage equipment). However, recent experience suggests that the existing system would respond well to an assault. An equipment failure-caused fire in 2000 destroyed much of Dominion Virginia Power's Ox Substation and knocked the entire facility out of service. Despite the critical location of the facility, the fire had a relatively small impact on the system; service was restored to all customers within one hour, and the substation was re-

stored to full service (and improved) within a month.

The intent to cause harm may not be a sufficient condition to create terror, either. The power sector handles several deliberate physical attacks each year, but these have generally been aimed at harming the local utility company, not at capturing headlines. Eco-terrorists have also attacked the electricity system but without much success.

The current system is not adequately managed to eliminate vulnerabilities at high-hazard facilities.

However, there is more to be learned from the study of past outages. Contingency planning, spare equipment preplacement, emergency preparedness training, and temporary personnel transfers have all been key. Power companies often lend trained workers in emergencies under fairly informal arrangements, knowing that some day they will likely need to make similar requests. NERC's 2000 system disturbances report highlights several aspects of successful management of electric system outages: planning, training, analysis, and communications. Communication during and after an event might be difficult, especially if the attack is not on the physical part of the electric power system but on its computer and telecommunications components.

The experience learned during several high-profile outages reinforces this message. The largest such event in U.S. history was the Great Northeastern Blackout of 1965, which shut down New York, as well as much of Ontario and New England, after an equipment failure. New York City was blacked out for an entire night, and about 30 million people were directly affected. The National Opinion Research Center studied this event and found that, "An outstanding aspect of public response to the blackout was the absence of widespread fear, panic, or disorder. There is probably little question that this absence is largely due to the ability of individuals to interpret their initial encounter with power loss as an ordinary event….Of equal importance in maintaining order was the rapid dissemination of information about the blackout."

A second, less-widespread outage in New York City in July 1977 was far more troubling, because looting became widespread. Although outright panic did not occur, the blackout was frightening and shocking in ways that ordinary electricity outages are not. These examples suggest that if terrorists do manage to cause a significant blackout, government and industry leadership will have key roles to play in curbing unrest and criminal activities that could induce widespread fear.

Institutions for reliability

The robustness of the U.S. electric power system and its ability to restore power quickly is no accident. Government regulatory bodies and private institutions have been established to promote reliability. Most important have been voluntary industry actions: Industry has taken seriously the "duty to serve" that comes with its monopoly franchise (bolstered by the threat of further regulation). But restructuring is undoing the monopoly franchise system, raising serious questions as to whether private approaches will be adequate. In addition, because reliability and security are not equivalent, it is not clear whether the existing reliability institutions will be able to adequately provide electricity system security. Because reliability and security are both crucial public goods, which implies that there are few incentives for private companies to invest in them, government will have to become more involved.

The oldest reliability institutions in the United States are state-level public utility commissions. In regulating the utility monopolies, these commissions sought to ensure efficient and reliable electric service for all customers. Restructuring of the electricity industry is dismantling this system by placing major portions of the electricity system beyond the scope of the commissions. It is also creating enormous uncertainties about who will eventually own transmission systems and how owners will be allowed to recover costs and earn returns. This has greatly reduced investment in the transmission system, whose safety margins are shrinking.

Competition in electricity generation has increased demands on the transmission system, because the generators are located in places that their owners find convenient, not in places that are necessarily

convenient for transmission. Public objections often make building new transmission lines difficult or impossible. In many cases expanded capacity could be achieved if advanced transmission technologies were used to increase the reliability and capacity of the existing system. But again, the lack of economic incentives is inhibiting investment. Thus, the transmission system provides the most immediate institutional challenge for improving the security of the electric power system.

