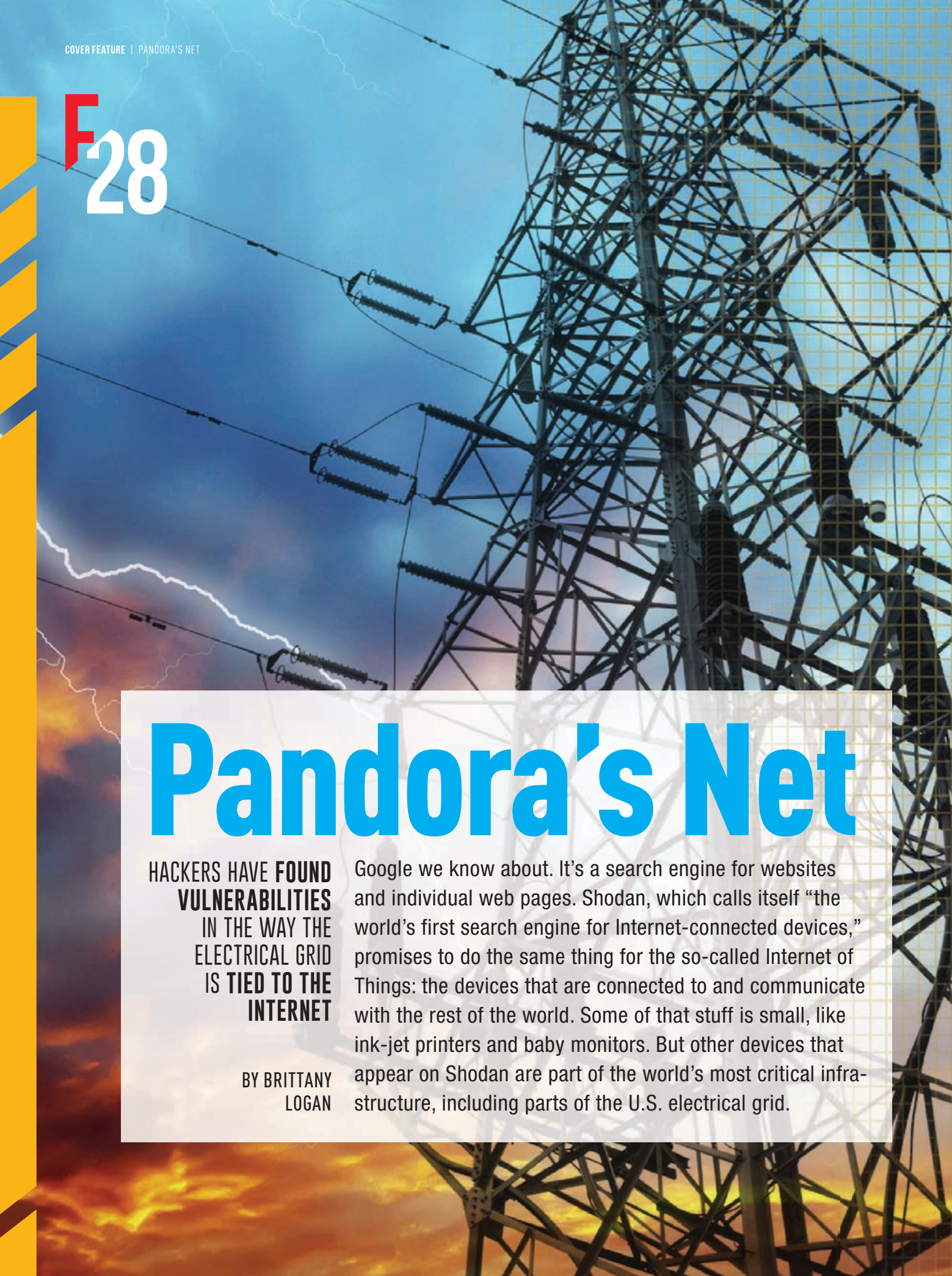
F28



Pandora's Net

HACKERS HAVE **FOUND VULNERABILITIES** IN THE WAY THE ELECTRICAL GRID IS **TIED TO THE INTERNET**

BY BRITTANY LOGAN

Google we know about. It's a search engine for websites and individual web pages. Shodan, which calls itself "the world's first search engine for Internet-connected devices," promises to do the same thing for the so-called Internet of Things: the devices that are connected to and communicate with the rest of the world. Some of that stuff is small, like ink-jet printers and baby monitors. But other devices that appear on Shodan are part of the world's most critical infrastructure, including parts of the U.S. electrical grid.

