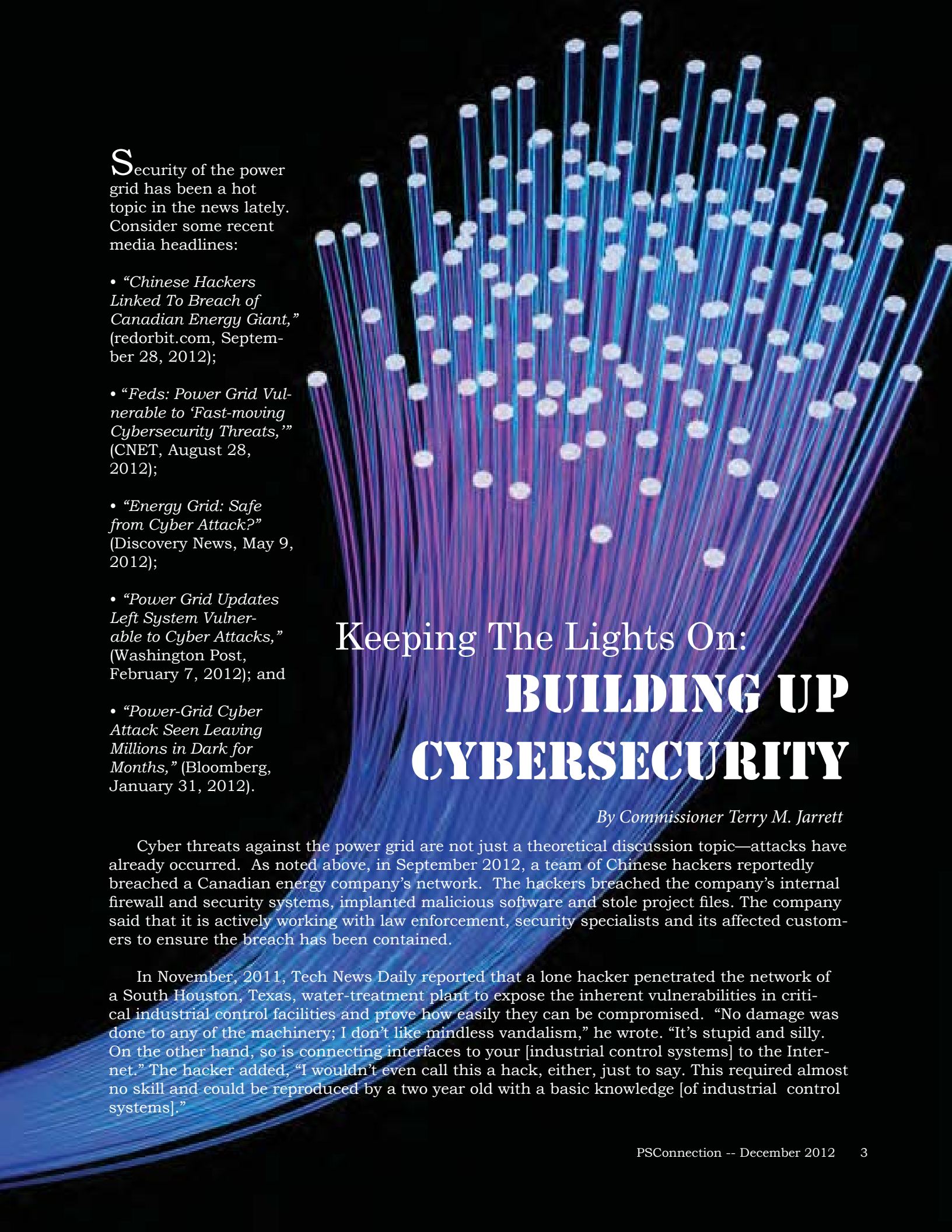

Security of the power grid has been a hot topic in the news lately. Consider some recent media headlines:

- *"Chinese Hackers Linked To Breach of Canadian Energy Giant,"* (redorbit.com, September 28, 2012);
- *"Feds: Power Grid Vulnerable to 'Fast-moving Cybersecurity Threats,'"* (CNET, August 28, 2012);
- *"Energy Grid: Safe from Cyber Attack?"* (Discovery News, May 9, 2012);
- *"Power Grid Updates Left System Vulnerable to Cyber Attacks,"* (Washington Post, February 7, 2012); and
- *"Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months,"* (Bloomberg, January 31, 2012).

Keeping The Lights On: BUILDING UP CYBERSECURITY

By Commissioner Terry M. Jarrett

Cyber threats against the power grid are not just a theoretical discussion topic—attacks have already occurred. As noted above, in September 2012, a team of Chinese hackers reportedly breached a Canadian energy company's network. The hackers breached the company's internal firewall and security systems, implanted malicious software and stole project files. The company said that it is actively working with law enforcement, security specialists and its affected customers to ensure the breach has been contained.

