SECURITY

Cyber raises threat against America's energy backbone

Blake Sobczak, Hannah Northey and Peter Behr, E&E News reporters • Published: Tuesday, May 23, 2017

In this May 2014 photo, rain clouds blanket a natural gas well pad operated by Cabot Oil and Gas Co. in northern Pennsylvania. Advances in hydraulic fracturing technology have made natural gas a cheap source for power generation, but experts say the interdependence between the electric and gas sectors could open doors for hackers. Photo by Blake Sobczak.

This article was updated at 4:17 p.m. EDT.

*First in a series. **Click here** for the second part and **here** for the third.*

Five years ago, an attack on nearly two dozen U.S. natural gas utilities set off alarm bells in the U.S. intelligence community. A hacker using the nickname UglyGorilla stole troves of sensitive data from gas pipeline companies, breaching the nation's 300,000-mile web of steel that's a critical backbone for the nation's economy.

News of the hacks trickled out in May 2012. Homeland security officials scrambled to schedule classified briefings with U.S. pipeline operators, and the wheels of law enforcement started building the case.

E&E SERIES

PIPELINES IN PERIL

With the U.S. electric grid increasingly reliant on natural gas, E&E News explores cyberthreats to the pipelines that are the system's backbone.

Two years later, the Justice Department unveiled charges against five members of an elite cyber division of China's military, outing People's Liberation Army officer Wang Dong as UglyGorilla and throwing light on a wide-ranging, "sophisticated" campaign of cyber theft dating back to 2006.

Wang's pipeline hacking spree peaked between December 2011 and June 2012, according to multiple sources. Since then, increased reliance on natural gas for power generation has made the gas transmission system one of the most consequential hacking targets in the country. Today, Wang and his team likely hold some of the blueprints needed to launch a cyberattack that could plunge parts of the nation into darkness for days, if not a lot longer, experts say.

Many gas companies say they have shored up security since then. But the sector's overall cyber readiness is a black box even to those charged with overseeing it, an *Energywire* investigation found. The Transportation Security Administration, better known and better funded for its role in aviation security, is tasked with ensuring the nation's biggest gas transmission companies stay at least a step ahead of hackers. Yet TSA's pipeline security office remains critically understaffed to tackle cybersecurity.

Meanwhile, the number of "advanced, persistent threats" going after U.S. energy systems has only grown since Wang's alleged series of intrusions. "There appears to be an increasing level of activity, sophistication and maturity of threat actors, in particular nation state actors, that wish to disrupt the U.S. bulk power system and the U.S. gas transmission or distribution system," gas and electric utility holding company Dominion Energy Inc. noted in a recent filing with the Securities and Exchange Commission, echoing similar disclosures from many of its publicly traded peers in the industry.

The Department of Homeland Security considers the threat of disruption to be low. But the impact could be enormous. William Evanina, director of the National Counterintelligence and Security Center in the Office of the Director of National Intelligence, said in March that a briefing from energy officials on the pipeline

threat "really scared me."

He noted that "if we have a cyberattack from one of our adversaries, and they hit the power grid in the East Coast," federal authorities have a good handle on the amount of time it would take to recover. "If the natural gas is shut off ... [there's] not even an estimate," he said.

Gas or bust

Until the mid-2000s, coal had supplied half the fuel to produce power in the United States, which was more than twice natural gas' share.

Then U.S. gas production soared by a startling 34 percent between 2007 and 2015, driven by hydraulic fracturing technology that pries open shale rock to release huge volumes of trapped gas. The drilling bonanza transformed electric generation. Natural-gas-fueled power production climbed steadily past coal's share, supplying 34 percent of U.S. electric power compared with coal's 30 percent last year.

Some regions' dependence on gas-fired generation is particularly concerning, according to the grid's security monitor, the North American Electric Reliability Corp. NERC's latest estimate is that 69 percent of on-peak generation capacity in and around Florida will come from gas by 2021, followed by California at 68 percent, Texas at 63 percent and New England at 52 percent.

"Within a relatively short time, a major [gas pipeline] failure could result in a loss of electric generating capacity that could exceed the electric reserves available to compensate for these losses," NERC observed in 2013. In other words, cutting off a major interstate gas pipeline could black out regions where there are too few other sources of electricity to pull from.

The likelihood of catastrophic pipeline failures was extremely low, NERC was quick to add, but that reassurance didn't take cyberattacks into account.

"Undercutting the gas supply is certainly a threat to the electric system. It's not just one among many resources," said NERC President and CEO Gerry Cauley in a recent interview. "It's become one that we're really very heavily dependent on."