That accessibility has been portrayed as a boon to grid operators, who can monitor activity and control various systems remotely. But it also creates opportunities for hackers.

"All the stuff we're doing in Western society in regards to cybersecurity is probably ten years or so behind the curve of what the bad guys are doing," said Dan Tentler, founder of the San Diego-based information security consulting firm Atenlabs.

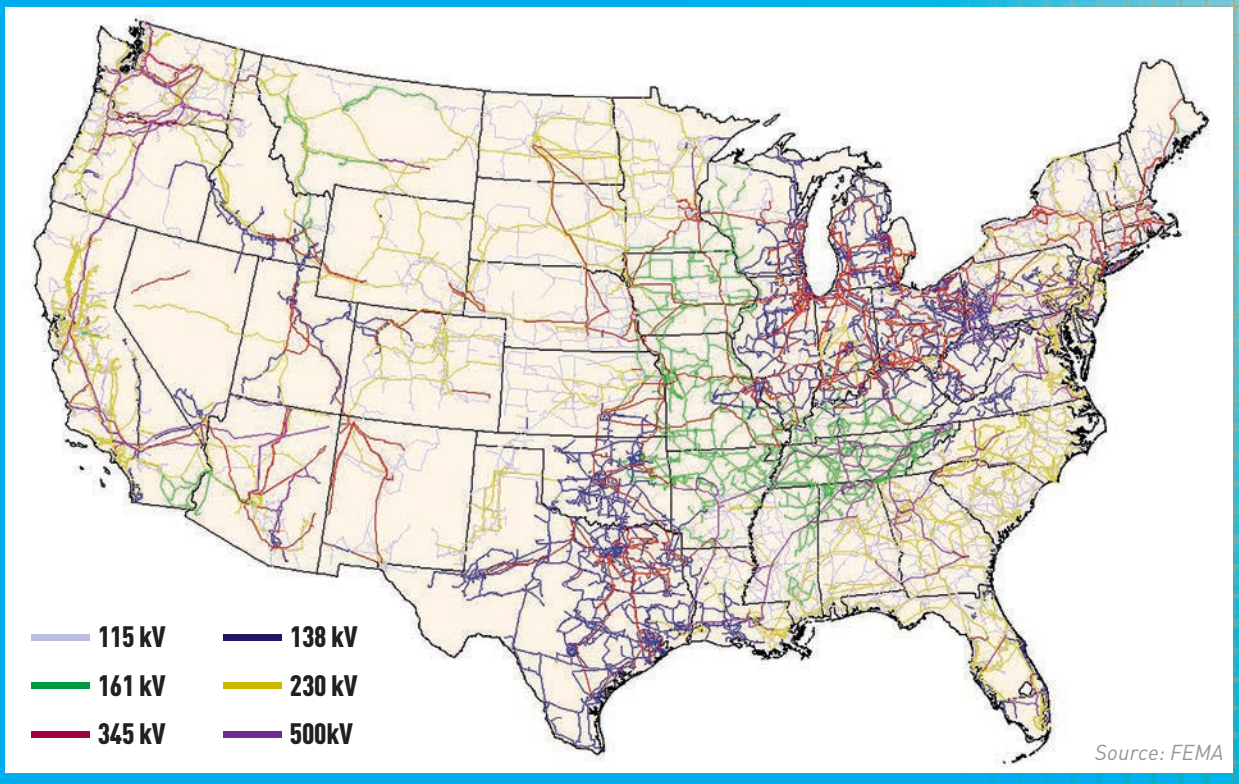
As a penetration tester, consultant, and former information security engineer at Twitter, Tentler knows a thing or two about information technology and cybersecurity. During presentations at the 2014 and 2012 Def Con cybersecurity conferences, he conducted real-time scans on all the connected devices he could find through Internet scans and Shodan. When it comes to securing critical infrastructures online, Tentler said, the lines between control system security and information technology security have blurred.

"The trouble is that, up until recently, these systems weren't considered IT's problem," Tentler said. "Generally speaking, these things ended up online because there was no security oversight of a technical background or nature looking at the concept of taking a giant 12,000 kV diesel generator behind the building and connecting it to the Internet."

