

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 Electric-

ity 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.

However, there is more to be learned from the study of past outages. Contingency planning, spare equipment preplacement, emergency preparedness

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,

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.

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 com-

na(protectoITw)39rity

stand-alone ;[(SCANvernd l. Ttion be-)Tj T 0.010309c 0.01comin(tems; Internet-alone . Prepana(protutions ctition 30

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. Surviv-

ability 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, and recovery

Tscovurr22 Tw (denesult of)TJ T* -0.0004 Tc 0.(
r thnted tal0 Tw , we deathe pexTw [al s,e placesservices
aldesign choost be invain of fun-

interrupt 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

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 pro-

posed 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 guarantees 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*