Thousands Seen Dying If Terrorists Attack U.S. Power Grid

By Brian Wingfield and Jeff Bliss - Nov 14, 2012 2:17 PM MT Bloomberg

A terrorist attack on the U.S. power grid could be more destructive than superstorm Sandy, possibly costing hundreds of billions of dollars and leading to thousands of deaths, the National Academy of Sciences said.

While such an event probably wouldn't kill people immediately, it could cause widespread blackouts for weeks or months, according to a recently declassified report released today by the Academy. If it occurred during extreme weather, heat stress or exposure to cold may lead to "hundreds or even thousands of deaths," the authors of the study wrote.

"An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness that would play directly into the hands of the terrorists," they said.

While other entities have issued reports on electric-grid vulnerabilities, the study released today provides an unusually stark picture of what might happen if hackers, extremist groups, disgruntled employees or even energy companies sabotage the nation's power network. It calls for the government to create a national inventory of portable generation equipment that can be used during such an event.

An attack "could be carried out by knowledgeable attackers with little risk of detection or interdiction," it said.

2007 Study

The study released today by the National Academy of Sciences was sponsored by the Department of Homeland Security and completed by the National Research Council, which is part of the National Academy of Sciences. Although the report was finished in 2007, President George W. Bush's administration a year later prevented it from being distributed publicly. The panel of experts who prepared the report, believing it contained no classified information, pressed for its dissemination. In August, the administration of President Barack Obama agreed to declassify most of the study.

National Academy of Sciences President Ralph J. Cicerone, and Charles M. Vest, president of the National Academy of Engineering, in a forward to the report, said its key findings remain "highly relevant." The men also are chairman and vice chairman, respectively, of the National Research Council.

Complicated Web

The U.S. electricity network consists of a complicated web of generators, high-voltage power lines, lower voltage lines that run to homes and businesses, substations and other gear to keep electricity flowing smoothly across the country. The National Academy of Engineering called the transmission and distribution system, or the grid, "the world's largest integrated machine."

Since 2007, the increased use of computerized systems, including so-called smart meters -- which give consumers greater control over their energy use -- highlights the need for vigilance against cyber attacks, David Owens, executive vice president of business operations at the Edison Electric Institute and a contributor to the study, said in a phone interview.

"The grid is changing," Owens said.

Threats to the network also include physical attacks on equipment that is often decades-old and lacks the technology to limit the effects of such an event, the study said.

Multiple Attacks

While a hurricane or ice storm usually only takes down distribution lines that utility crews can put back up, terrorists can disable transformers, which may take years to replace, said Alan Crane, a senior scientist who worked on the report. A well-planned operation could take out several substations, he said.

"It's the multiple attacks that have the really scary consequences," Crane said. Although the probability of such a conspiracy is low, the consequences "could just be really awful."

The report raises questions about how a blackout would affect services including medical care, the water supply and the pumping of natural gas, which uses compressors powered by electricity, he said.

"Living without electricity is one thing," Crane said. "Living without water is something else."

An attack could inflict more damage than superstorm Sandy, which roared across the Eastern U.S. at the end of October, according to a statement released with the study. The storm temporarily tripped power to three nuclear reactors and caused a fourth, owned by Exelon Corp. (EXC), to declare an alert.

Insured losses from the disaster will probably exceed $20 billion, according to QBE Insurance Group Ltd. (QBIEY), which had a 3.5 percent share of U.S. commercial property insurance during the second quarter.

High-Voltage Transformers

“High-voltage transformers are of particular concern because they are vulnerable to attack, both from within and from outside the substation where they are located,” according to the report. Transformers are often custom-built, difficult to transport because of their size, and made outside the U.S., meaning that the industry’s inventory could be “overwhelmed by a large attack,” it said.

The Edison Electric Institute, a Washington-based industry group for publicly traded utilities including Duke Energy Corp. (DUK) and Southern Co. (NSC), is leading a pilot program to install spare transformers at sites where they can be transported for use in the event of an emergency, Owens said.

Exacerbating the risk to the grid is a patchwork of energy- market structures, established since the 1990s to spur competition, according to the study.

Network Stress

“The push by federal regulators to introduce competition in bulk power across the country has also resulted in the transmission network being used in ways for which it was not designed,” the study’s authors wrote.

A 2005 U.S. energy law included measures to strengthen the power grid’s reliability, and the Federal Energy Regulatory Commission now has the ability to issue fines as high as $1 million per day for each reliability violation.

Cyber attackers “could magnify the damage of a physical attack” by disabling computerized security systems or blocking signals to grid operators, the report said.

Other threats to the grid may include terrorist groups, disgruntled or bored individuals, or energy companies seeking to thwart competitors, it said. A 2011 report from the Electric Power Research Institute said that about $3.7 billion in investment is needed to protect the grid from cyber attacks.

Increased Investment

Energy companies including utilities would have to increase their investment in computer security more than seven-fold to reach an ideal level of protection, according to a January survey done for Bloomberg Government by the Ponemon Institute LLC, a data-security research firm based in Traverse City, Michigan. The survey of network managers at 21 energy companies including 14 utilities found the companies would need an average annual budget of $344.6 million to stop 95 percent of their cyber threats.

The report released today recommends that the Homeland Security Department take the lead in overseeing electric-grid security, working with the Energy Department and private

companies to create a stockpile of mobile reserve equipment, including transformers, for the network. It also calls for the security agency to work with the FERC, state regulators, utilities and grid operators to make sure they have “appropriate incentives” to upgrade the system.

The release of the report will speed the adoption of new technology that will better protect the grid, Cicerone and Vest said.

Utilities including American Electric Power Co. (AEP) of Columbus, Ohio, have already been working together to share cyber-threat information learned from software developed by Lockheed Martin Corp. (LMT)