The most vulnerable parts of the electrical grid lie behind locked gates and razor wire-topped fences, but the Internet was not designed with security in mind. That means that operators who work with Internet-connected infrastructure have to play a never-ending game of catch-up with security measures.

Until relatively recently, supervisory control and data acquisition, or SCADA, systems—which are the hardware and software that control and monitor infrastructure and industrial processes—ran on proprietary networks that communicated internally. Password requirements and firewall protections were weak, but that wasn't considered a security problem since the systems were inaccessible to the outside world.

UNITED STATES TRANSMISSION GRID

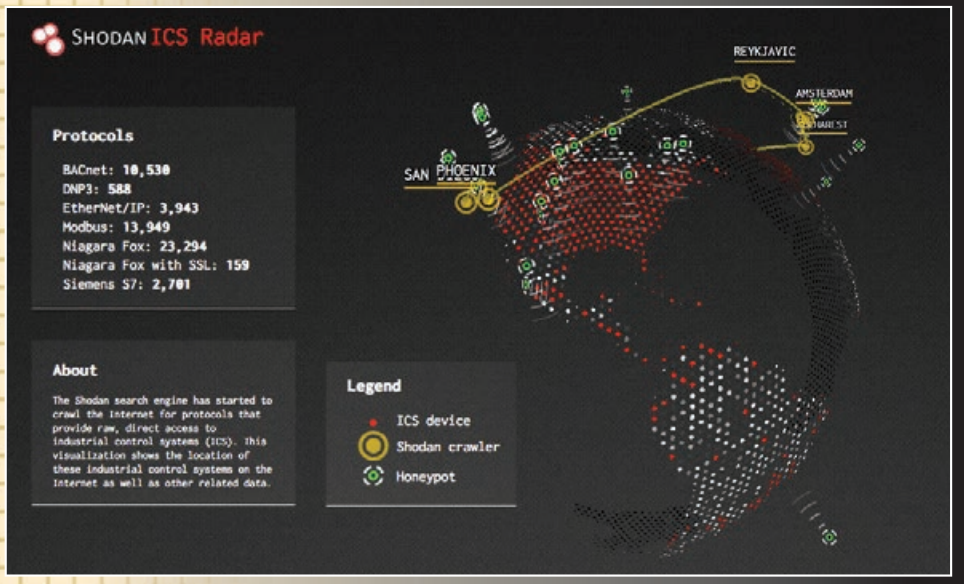


Ever more connected, the U.S. electricity grid is accessible through the Internet.

When industrial systems moved to public technology like Ethernet and Windows, it enabled companies to save time and money by permitting employees to monitor equipment offsite through field devices. Efficiency was a selling point to customers, who expected quicker service and data collection. But this remote accessibility has a cost.

"These systems are really, really, really vulnerable," said Joe Weiss, an industrial control systems and cybersecurity expert with more than 35 years of experience. Weiss is a former technical manager of the enterprise infrastructure security and critical infrastructure programs at the Electric Power Research Institute in Palo Alto, Calif.

"In the IT world, their focus is security. In the control systems world, the focus is reliability and safety," Weiss said. "And the problem is that there are times when they are mutually exclusive."



Screen shot from the Shodan search service.

REAL-WORLD VULNERABILITY

The potential security weakness of SCADA systems was exposed by a cyber attack against the Natanz uranium enrichment facility in Iran. The plant was the target of a computer worm, called Stuxnet, which was introduced to the site via an infected thumb drive. (The facility itself was isolated from the Internet.) The worm was programmed to search for specific systems pertaining to Iran's nuclear-enrichment program, including Simatic WinCC (a SCADA system from Siemens written for the Windows operating system) and programmable logic controllers for uranium centrifuges. Once Stuxnet found its target, it essentially used the control systems to make the centrifuges spin out of control while using previously captured data to trick them and the operator into thinking the system was fine. The worm also hid its files to avoid detection.

The damage caused by the attack destroyed about 20 percent of the centrifuges in the Iranian nuclear program.

Stuxnet may have been launched against an international security target, but the result had a broader, negative impact.

"Prior to Stuxnet, the hacking world really didn't know or care about the control system world," Weiss said. "The hacking world was either there for financial gain or reputation. And they didn't see either of those from the control system world. One of the blowbacks—the unintended consequences—of Stuxnet was all of a sudden, the control systems world popped up in the hacker's world."

