THE WALL STREET JOURNAL.

A GAME CHANGER

PERSONAL JOURNAL | D1

Justice Ginsburg's Exit Interviews

OPINION | A10

DOW JONES | News Corp ** THURSDAY, JULY 14, 2016 ~ VOL. CCLXVIII NO. 11 WSJ.com ★★★ $3.00

..... A7

Ms. May, who assumed the ... was named foreign secretary. Please see MAY page A7

Please see VIACOM page A2

es

VANIA

45

36

848

JOURNAL.

in Ohio

find. A4

POWER GRID LEFT EXPOSED TO SABOTAGE

Recent attacks show thousands of electrical substations lack defenses

By Rebecca Smith

An early morning passerby phoned in a report of two people with flashlights prowling inside the fence of an electrical substation in Bakersfield, Calif. Utility workers from Pacific Gas & Electric Co. later found cut transformer wires.

The following night, someone slashed wires to alarms and critical equipment at the substation, which serves 16,700 customers. A guard surprised one intruder, who fled. Police never learned the identities or motive of the burglars.

The Bakersfield attacks last year were among dozens of break-ins examined by The Wall Street Journal that show how, despite federal orders to secure the power grid, tens of thousands of substations are still vulnerable to saboteurs.

The U.S. electric system is in danger of widespread blackouts lasting days, weeks or longer through the destruction of sensitive, hard-to-replace equipment. Yet records are so spotty that no government agency can offer an accurate tally of substation attacks,

Please see GRID page A8

GRID

Continued from Page One

whether for vandalism, theft or more nefarious purposes.

Most substations are unmanned and often protected chiefly by chain-link fences. Many have no electronic security, leaving attacks unnoticed until after the damage is done. Even if there are security cameras, they often prove worthless. In some cases, alarms are simply ignored.

The vulnerability of substations was revealed in a Journal account of a 2013 attack on PG&E's Metcalf facility near San Jose, Calif. Gunmen knocked out 17 transformers that help power Silicon Valley; a blackout was narrowly averted. The assailants were never caught.

The following year, the Federal Energy Regulatory Commission, which regulates the country's interstate power system, began requiring that utilities better protect any substation that could disable parts of the U.S. grid if attacked.

FERC's new rule, however, doesn't extend to tens of thousands of smaller substations, including Metcalf and the one in Bakersfield. Security experts say a simultaneous attack on several of these substations also could destabilize the grid and cause widespread blackouts.

Gerry Cauley, head of the North American Electric Reliability Corp., —which writes standards for the grid—was asked at a FERC hearing in June on grid security what kept him up at night. He said the prospect of "eight or 10 vans going to different sites and blowing things up." Recovery from a coordinated attack, he said, could take weeks or months.

The Metcalf substation, while undergoing security upgrades, was hit again in August 2014. Intruders cut through fences and burglarized equipment containers, triggering at least 14 alarms over four hours. Utility employees didn't call police or alert guards, who were stationed at the site, according to a state inquiry.

Three days after the break-in, Stephanie Douglas, PG&E's senior director of corporate security, sent a memo to the utility's president saying security was in a fail mode, and her department lacked clout and resources: She had 26 full-time jobs to protect 900 substations, as well gas pipelines and other utility assets.

Ms. Douglas, no longer with PG&E, declined an interview request. PG&E spokesman Matt Nauman said the utility has responded with a $200-million program that includes better security equipment, more training and hiring.

The U.S. electric system is in danger of widespread and prolonged blackouts.

The sprawling U.S. electric system is regulated by government but mostly owned and operated by utility companies and grid operators that monitor electricity supply and demand every minute, every day. The system is always on—and for years few thought anyone would try to turn it off.

The motive of most substation break-ins appears to be theft. Intruders and, potentially, terrorists also could be trying to hack into control systems through computer equipment in substations—either to cause immediate damage or to gather information for later use.

"A substation is not an obvious target for criminals like a bank," said Joseph Weiss, a security consultant to utilities. "Common sense says they want to get into the electric system."

Complex system

The U.S. power grid is like a giant puzzle that can be configured in different ways to deliver power where and when it is needed.

Major power sources—gas-fired generators and nuclear-power plants, for example—connect to substations that raise voltages to ferry electricity long distance over a network of power lines. At cities and other destinations, substations lower the voltage to safely deliver electricity to homes and businesses. Substation computers help grid operators control those electrical flows.

