

Electric Power System Is Called Vulnerable, and Vigilance Is Sought

Ref: New York Times, 28 Feb 2002

<http://www.nytimes.com/2002/02/28/national/28SECU.html>

by Matthew L. Wald

ENOX, Mass., Feb. 27 - The computers that control the electric power system around the nation have been probed from the Middle East, and terrorists may have inspected the physical equipment, said experts at a conference on the security of the electric system.

Government experts identified nuclear power plants as perhaps the most attractive targets but said dams, gas pipelines and oil refineries were not far behind. Federal officials urged companies that generate, transmit and distribute electricity to take steps to increase security. "In a single-superpower world, there's a single best target," said Lt. Col. Bill Flynt, director of the Threats to Critical Infrastructures program at the Foreign Military Studies office of the Army.

"You're the best face of that best target," Colonel Flynt told the power officials. "Your corporations are the best target set." But the extent of the threat, and of the vulnerability, was not clear from the unclassified two-day conference, where a panel of government and industry experts refused to provide details about what they knew or how they knew it.

The electric system is set up to perform reliably even with significant component failures and to recover quickly from those failures. But it might not stand up to multiple coordinated attacks, and the Sept. 11 attacks demonstrated that such an event was possible. Some parts of the system, like transformers, are large, require months to build and are not held in inventory in an increasingly competitive industry that shuns expensive spares, experts said.

The conference brought together about 60 plant managers, power system administrators, state regulators and other experts from New York and New England to hear from officials of the F.B.I., the C.I.A. and state governments. The industry officials showed some frustrations about the murkiness of federal advice.

For example, James D. Castle, manager of operations at the New York Independent System Operator, or ISO, said the system was usually operated by running the cleanest and least expensive generating stations. But the system could be less vulnerable if plants close to the high demand cities were started up, to minimize the importance of transmission lines.

Mr. Castle, who is also the chairman of the Northeast Power Coordinating Council, which covers New York, New England, Ontario, Quebec and the Maritimes, said there was no consensus on when to do so. Members of the council have a once-a-week conference call on terrorist threats, he said, and have developed code words to discuss what actions to take to protect the power system from terrorist threat. The problem, he said, was that threats thus far have been vague.

"Is it really enough for me to change the way I run the power system, in other words, to pollute the air, and cost people money? Probably not," Mr. Castle said.

James Fortune, a program manager at the Electric Power Research Institute, a utility research consortium based in Palo Alto, Calif., said that computers used by a variety of critical industries had been probed by unknown intruders.

"We do know that surveillance has increased, from the Middle East," Mr. Fortune told the industry executives. "Where do you think the majority of those probes have gone? To us, the overall energy system," he said. In an interview, he said this had been verified by a computer security firm, but he would not give further details.

"Are they surveilling now? That's what you do before you launch an attack," Mr. Fortune said, and he urged the participants to re-examine their computers.

Another speaker, Harvey Blumenthal, a C.I.A. official who is on loan to the National Infrastructure Protection Center, a federal agency created by President Bill Clinton, said a review of reports received by the federal government since Sept. 11 showed that electric installations "are under active physical surveillance."

"The bulk of these reports have been discounted as being not credible," Mr. Blumenthal said. "However, there are a few that really may represent an attempt to collect useful intelligence, operational information that could presage future attacks."

Charles E. Noble, the director of Information Technology Security at the ISO New England, the independent system operator for the six-state region, pleaded with the people who run power plants and transmission and distribution systems to report anything they saw so the reports could be analyzed and integrated, with help from the North American Electric Reliability Council, known as NERC.

"If you see suspicious people around, report it," Mr. Noble said. "The nuclear sites and some of the others, if you see airplanes flying around, report it. There's no way at the ISO level, NERC or the federal level we can respond if we don't know what's going on out there."

The conference was sponsored by the New York and New England independent system operators. It was held in the Cranwell Resort and Golf Club here, a complex of stately old buildings that have been recently restored and remodeled; as if to emphasize the centrality of electricity to American life, even the soap and paper towel dispensers in the restrooms at the conference center ran on electricity.

The electricity executives got a pep talk from James K. Kallstrom, the New York State director of public security, who said that a loss of electric service would have "a dramatic major impact to every facet of our economy." But speaking of the power plants and transmission lines, he added, "we have not built these things with the condition we have today in mind."