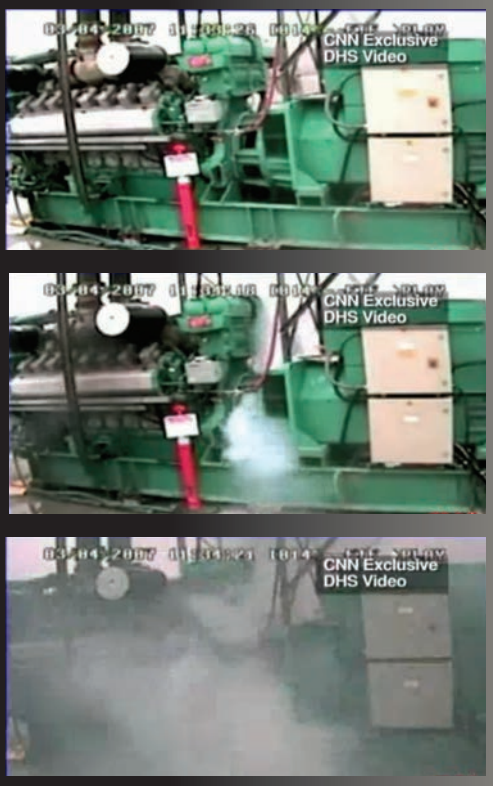
Other systems also proved vulnerable to cyber attacks. In 2012, Saudi Aramco became the victim of what was then referred to as the most destructive attack conducted against a business. After being injected through a thumb drive allegedly used by an employee, a computer virus known as Shamoon erased data on servers and wiped clean 30,000-55,000 of Aramco's hard drives.

The Shamoon virus contained a kill switch timer that when detonated, spread through Aramco's hard drives, erased information, and sent data back to the attackers. In addition to infecting computers connected through the Internet, it also corrupted non-connected computers that ran Microsoft Windows, according to a blog run by Eric Byres, a SCADA security expert and chief technology officer of Tofino Security in Lantzville, British Columbia.

Leon E. Panetta, U.S. Secretary of Defense at the time, expressed his concern about the virus at a Department of Defense press conference later that year.

"It raises tremendous concerns about the potential for the use of that kind of tool when it comes to our power grid, when it comes to our financial systems, when it comes to our government systems," Panetta said.

In 2014, Symantec, a cybersecurity company, released a report identifying a group of attackers called Dragonfly, who targeted the U.S. and European energy sectors. Using "Trojan horse" software, e-mail campaigns, and remote access tool malware, Dragonfly "managed to compromise a number of strategically important organizations for spying purposes and, if they had used



Stills from a video of the Aurora Generator Test, a simulated attack by hackers against a 2.25 MW generator that was connected to a substation: (Top) The generator gets out of sync and starts to bounce; (Middle) bits start flying off the generator; (Bottom) black smoke envelops the machine as the generator is destroyed.

the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries," the report said. Of the top ten countries information was stolen from, only Spain's energy sector was attacked more than the U.S.

To demonstrate that a cyber attack might have a physical consequence as well as a financial one, the U.S. Department of Homeland Security briefed stakeholders on a 2007 test conducted by Idaho National Laboratory. Known as the Aurora Generator Test, it simulated an attack by hackers against a 2.25 MW generator that was connected to a substation. Remote commands caused the 27-ton generator to get out of sync and start to bounce. A video of the test shows bits flying off the generator and black smoke enveloping the machine. Within minutes, the generator was destroyed.

The Aurora test, along with the Shamoon and Stuxnet attacks, provided a glimpse of what a future attack may be able to accomplish against critical infrastructures. The electric grid has always been somewhat open to physical attacks, but now it relies on systems that are vulnerable to cyber warfare that may not be detectable until after the damage has been done.

The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team reported responding to 256 incidents in 2013. About three-fifths of them, 59 percent, were in the energy sector. It is a significant increase from 2012, when 198 incidents were reported, of which 41 percent were energy-related.

In 2009, when ICS-CERT was launched, there were nine reported incidents.

One possible motive for the increase in incidents is the potential financial benefit gleaned from information taken by hackers. Another motive may be the potential gain in soft power.

According to Herbert Lin, chief scientist at the Computer Science and Telecommunications Board of the National Research Council and a consulting scholar at Stanford University's Center for International Security and Cooperation, soft power can be a serious threat.

One of the benefits of soft power is that it offers the ability to use coercive force and create confusion without using overt means, Lin said. Unlike military power, soft power tends to be less visible and more involved in influence and psychological impact.