After the Great Northeastern Blackout of 1965, there were calls to increase the federal role in the electricity industry, both by strengthening regulations and by expanding funding of federally controlled research. The industry responded by quickly creating a system of voluntary, regional reliability organizations, loosely organized under NERC and dedicated to promoting the reliability of bulk electric supply in North America. NERC operates by developing reliability planning and operating standards. Traditionally, the industry has complied with these standards on a voluntary basis, with the only monitoring occurring in regional councils in which peer pressure can be applied. Recently, however, NERC has moved towards mandatory compliance with the possibility of sanctions.

The Electric Power Research Institute (EPRI) was created in 1973, following a threatened federalization of electricity R&D. Still, even with EPRI, the entire energy sector had one of the lowest rates of private R&D investment of any part of the U.S. economy; in 1995, it was less than 0.5 percent of net sales. Industry R&D has declined since then, with EPRI's budget shrinking by about a third. And federally funded energy R&D spending dropped by about 40 percent between 1980 and 1995.

These electricity security institutions have done an admirable job of developing a power system in this country that is highly resistant to natural threats. It is not clear, however, that such voluntary cooperative organizations can continue to function adequately in a competitive environment. In other industries, such as transportation, the United States relies on government safety regulators, and companies tend to invest in more proprietary research. Further, standards designed to promote reliability in the face of weather and accidental equipment failures are not likely to be adequate in the face of well-organized assaults. Currently, it is unclear where responsibility and authority for restructuring lies. Several agencies argue that they have an important role to play: the Department of Energy, the Federal Bureau of Investigation, the Federal Energy Regulatory Commission, and the many state-level energy and law-enforcement bodies. Until this important institutional issue is sorted out, it will be impossible for the industry to develop a rational response.

In short, one of the key future challenges is ensuring that institutional solutions to emerging security problems are created for whatever new structure the electricity industry takes. This includes looking at threats that go beyond those considered in traditional contingency planning.

High-hazard facilities

Some parts of the electric power system, such as nuclear power sites, certain locks and dams, and fossil fuel storage locations, are tempting targets for terrorists. In addition, cooling towers in urban areas might be used to disseminate a chemical or biological agent into the atmosphere. These attacks could cause panic, deaths, or extensive property damage. Further, as testament to the power and technical sophistication of the United States, many of these facilities may tempt terrorists for their symbolic value.

Nuclear reactor containment buildings are massive structures designed to withstand significant impacts. However, no conclusive analysis shows that they and the reactor vessels they house can withstand a direct hit by a jumbo jet. Far more vulnerable are the buildings that house spent reactor fuel, which is currently stored in water-filled pools or aboveground containers at all operating reactor sites. These "temporary" facilities have grown because of the U.S. failure to develop a permanent high-level nuclear waste disposal site. The Bush administration has taken some steps to resolve this problem, but legal battles are expected to continue for some time. Even after the issue of secure long-term waste storage is resolved, it will still take a decade or more to complete the facility and move the waste into it, during which time the terrorist threat will remain.

Security programs in place around nuclear power plants frequently test them against simulated commando assaults. However, a 1999 Nuclear Regulatory Commission (NRC) review found "significant weaknesses" in 27 of the 57 plants that were evalu-

ated. Despite this poor performance, the nuclear energy industry has long sought reduced federal oversight of security planning and had planned to move toward a self-regulation model starting in mid-September 2002. The terrorist attacks have halted these plans temporarily, and the NRC and other federal organizations have ordered increases in security.

As the owners of high-hazard electricity facilities have begun to face competition and the bottom line has become more important, security costs have received greater scrutiny. Adequate institutions for the protection of high-hazard electricity facilities in the new competitive industry have yet to be developed.

A system with many small, scattered generators would be less vulnerable to attack.