The grid was cobbled together during the electrification of the U.S. over the past 125 years. It is a fragile, interdependent system generally more vulnerable in summer when it is running closer to its limits. It is also at risk during low-demand periods, when power-plant operators and linemen perform maintenance. Fewer plants and transmission lines operating mean fewer options for delivering electricity during emergencies.

There is so much variability in the grid that what causes a catastrophe one day might not the next, which makes security issues complex. Small problems can quickly spiral out of control.

On Sept. 8, 2011, equipment problems and human error caused a large transmission line in Arizona to trip out of service. The grid is supposed to withstand the loss of any one line. On this day, electric current shifted to nearby lines and overloaded them; that overtaxed transformers at two small substations, which shut down defensively to prevent equipment damage, and disruptions spread.

San Diego was blacked out 11 minutes later. Traffic snarled. Flights were canceled. Raw sewage flowed into the ocean. Altogether, 2.7 million utility customers lost power in California, Arizona and Mexico.

Federal officials have long known about the vulnerability of electrical substations. A 1990 report from the federal Office of Technology Assessment warned that "virtually any region would suffer major, extended blackouts if more than three key substations were destroyed."

A 2012 report from the National Research Council of the National Academies of Sciences looked at different parts of the electric system and concluded that substations were "the most vulnerable to terrorist attack."

"We've known we had an issue for a long time and have been very slow to do anything about it," said M. Granger Morgan, a professor of engineering at Carnegie Mellon University who studied the San Diego blackout.

Security adviser James Holler said his company, Abidance Consulting, inspected nearly 1,000 substations over the past year for utilities in 14 states. "At least half had nothing but a padlock on the gate," he said. "No cameras. No motion sensors or alarms."

One utility lost a set of substation keys that were in a truck stolen for a joy ride. After the truck and keys were recovered, Mr. Holler said, the utility didn't change the substation locks.

Richard Donohoe, director of security for the consulting firm Black & Veatch, said the security departments of utility companies are often so low in the pecking order that "the rest of the organization ignores them half the time."

After the attack on the Metcalf substation, FERC required better protection for individual substations "that if rendered inoperable or damaged could result in widespread instability," or cascading blackouts in any of the three separate sections of the U.S. power grid.

That is a high bar. Utility experts aren't sure how many substations the new rules cover but estimate it is fewer than 350 out of approximately 55,000. They say more protections are needed at smaller substations that could trigger blackouts if attacked in combination.

The exact combinations depend on energy demand and the direction of electricity flow. In spring, for example, hydroelectric power plants send electricity from the Pacific Northwest to California. In winter, electricity flows in the opposite direction, mostly from gas-fired and nuclear power plants in California and Arizona.

One security-focused nonprofit group called the Foundation for Resilient Societies has called for an analysis of the impact of simultaneous attacks, both physical and cyber.

Thomas Popik, chairman of the group, told FERC in June that existing grid protections were inadequate and his group believed the grid was "a battlefield of the future" that required military-type defenses for key infrastructure.

Michael Bardee, director of the Office of Electric Reliability at FERC, said the agency could do more to study security vulnerabilities at the thousands of substations not covered by the new rule. FERC expects a progress report on the new rule later this year.

"Clearly, there's some sense that as events go on we may need to re-evaluate the applicability of this standard," Mr. Bardee said, and possibly expand its reach.

The Vermont Electric Power Co. approved a $12 million program to beef up security at 55 locations after substations were penetrated more than a dozen times by thieves stealing copper during break-ins from 2012 through early 2014.

"We haven't seen a theft in over a year," said Kerrick Johnson, a spokesman. The utility installed more secure fencing and better security cameras.

Most utilities are reluctant to spend money on security unless under government orders. They must justify their expenses to regulatory agencies to pass on the costs to ratepayers, said John Kassakian, an emeritus professor of electrical engineering at the Massachusetts Institute of Technology.

Security upgrades generally include cameras, lights and motion sensors, as well as password-controlled doors and gates that electronically monitor entries and exits. Terror threats, Mr. Kassakian said, probably seem less pressing than spending to comply with federal environmental rules.

Alarms unheeded

Utilities don't always report attacks despite a legal requirement to notify the Energy Department within six hours of any event that could interrupt electricity or if a break-in targets security systems.