He said NERC is planning for multiple scenarios, from a cold snap like the one that **snarled natural gas delivery** in the Southwest in 2011 to an equipment breakdown at a pivotal gas pipeline or storage facility. A massive natural gas leak at a Sempra Energy storage facility in Aliso Canyon, Calif., in late 2015 left grid reliability on a knife's edge throughout the following summer, as regional power producers struggled to come up with alternate gas supplies. Five years earlier, an explosion along a Pacific, Gas & Electric Co. gas transmission line killed eight people and demonstrated the kind of damage that can occur without any control system intrusion.

Natural gas pipeline explosions, while devastating and often deadly, aren't the biggest worry for the power sector.

Instead, multiple sources described how outages at crucial gas compressor stations could sever gas supplies to power generators. Low gas pressure could force power plants to burn through emergency fuel. If compressor stations — those often-unstaffed, gas-pushing workhorses that dot major pipeline routes — exhausted their own diesel backups for generating electricity, both industries could find themselves in a chicken-and-egg dilemma. The compressor stations couldn't resume pumping gas until power was restored, and electric utilities couldn't restore power without natural gas to fuel the generators.

"Because [hacking] is an intentional act, we would potentially have to look at multiple gas facilities being taken out concurrently, which is something we haven't really studied," Cauley said.

'One-stop shop'

Energy executives are tight-lipped about the online threats and vulnerabilities they face, not wanting to draw unwanted attention or offer a blueprint to saboteurs. There are no requirements for major gas pipeline operators to report hacking incidents to authorities, unless attackers wreak enough havoc to trigger safety or environmental rules.

Publicly traded firms often discuss their cyber risk in general terms in SEC filings. Boardwalk Pipeline Partners LP, a major gas transmission firm, warned in a recent financial disclosure that "certain cyber incidents may remain undetected for an extended period," adding that "our insurance coverage for cyberattacks may not be sufficient to cover all the losses we may experience" as threats continue to evolve.

Enterprise Products Partners LP, based in Houston, has cited the possibility that "one or more facilities or electronic systems that we own or that deliver products to us" could be damaged by a cyberattack, severe weather or other disruption.

"These interruptions could involve significant damage to people, property or the environment, and repairs could take from a week or less for a minor incident to six months or more for a major interruption," the company concluded.

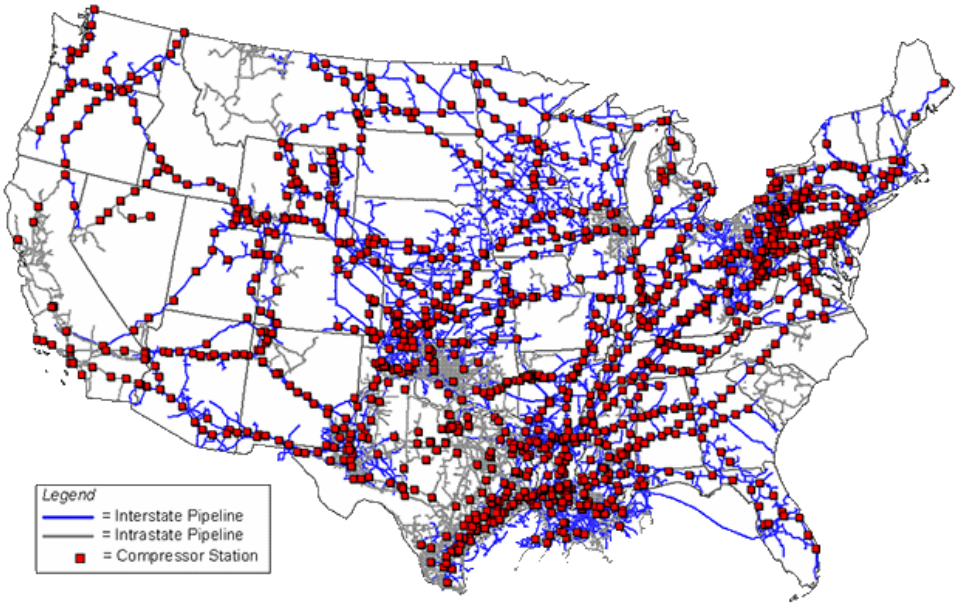
The documents are meant to warn investors of risks and don't speak to the likelihood of any particular attack. But multiple companies alluded to government warnings "that indicate that energy assets might be specific targets of cybersecurity threats."

Industry groups have warned about publicly accessible tools that could be used by saboteurs to build a dossier of potential U.S. pipeline targets. The National Pipeline Mapping System, a resource offered by the Department of Transportation, offers anyone with an internet connection the chance to see where gas transmission lines run, and how close they are to homes, schools and businesses.