New vulnerabilities

In contrast to the issues of physical security, electricity system planners have given less attention to cyber attacks on their real-time supervisory control and data acquisition (SCADA) systems that provide system status information and control its operation. SCADA technologies were originally designed as proprietary, stand-alone systems and often the specific technologies vary from company to company. Until several years ago, almost all of these functions were carried out with entirely private and highly secure communication links. More recently, dialup modems have been installed in some systems for remote monitoring and, in a few cases, for control. Greater interaction between public and secure communication networks occurs in a few systems; fiber optic capacity may be leased out, or the Internet may be used for communication or control. The widespread use of networking technologies has begun to transform SCADA systems; Internet-based applications are being used for SCADA and other functions, such as energy management. To further complicate matters, these systems are becoming open to more users as more companies participate in regional electricity markets and transmission-system operation.

This evolution has produced a troubling combination of older, secure systems; new, insecure uses for formerly stand-alone systems; and nearly wide-open Internet-based systems. Preparation for the successful Y2K rollover led to some improvements and upgrades, and provided a model for dealing with cyber threats in the electricity industry. However, private security consultants and the Department of Defense both report successfully penetrating electric power control systems. Some electric companies have inadequate security policies, including computer systems that allow for blank passwords. Again, because of unclear responsibilities and inadequate incentives, no adequate, systematic approach is being taken to address this problem.

In addition to the conventional modes of attack, some exotic scenarios also warrant consideration. For example, relatively simple, inexpensive devices that can deliver a very fast rise-time electromagnetic pulse (EMP) have been designed and tested by the United States and other nations. An EMP can induce instantaneous voltages of thousands of kilovolts in conductors, irreversibly damaging electrical and electronic devices. EMP has long been understood as an area-wide risk from nuclear weapons. Smaller, non-nuclear EMP weapons might be used on a much more localized scale to attack critical electric power system components, networked computers, and telecommunication systems, without physically penetrating facility perimeters. It is not clear how vulnerable the current system is to such an assault. Nor do we know what could be done to defend against them. More research is clearly needed.

During the past few years we have also begun to understand that the physical electric power system is just one part of a complex adaptive system that has strong interactive effects. Other parts include the SCADA systems that control the physical power system, the market data systems that plan its short-term operation, and the fuel delivery systems that keep it running. The tightness of these couplings, the specific mechanisms by which different networks are interdependent, and the ways in which these mechanisms can transmit faults from one network to another can vary greatly. For example, the fact that there is little electricity storage means that power could be cut off at any time, disrupting communications, gas

line compressors, and other systems that depend on electricity. Lack of power could also cause traffic lights to go out, slowing the arrival of emergency service vehicles. In contrast, the coupling between a coal-fired power plant and its the fuel supply system is fairly loose, because there are generally several weeks of fuel on site and multiple routes for obtaining additional fuel.

The increasing reliance on natural gas for electricity generation is increasing dependence on the gas transmission system. Fortunately, the gas system is harder to attack and more robust than the electric system, largely because it is buried underground and because gas can be stored in the transmission system and at relatively secure locations close to demand, such as in depleted oil and gas wells. And just like the electricity industry, gas companies have long recognized and effectively planned for contingencies designed to mitigate terrorism. Spare parts are generally kept on hand to effect quick repairs. However, problems in gas system maintenance were recently highlighted when internal corrosion caused a 30-inch gas pipe near Carlsbad, New Mexico, to rupture and explode in August 2000, killing 12 people. The explosion led to significant increases in gas prices in California, exacerbating the electricity crisis there. The National Transportation Safety Board subsequently determined that decades of inadequate testing and maintenance by the pipeline company caused the accident. This example shows that the interdependent systems that support the supply of electricity to the United States are not perfect, and that institutional mechanisms to support reliability and security may need to be strengthened. Moreover, only recently have analysts at DOE, the national labs, and EPRI begun to examine infrastructure interdependencies. Several of the strategic planning documents produced by the government during the past few years have pointed to this issue as one in particular need of fundamental and applied research.

Potential solutions

How might we deal with or mitigate the vulnerabilities in the electric power system? In recent years, the concept of survivability has emerged as a result of research and practice at the places such as the Software Engineering Institute at Carnegie Mellon University to counter Internet security threats. Survivability is the ability of a system to fulfill its mission in a timely manner, despite attacks, failures, or accidents. It is designed for "unbounded systems" that lack centralized control or global visibility and that typically are unable to distinguish between insiders and outsiders. Because of restructuring, the electric power industry must move toward a survivability approach to security.