In November, 2011, Tech News Daily reported that a lone hacker penetrated the network of a South Houston, Texas, water-treatment plant to expose the inherent vulnerabilities in critical industrial control facilities and prove how easily they can be compromised. "No damage was done to any of the machinery; I don't like mindless vandalism," he wrote. "It's stupid and silly. On the other hand, so is connecting interfaces to your [industrial control systems] to the Internet." The hacker added, "I wouldn't even call this a hack, either, just to say. This required almost no skill and could be reproduced by a two year old with a basic knowledge [of industrial control systems]."

Author Brian Krebs, citing a May 27, 2010, FBI Intelligence Bulletin, reported that a series of hacks against smart meters may have cost a Puerto Rico electric utility $400 million annually over the past several years. The FBI believes that former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash and training others to do so. "These individuals are charging $300 to $1,000 to reprogram residential meters, and about $3,000 to reprogram commercial meters," the alert states. The thieves were able to hack into the smart meters with their laptop computers using software downloaded from the Internet. Once they altered the settings in the meters for recording power, customers were able to steal power from the utility.

According to the Department of Homeland Security (DHS), America's water and energy utilities face constant cyber-espionage and denial-of-service attacks against industrial control systems. While almost all of these attacks have either failed or have only been minor inconveniences to date, DHS believes that it is only a matter of time before a cyber attack has more serious consequences.

Utility-owned critical infrastructure has become more difficult to protect because it is not just the physical assets that need protecting anymore. When we talk about cybersecurity and infrastructure, we are referring to the cybersecurity of not only the physical distribution and transmission grids, substations and offices, but also equipment and systems that communicate, store and act on data. As the power grid is updated and modernized to include more computer networks, control systems and smart grid technology, the opportunity increases for computer hackers to cause mischief. While many of these hackers may not have a malicious intent, others may want to steal money or confidential information (like credit card numbers) or shut down the grid entirely. Under a worst case scenario, a

When we talk about cybersecurity and infrastructure, we are referring to the cybersecurity of not only the physical distribution and transmission grids, substations and offices, but also equipment and systems that communicate, store and act on data.

Simple steps to help protect your online information

Computers are an integral part of the power grid. But, we also use the Internet to stay connected and informed. We rely heavily on the Internet for everything from submitting taxes, to applying for student loans, to following traffic signals, to even powering our homes. Securing online data is important to protect personal information.

Americans can follow simple steps to keep themselves, their personal assets, and private information safe online.

Here are a few tips all Internet users can do to practice cybersecurity:

- Set strong passwords and don't share them with anyone.
- Keep your operating system, browser, and other software optimized by installing updates.
- Use anitvirus software.
- Limit the amount of personal information you post online and use privacy settings to avoid sharing information widely.
- Don't open any suspicious e-mails or attachments.

-- U.S. Department of Homeland Security

successful cyber attack could disrupt our economy and national security.

The Federal government has taken a number of steps to beef up cybersecurity oversight. On September 20, 2012, the Federal Energy Regulatory Commission (FERC) announced the creation of a new FERC office that will help FERC focus on potential cyber and physical security risks to energy facilities under its jurisdiction. The new Office of Energy Infrastructure Security (OEIS) will provide leadership, expertise and assistance to FERC to identify, communicate and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyber attacks and such physical threats as electromagnetic pulses. Additionally, for some time Congress has been considering cybersecurity legislation.

Likewise, protecting the grid and sensitive consumer information is an important function for the Commissioners at the Missouri PSC. State commissioners are responsible for ensuring that regulated utilities provide safe and reliable service at just and reasonable rates. Cyber attacks threaten safe and reliable service and the cost of implementing cybersecurity measures affect utility rates. Therefore, we need to know that our regulated utilities in Missouri are aware of the cyber threat issues and are taking reasonable steps to protect their systems in the event of cyber attacks.

Cybersecurity is really a three-pronged approach. First, utilities need a set of tools to prevent a cyber attack in the first place. Such preventative strategies involve not only traditional security controls, like performing background checks on employees, but also use new technologies, much like antivirus software that you would install on your personal computer. Second, utilities must collaborate with other utilities to learn about the different kinds of threats out there as well as share best practices to combat them. Third, should a cyber attack succeed, our utilities must be resilient in quickly responding to and effectively recovering from such an attack, just like utilities have had to do with natural disasters for decades.

Recently, the Missouri PSC opened a workshop to obtain information from our regulated electric utilities about their cybersecurity activities. We asked a series of 47 questions so that we can comprehensively evaluate what the utilities are doing to keep their systems safe from cyber threats. We have received responses from all of them and our staff currently is evaluating those responses. Once we have had a chance to review the information, we will have a better picture of our electric utilities' preparedness for cyber threats, and can take appropriate steps if they are falling short in any way.

At the end of the day, we want Missouri consumers to have confidence that our utilities are doing the right things to keep confidential customer information safe from theft and keep the power grid protected and reliable. We want to make sure that the lights are kept on.

Commissioner Terry M. Jarrett has served on the Missouri Public Service Commission since 2007. He is chairman of the National Association of Regulatory Utility Commissioners (NARUC) Critical Infrastructure Committee.