No utility has been fined for failing to comply as far as he knew, said David Ortiz, deputy assistant secretary at the Energy Department: "I don't have an enforcement team."

The Journal found nine substation break-ins over the past two years where theft wasn't the apparent motive. The tally and details of the break-ins were gleaned from interviews and public records requests. The count included attacks affecting the federally owned Liberty substation in Buckeye, Ariz.

The substation, about 35 miles west of Phoenix, is a critical link in the southwest power corridor, delivering electricity to heat homes in northwestern states during winter and cool buildings in the southwest during summer.

On Nov. 5, 2013, someone slashed fiber-optic cables that serve Liberty, as well as the larger Mead substation near Hoover Dam. It took workers about two hours to re-establish proper communications and normal controls.

Liberty is operated by the Western Area Power Administration, which controls 17,000 miles of high-voltage power lines used by utilities serving 40 million people in 15 states. If this system suffered a catastrophic failure, it would take down other utilities with it, experts said.

Alarms signaling trouble at Liberty began ringing at a utility operations center in Phoenix 13 days after the communications outage. Dozens of alarms sounded over two days before an electrician was dispatched.

The electrician expected a false alarm. Instead, he found the perimeter fence sliced open and the steel door to the control building "peeled back like a sardine can," said Keith Cloud, the utility's head of security.

The substation's computer cabinets were pried open. The substation's security cameras proved useless: eight of 10 were broken or pointed at the sky, Mr. Cloud said. Most had been out of operation for a year or more.

Two months later, on Jan. 30, 2014, Liberty was hit again. Two men with a satchel cut the gate lock and headed to the control building. They left after trying, unsuccessfully, to cut power to a security trailer outfitted with cameras and blinking lights, which were installed after the first break-in.

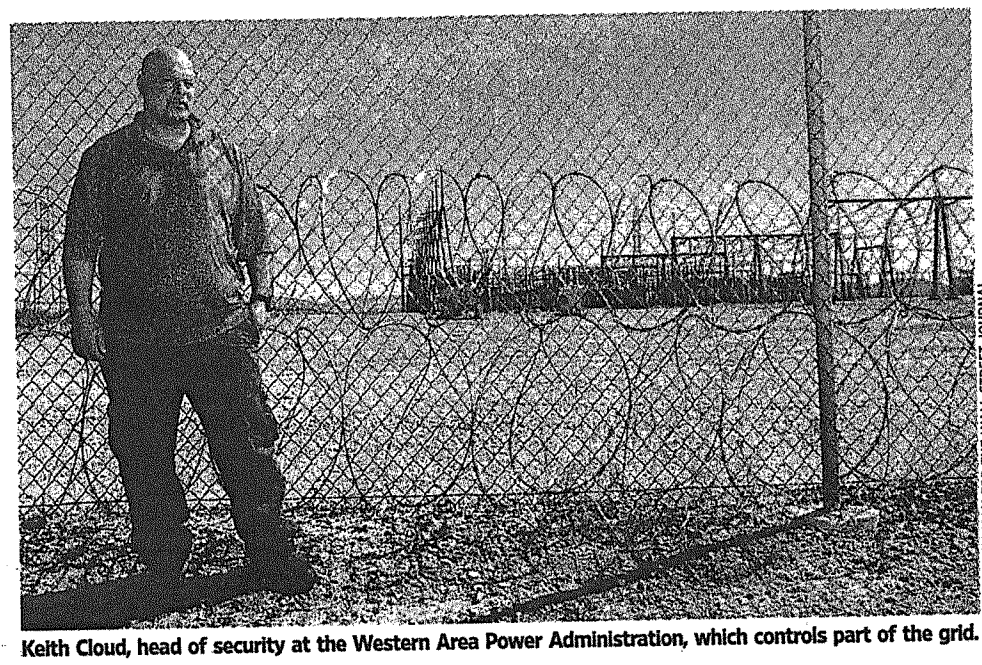
This time, Mr. Cloud said, utility officials found 16 of 18 security cameras had failed. Most were installed after the first break-in and hadn't been properly programmed. Investigators retrieved a single fuzzy video from a thermal-imaging camera.

Mark Gabriel, WAPA's administrator, said the utility has "taken steps to improve our physical security program and processes," including creating the security department in 2013 that Mr. Cloud now heads.