A fundamental assumption of survivability analysis and design is that no individual component of a system is immune from attacks, accidents, or design errors. Thus, a survivable system must be created out of inherently vulnerable subunits, making survivability an emergent property of the system rather than a design feature for individual components.

Survivability resembles a quasi-biological model and has three components: resistance, recognition, and recovery. In unbounded systems, it is difficult to recognize attacks until there is extensive damage. Thus, ways must be found to recognize attack early and to protect the system without taking the time to discover the cause of the attack. Survivable systems must be able to maintain or restore essential services during an attack and to recover full service after the attack. In essence, the system must fail gracefully, shedding low-priority tasks and then adding tasks in order of priority during recovery. The current system for electric power supply and use generally doesn't use this approach, with a few exceptions, such as plants for systematic emergency load shedding and critical facilities such as hospitals that choose to invest in backup generators.

A simple example concerns traffic signals. In most cities, the same circuits that provide service to much less critical buildings and billboards also power traffic signals. During the rolling blackouts in California in 2000, one of the major causes of injury and property loss were crashes due to blank traffic signals. Worsening the problem, blackouts cause gridlock that prevents police and fire vehicles, as well as emergency response crews, from reaching their destinations. Fortress-type thinking creates a system in which blackouts are never supposed to occur, but when they do, the consequences are severe. In contrast, a system designed with survivability concepts might use commercially available low-power LED traffic lights with uninterruptible power (such as trickle charge batteries) to ensure that a blackout did not in-

terrupt traffic flow. There would be a cost to doing this, but it might well be lower than the cost of disruption and of stationing police at intersections at a time when they are needed elsewhere.

One relatively straightforward solution to some security concerns would be to eliminate high-hazard facilities, such as dams and on-site storage of spent nuclear fuel. This is feasible for a few potential targets but would require time to implement and would likely make electricity much more expensive, because nuclear energy and hydropower make up well over a quarter of the nation's electricity supply. Some selective retrofitting makes sense, and certainly devoting greater consideration to vulnerabilities to terrorism makes a great deal of sense for new investments. However, progress in reducing overall vulnerability will clearly be slow.

Congress, at a minimum, must assign clear responsibility for oversight and coordination to a single entity.

The current electricity system with its large, central generators and long transmission and distribution lines is inherently vulnerable. In contrast, a system with many small generators located at large customers or in neighborhoods could be made much less vulnerable. These systems would still be grid-connected but could operate when the grid went down. A variety of existing and emerging technologies make it possible to design power systems based on distributed generation (DG). DG units are attractive because they produce electric power onsite to supplement or serve the grid and because they recover waste heat for use onsite, making them more efficient than central station generation, which dumps waste heat. Small-scale renewable forms of energy such as wind and solar may also hold promise, because they eliminate the need for fuel. However, solar-electric technologies are still expensive, not all locations have a good renewable resource base, and even those with an adequate base face intermittent supply problems, because the wind does not always blow nor the sun always shine.

Fossil-fueled DG is no longer a fringe idea. Equipment manufactures such as ABB and Capstone are building business plans around these technologies. In some countries, the installed capacity of DG is becoming quite large. For example, in the Netherlands, distributed generation units of less than 1 megawatt now constitute about 6 percent of installed electrical capacity.

In the United States, many electricity providers have opposed DG, believing that it undermines their large investments in central generation and transmission facilities and threatens their core competencies in these areas. Despite laws requiring easy DG interconnection, a number of regulatory and commercial barriers have been used to block many proposed DG installations. A major reason for the success of DG in the Netherlands was the breakup of vertically integrated power providers, which barred distribution companies from owning large-scale generation but allowed them to participate in DG. This is another example in which institutional and regulatory choices will be critical to the feasibility of technical solutions to electric power system security.

