Electricity Grid in U.S. Penetrated By Spies
By SIOBHAN GORMAN
April 8, 2009

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.

"The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians."

The espionage appeared pervasive across the U.S. and doesn't target a particular company or region, said a former Department of Homeland Security official. "There are intrusions, and they are growing," the former official said, referring to electrical systems. "There were a lot last year."
Question of the Day

Many of the intrusions were detected not by the companies in charge of the infrastructure but by U.S. intelligence agencies, officials said. Intelligence officials worry about cyber attackers taking control of electrical facilities, a nuclear power plant or financial networks via the Internet.

Authorities investigating the intrusions have found software tools left behind that could be used to destroy infrastructure components, the senior intelligence official said. He added, "If we go to war with them, they will try to turn them on."

Officials said water, sewage and other infrastructure systems also were at risk.

"Over the past several years, we have seen cyberattacks against critical infrastructures abroad, and many of our own infrastructures are as vulnerable as their foreign counterparts," Director of National Intelligence Dennis Blair recently told lawmakers. "A number of nations, including Russia and China, can disrupt elements of the U.S. information infrastructure."

Officials cautioned that the motivation of the cyberspies wasn't well understood, and they don't see an immediate danger. China, for example, has little incentive to disrupt the U.S. economy because it relies on American consumers and holds U.S. government debt.

But protecting the electrical grid and other infrastructure is a key part of the Obama administration's cybersecurity review, which is to be completed next week. Under the Bush administration, Congress approved $17 billion in secret funds to protect government networks, according to people familiar with the budget. The Obama administration is weighing whether to expand the program to address vulnerabilities in private computer networks, which would cost billions of dollars more. A senior Pentagon official said Tuesday the Pentagon has spent $100 million in the past six months repairing cyber damage.

Overseas examples show the potential havoc. In 2000, a disgruntled employee rigged a computerized control system at a water-treatment plant in Australia, releasing more than 200,000 gallons of sewage into parks, rivers and the grounds of a Hyatt hotel.

Last year, a senior Central Intelligence Agency official, Tom Donahue, told a meeting of utility company representatives in New Orleans that a cyberattack had taken out power equipment in multiple regions outside the U.S. The outage was followed with extortion demands, he said.

The U.S. electrical grid comprises three separate electric networks, covering the East, the West and Texas. Each includes many thousands of miles of transmission lines, power plants and substations. The flow of power is controlled by local utilities or regional transmission organizations. The growing reliance of utilities on Internet-

based communication has increased the vulnerability of control systems to spies and hackers, according to government reports.

The sophistication of the U.S. intrusions -- which extend beyond electric to other key infrastructure systems -- suggests that China and Russia are mainly responsible, according to intelligence officials and cybersecurity specialists. While terrorist groups could develop the ability to penetrate U.S. infrastructure, they don't appear to have yet mounted attacks, these officials say.

It is nearly impossible to know whether or not an attack is government-sponsored because of the difficulty in tracking true identities in cyberspace. U.S. officials said investigators have followed electronic trails of stolen data to China and Russia.

Russian and Chinese officials have denied any wrongdoing. "These are pure speculations," said Yevgeniy Khorishko, a spokesman at the Russian Embassy. "Russia has nothing to do with the cyberattacks on the U.S. infrastructure, or on any infrastructure in any other country in the world."

A spokesman for the Chinese Embassy in Washington, Wang Baodong, said the Chinese government "resolutely oppose[s] any crime, including hacking, that destroys the Internet or computer network" and has laws barring the practice. China was ready to cooperate with other countries to counter such attacks, he said, and added that "some people overseas with Cold War mentality are indulged in fabricating the sheer lies of the so-called cyberspies in China."

Utilities are reluctant to speak about the dangers. "Much of what we've done, we can't talk about," said Ray Dotter, a spokesman at PJM Interconnection LLC, which coordinates the movement of wholesale electricity in 13 states and the District of Columbia. He said the organization has beefed up its security, in conformance with federal standards.

In January 2008, the Federal Energy Regulatory Commission approved new protection measures that required improvements in the security of computer servers and better plans for handling attacks.

Last week, Senate Democrats introduced a proposal that would require all critical infrastructure companies to meet new cybersecurity standards and grant the president emergency powers over control of the grid systems and other infrastructure.

Specialists at the U.S. Cyber Consequences Unit, a nonprofit research institute, said attack programs search for openings in a network, much as a thief tests locks on doors. Once inside, these programs and their human controllers can acquire the same access and powers as a systems administrator.

NERC Letter

The North American Electric Reliability Corporation on Tuesday warned its members that not all of them appear to be adhering to cybersecuirty requirements. Read the letter.

The White House review of cybersecurity programs is studying ways to shield the electrical grid from such attacks, said James Lewis, who directed a study for the Center for Strategic and International Studies and has met with White House reviewers.

The reliability of the grid is ultimately the responsibility of the North American Electric Reliability Corp., an independent standards-setting organization overseen by the Federal Energy Regulatory Commission.

The NERC set standards last year requiring companies to designate "critical cyber assets." Companies, for example, must check the backgrounds of employees and install firewalls to separate administrative networks from those that control electricity flow. The group will begin auditing compliance in July.

—Rebecca Smith contributed to this article.

Write to Siobhan Gorman at siobhan.gorman@wsj.com

Corrections & Amplifications

Central Inteligence Agency official Tom Donahue's last name was misspelled in a previous version of this article.

Printed in The Wall Street Journal, page A1