A federal audit faulted WAPA in April for violations of security regulations, including broken or obsolete equipment, lax control over keys to critical substations and failure to install intrusion-detection systems.

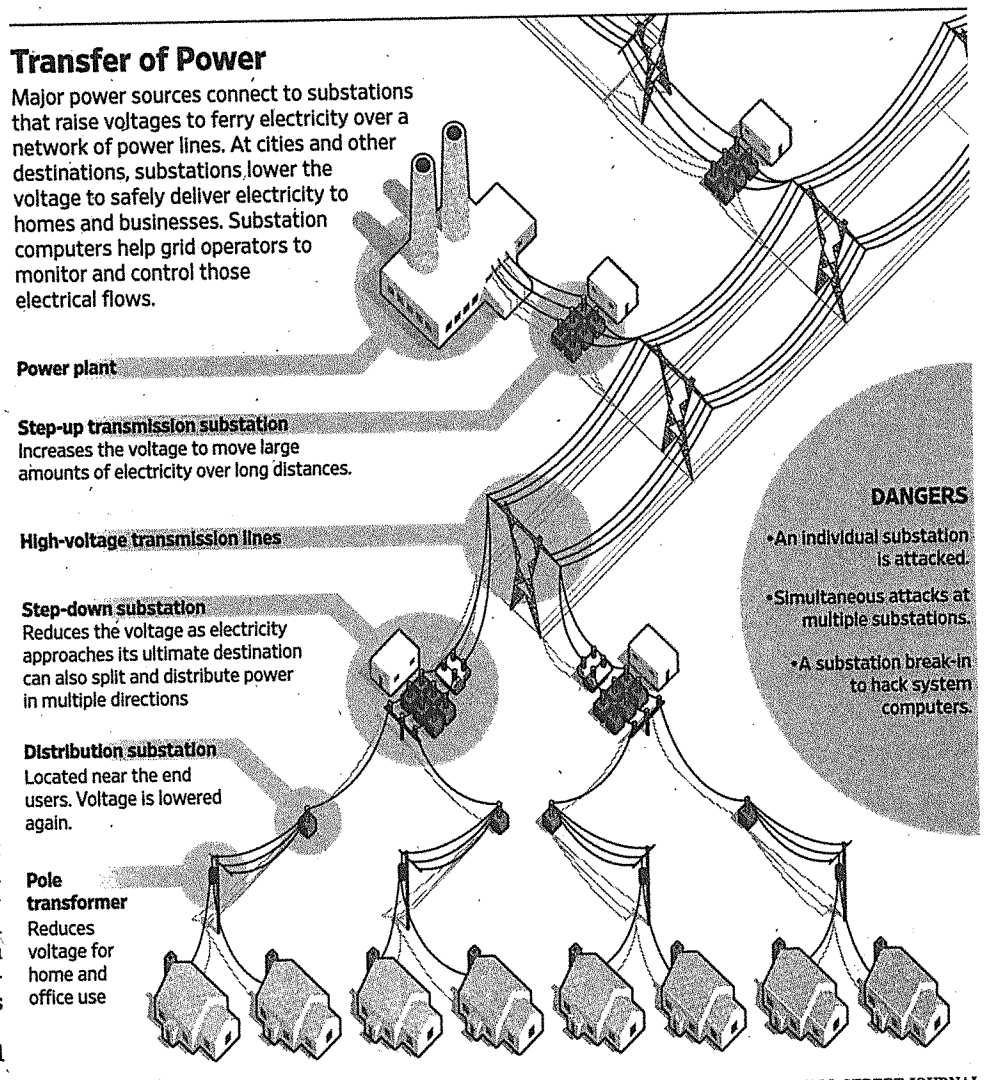
Mr. Gabriel said WAPA spends a couple of hundred million dollars on capital improvements annually, which includes money for security improvements. "The bigger story is how that break-in and others in the industry changed the thinking," he said.

Mr. Cloud said he has received about $300,000 for security upgrades at a handful of WAPA's 328 substations, including Liberty. To protect the system's 40 most important substations and control centers, he said, he needs $90 million: "I don't have the authority or budget to protect my substations."



MARK PETERMAN FOR THE WALL STREET JOURNAL

Keith Cloud, head of security at the Western Area Power Administration, which controls part of the grid.



Source: Energy Information Administration.

THE WALL STREET JOURNAL.