Implications of restructuring

Industry deregulation and restructuring dominate all other issues in the electric power industry today, strongly modifying successful business models. Adequate solutions to the problems of security and survivability of the electric power system in the face of terrorist threats will simply not be possible without an adequate resolution of several basic restructuring problems.

The U.S. electric power industry developed as a collection of regulated, vertically integrated companies, each of which had responsibility for its own area. The companies were only loosely connected, because each tended to generate, transmit, and distribute electricity only within its own service territory. This system enhanced security by making it difficult for an attack to spread to other companies. Because companies tended to use different communication technologies and protocols, the risks of cyber attacks were limited. Finally, the legal framework and social culture of regulated monopoly electricity suppliers tended to place a great emphasis on pro-

viding reliable service to customers; cost was less important because it could be passed along in regulated rates to captive consumers.

Restructuring changes virtually all of this. It tends to relieve generators of any obligation to meet demand now or in the future, and so far it has left the future ownership and cost recovery of the transmission system very unclear. As in California, it can leave retail providers with the obligation to serve customers but without the assets to do so themselves. Restructuring relies on market forces to resolve supply and demand issues. Markets tend to do this very well when the rules are clear and well-designed. Electricity market structures today are neither stable nor clear—nor, it seems, well-designed in all cases.

So far we've been lucky. Summer weather has been mild for the most part during the past few years, stressed components have not failed, and no well-organized terrorist group has attacked the electric power system. But the time to get adequate institutional arrangements into place is quickly running out. In Congress, general security legislation and industry-restructuring bills have major implications for security in the electricity sector. The tightening of security nationwide after September 11 included increased vigilance at some electricity facilities, and the counterterrorism legislation (the USA Patriot Act) passed in October will significantly increase the federal government's ability to track and disrupt potential terrorists. In addition, the new law states that actions necessary to achieve the new security policy will be carried out by a public-private partnership involving corporate and nongovernmental organizations. It remains to be seen how this provision will be implemented.

More than 40 restructuring bills have been introduced in the current Congress; about a half-dozen of them have provisions associated with reliability, generally creating mandatory, private reliability organizations. For the most part, these bills do not address security issues, although Title 18 of the proposed Energy Policy Act of 2002 (S.1766) authorizes the secretary of energy to establish programs of various sorts to improve critical energy infrastructure. There are likely to be more such efforts as industry presses for more action, including insurance subsidies and protection from lawsuits, exemption from some antitrust and information laws, federal power of eminent domain for transmission lines, and guaranties of cost recovery for security-related expenses.

Congress must sort out the confusing multiplicity of interests that different agencies have in counterterrorism and, at a minimum, assign clear responsibility for oversight and coordination to a single entity that understands the multifaceted nature of the electric power system and the need to balance security and other interests. Whether more than that would be appropriate is less clear. Although it is tempting to suggest consolidating decisionmaking authority in a single federal security agency, such a move would dramatically expand federal power into areas that have been the responsibility of the states. Either way, additional federal funding will be needed to cover the costs of some of the necessary upgrades, because many such investments will not serve the private needs of the industry.

Recommended Reading

Lipson, H., D. Fischer, (1999). *Survivability—A new technical and business perspective on security.* Proceedings of the New Security Paradigms Workshop. Caledon Hills, ON: ACM.

Morgan, M.G. and S.F. Tierney. (1998) Research Support for the Power Industry. *Issues in Science and Technology*, 1998. Fall: p. 81-87.

Rinaldi, S.M., J.P. Perenboom, and T.K. Kelly. (2001) *Critical Infrastructure Interdependencies.* IEEE Control Systems: 11-25.

Zerriffi, H., H. Dowlatabadi, and N.D. Strachan. (2002) Electricity and Conflict: The Robustness of Distributed Generation. *Electricity Journal*. forthcoming.