"A 'one-stop shop' increases the ability for adversaries targeting our nation's infrastructure to pick the most disruptive targets," noted Danika Yeager, vice president for regulated business at Enterprise Products, in a public meeting to discuss potential changes to the mapping system in 2014.

Today, the public version of the site limits users to a zoomed-out look at transmission pipelines and allows them to view only one county at a time. Yeager noted in her 2014 presentation that "information housed in a password-protected site still remains susceptible to attacks and security breaches."

"The security of specific pipeline attributes on a segmented basis remains a critical concern, especially those that could underscore potential high consequence targets," she wrote in a slideshow.



[+] Delivery of natural gas through large transmission pipelines is carried out by compressor stations that maintain pressure in the pipelines to push the gas to its destinations. Compressor stations typically have manual controls that could be used to restore service and automatic shut-off devices. Exposure to cyberattacks increases as pipeline companies use more automated communications between compressor facilities and central control rooms, or link control systems to office business systems that face the Internet. Map by the U.S. Energy Information Administration.

Internet exposure

It's one thing to map out and home in on weak points in the pipeline system. It's quite another to remotely hack into those points and disrupt operations, according to cybersecurity experts and energy industry professionals.

Natural gas networks rely on a two-way stream of data channeled through "supervisory control and data acquisition" (SCADA) systems. These gather data sent up from "remote terminal units," staged at valve stations along the pipeline, to keep tabs on the health of the overall network. SCADA controls can also pull signals from automation equipment at compressor stations and other facilities along thousands of miles of pipe.

The far-flung U.S. power grid relies on a similar web of interconnected devices and control systems. But its counterpart in gas transmission is fundamentally less vulnerable to a crippling cyberattack, according to Terry Boss, senior vice president for operations, safety, environment and security at the Interstate Natural Gas Association of America.

Electric power races at near light speed across tightly synchronized paths programmed to disconnect when damaging instability occurs. Gas comparatively crawls along at 20 miles an hour through the pipeline matrix, giving operators more time to react, Boss said. "The natural gas pipeline business was built before they had computers. We are essentially a mechanical system."

The SCADA system may sit on top, but operators can go back and turn on valves by hand if necessary, he added. "If somebody wanted to attack the infrastructure in the U.S. and make a big impact, we would not be a good target."

But pipelines' defensive advantage is steadily eroding as more automated monitoring and control systems are installed, widening exposure to cyberattacks, industry officials and analysts agree.

Sempra Energy said in a recent SEC filing that "deployment of new business technologies represents a new and large-scale opportunity for attacks on our information systems and confidential customer information, as well as on the integrity of the energy grid and the natural gas infrastructure."

Schneider Electric, a major vendor for the electricity sector, has warned that pipeline control systems are becoming more sophisticated and connected, and thus more vulnerable to attack. Sensors and controllers are increasingly linked to utility networks, and even the internet, to make operations more convenient and efficient. "This convenience, however, is not without substantial risk," the company noted in a blog this year.

The spread of automated technology is making it more difficult for the bulk power system to fall back on manual operations, Bill Lawrence, senior director at NERC, pointed out at a recent conference. He also cited the electric sector's dependence on other, increasingly interconnected systems for reliability — including natural gas for fuel, water for steam and cooling, and communications. One concern is that poorly defended, internet-connected devices in any of these industries could be used to amplify certain types of cyberattacks on others.

One DHS official, not speaking for attribution, described the potential for malware that simply floods a pipeline's control network, overwhelming the limited computing capacity of devices that make it work. Other experts worry about massive denial-of-service cyberattacks designed to disable utilities' daily scheduling of gas deliveries. Utilities with gas generators are often last in line for gas deliveries and would be particularly vulnerable to such disruptions.

"Ransomware" is another constant cause for concern. Earlier this month, Spanish energy giant Gas Natural Fenosa reported being hit by the "WannaCry" malware, which locks up digital files and holds the key to unlock them hostage. While the WannaCry attack did not affect operations, any control system linked to a corporate network could, at least in theory, be paralyzed by a similar attack.

Technical nightmares

Adding to the concern have been the ups and downs of the gas business. The shale gas boom that started around 2007 and expanded through the end of 2014 set off mergers and acquisitions across the industry. Experts say that might be making matters worse on the security front.

Taking over a new SCADA system "is not exactly a cookie cutter," said Marco Ayala, senior

principal specialist for industrial control system/SCADA security at the Houston-based consultancy aeSolutions. Systems aren't identical and can rely on a number of modes of communication to send and receive data, including satellites, radio, phone lines and wireless networks.