In the world of energy, the industrial control systems monitoring the physical processes of machines are less tangible than the actual physical machines they control. But if a person, company, or government were to gain control of a country's physical machines through manipulating their control systems, the hacker could have both influence and power over that system, and over the people and environments it affects.

The need for cybersecurity makes for some difficult decisions for companies because costs and benefits are hard to calculate and there are no guarantees.

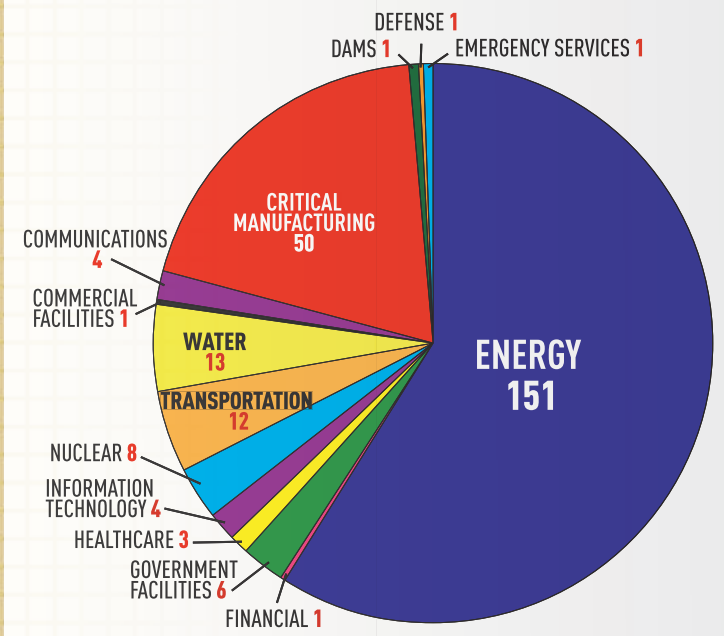
"You can spend every dollar you have on computer security and that can't necessarily be the right thing," said Scott Charney, vice president of trustworthy computing at Microsoft and a former chief of the computer crime and intellectual property section of the U.S. Department of Justice.

Investments in innovation, training, and human resources are still vital to a company's success.

Still, the awareness of grid vulnerabilities may tip the scale toward beefed up security in SCADA and related systems.

"I think there is a growing consensus, in a good way, that security is about risk management, not risk elimination," Charney said. "You see more and more material in the literature, and more and more discussions where people are practical about the fact that you're not going to get risk to zero. It's about managing risk well."

But preparation doesn't automatically mean execution. Last year Unisys Corp. and the Ponemon Institute in Traverse City, Mich., published results from a study of 599 global IT professionals about security prepared-



UNWANTED ATTENTION: CRITICAL INFRASTRUCTURE

Just what sorts of critical infrastructure are coming under cyber attack? The Department of Homeland Security's Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) responded to 256 incidents in 2013. Most of these incidents were first detected within the networks of critical infrastructure organizations that operate industrial control systems. The breakdown of the type of infrastructure coming under attack is shown at left—energy infrastructure was by far the most targeted, with 151 incidents, representing 59 percent of the reported attacks. Critical manufacturing facilities were next most likely, targeted by about 20 percent of the attacks.

The ICS-CERT evaluates each reported incident to determine the actual extent to which the systems have been compromised, especially looking for intrusions into the control environment or downloading of sensitive business information. It's estimated that there are many more incidents that go unreported, either because they are not detected or they are being deliberately not reported.

Source: U.S.Dept. of Homeland Security ICS-CERT Monitor, Oct./Nov./Dec. 2013

ness and maturity in critical infrastructure. Among the main findings was that almost "70 percent of companies surveyed that are responsible for the world's power, water, and other critical functions have reported at least one security breach that led to the loss of confidential information or disruption of operations in the past 12 months."

The study also found that more than half the respondents lacked confidence that "their organization would be able to upgrade legacy systems to the next improved security state in cost-effective ways without sacrificing mission-critical security."

Black & Veatch, the global engineering, consulting, and construction company, surveyed 576 electric industry participants last year as part of its annual "Strategic Directions: U.S. Electric Industry" report. Of those surveyed, only 32 percent replied that their security systems were integrated "with proper segmentation, monitoring and redundancies" for infrastructure protection. An additional 48 percent said their systems were not integrated. The rest stated that they did not know.

"I think that it's fair to say that the cyber vulnerability of critical infrastructure is an unsolved problem at this point," Lin said. "That doesn't mean that no one is working on it. It's just that nobody knows how best to do it at this point."

FIGHTING A LOSING BATTLE

Within the world of SCADA security, there are so-called white hats, grey hats, and the black hats. White hats are the "good cops," the cybersecurity experts safeguarding systems through hacking them to find flaws. Grey hats are hackers who work for a fee and use a combination of tactics. Meanwhile, black hats are those hacking for a malicious or detrimental purpose, and their ranks range from mainstream career hackers to agents of sponsored, terror-related organizations. In this realm, the white hats are fighting a losing battle in both numbers and perception.

"The white hats have had less than stellar luck trying to get large organizations to take security seriously," Tentler said, explaining that companies tend to view people with information about a system flaw as black hat hackers. That hasn't stopped Tentler, or his colleagues, whose approach is of the white hats. Tentler's Atenlabs blog and Twitter account regularly feature posts with security flaws on various systems in the hopes that the companies in charge will fix them.

For his part, Weiss has testified several times to Congress on cybersecurity and control systems. He advises companies, governments, and universities on infrastructure security and attempts to bridge gaps between IT and control system specialists by arranging gatherings to explore problems of cybersecurity and consider solutions.

Others have recommended the energy sector implement back-up and defense-in-depth systems. The concept of a common computer language for SCADA has also been mentioned in the security community, but could come with challenges.

"I think creating a common language for SCADA—like JavaScript—would contribute to improved security," wrote Chuck Adams, a SCADA security expert and president of Capstone Works Inc., in an e-mail.

Because many SCADA systems are written in a

variety of older, more obscure languages, a common one like JavaScript would enable security experts to search for vulnerabilities and share information. The easier everyone can communicate, the quicker and more likely a system's quirks and flaws can be found and patches issued. (An example of how this could work is to look at how quickly security experts can find and communicate flaws in Microsoft Windows products.)

"But with the disparate systems in place and the long lived nature of many of these systems, it would potentially take decades for enough adoption to significantly mitigate some of the security threats to the existing systems," Adams said.

More formal efforts are also taking place. The International Society of Automation, which has a global membership of 30,000 automation professionals, has released a series of international standards for industrial automation and control systems security.

In 2013, President Obama issued an executive order on improving critical infrastructure cybersecurity. As part of that order, he assigned the National Institute of Standards and Technology the task of developing a cybersecurity framework with standards and practices to address cyber risks. In early 2014, NIST released its report including voluntary guidelines for improving security and managing risks for critical infrastructure companies. In addition, the U.S. Department of Energy released "Cybersecurity Procurement Language for Energy Delivery Systems" to provide guidance on cybersecurity protections specific to the energy sector.

"There is not a single solution," said Black & Veatch's report of tackling cybersecurity issues in the electric industry. "But with an approach that addresses the physical elements of cybersecurity and the cyber elements of physical asset security, organizations will be better equipped and educated to manage the full spectrum of dangers."

Black & Veatch also made a point to note that respondents ranked cybersecurity as one of the top five electric industry issues. As recently as 2012, cybersecurity wasn't even listed in the top ten.

ACCESSIBLE TO ANYONE

There are steps that companies can take to beef up their cyber security. Requiring strong passwords and login credentials for SCADA systems are among the immediate, fundamental ways to improve security.

Following best practices, such as those described in the Security Benchmarks program of the Center for Internet Security, can help minimize vulnerabilities in IT systems.

Disconnecting any unnecessary network connections and restricting personnel access to only essential programs will limit unwanted access to SCADA systems through backdoor networks. Also useful: employing an offensive strategy of working together with respected white hats who can search for weaknesses ("penetration tests") the way hackers would.

Increased awareness is important, but protecting the electrical grid from cyber threats requires doing more. The Internet has an ingrained culture of security as a secondary concern. That same approach can no longer be applied to cybersecurity in critical infrastructures. SCADA and other industrial control systems previously isolated from the public are now potentially accessible to anyone with an Internet connection.

The National Supervisory Control and Data Acquisition Test Bed at Sandia National Laboratories in Albuquerque is tasked with finding and addressing critical security vulnerabilities in the energy sector.

The option to return to the way things were pre-World Wide Web no longer exists. The economy demands speed and automation on levels unheard of by previous generations.

The only direction left is towards resiliency and better technology and safeguards. ME

BRITTANY LOGAN is a freelance writer based in Paris.