When pipeline companies merge, that might mean increasing their security posture, Ayala said. "But some companies may not have a very strong security practice, or they're just looking at turning a coin," he said. "In other words, 'let's get something in there, let's rock and roll with it for a couple years, and then turn it around and sell it.'"

Quick fixes can leave pipeline equipment accessible online. Hackers can conduct tailored searches, perhaps modeled after the Shodan tool, to locate parts to attack en masse (***Energywire***, Aug. 15, 2014). If enough pieces of equipment are brought down simultaneously at gas pipeline compressor stations, the result could be a catastrophic loss of pressure.

> **Because [hacking] is an intentional act, we would potentially have to look at multiple gas facilities being taken out concurrently, which is something we haven't really studied.**
>
> *Gerry Cauley, president and CEO of the North American Electric Reliability Corp.*

The Department of Homeland Security has cooperated with Shodan's founder to drag particularly sensitive equipment offline. But with thousands of control systems still accessible, theirs is a Sisyphean task. New smart devices pop up on the internet every day as companies patch over connectivity problems, and they may stay visible online for years, with none the wiser.

"No one knows what [internet] access is out there," said Jim Guinn, who leads the energy, mining, chemicals and utilities cybersecurity practice at the consulting firm Accenture. "Everyone knows their little piece of the woods, but nobody knows what's in the resident forest."

Guinn seconded Ayala's concerns about the cybersecurity side effects of multibillion-dollar takeovers. "It becomes a technical nightmare to ensure that whatever cyber disease company A has, that when you tie these networks, you don't move that cyber disease to the other company," he said. When compared with hashing out financial details in boardrooms or on golf courses, he said, "That's a bigger problem."

'It's not magic'

Sandy Rice knows firsthand how painstaking it can be to boost cybersecurity in a SCADA system.

Rice, industrial control system security architect at gas transmission and distribution company Atmos Energy Corp., has led a decadelong crusade to improve his own organization's security practices.

"At first, I wanted to fix everything — and I wanted to do it *now*," Rice said. "But if you've ever worked in a control system environment, you know that no matter how hard you move, things just don't move fast."

Atmos, headquartered in Dallas, operates major pipelines that crisscross gas-reliant Texas and parts of Louisiana, among other states.

When Rice attended his first SCADA cybersecurity conference in 2009, hacking critical infrastructure was still widely viewed as a theoretical threat. Since then, several online attacks, including two that damaged parts of Ukraine's power grid, have shown how even seemingly isolated computer systems can be vulnerable to hackers.

"Things are coming around at the upper levels, at the C-suite level, where there is some awareness now, which is a big help," Rice said. "But for a long time, I don't think that there was a general awareness of how vulnerable we are as a society to cyberintrusion or cyberattacks."

Rice, speaking on the sidelines of an industrial cybersecurity conference in March, said he has directed his own team to "focus on the basics and do all those right," while counting on the IT department to provide a first line of defense on Atmos' corporate network.

"Frankly, we've been lucky," he said. "You know, luck favors the prepared, right?"

Not all natural gas companies have been fortunate.

Mark Bristow, deputy division director of DHS's Hunt and Incident Response Team (HIRT), recounted one case where "a number of pipeline operators" were intruded upon by a so-called APT actor — short for "advanced, persistent threats" like those from Russia or China.

"The actor never got into the control systems, at least that I can prove," Bristow said. "But what they did was they stole really sensitive information about control systems operations from the corporate networks," scanning computers for all signs of the term "SCADA."

Bristow did not identify China as the prime suspect, but his description fits with other experts' comments about UglyGorilla's activity five years ago.

Still other hacking groups have made it clear that pipeline operators are prime targets. One example, Bristow noted, included a nation-state actor that in one instance snaked his way through a system, breaking through the organization's firewall, stealing login credentials and reaching the boundary of the control system.

"The adversary had been in there for almost a year and a half at that point in time," Bristow said.

"You can't suddenly go, 'Oh, I've had an incident,' and recreate everything that happened in your environment," Bristow said. Preparation is critical.

Multiple sources have said larger energy companies have invested heavily in cybersecurity since the early 2010s. Accenture's Guinn noted that he has "not worked with a major company yet where this is not on the top of their list of priorities."

But small- to midsized firms, even if executives are on board with the need for online defenses, can face staffing and technical challenges where the rubber hits the road.

DHS statistics suggest many infrastructure operators still aren't recording what happens on their networks.

In fiscal 2016, DHS's Industrial Control Systems Cyber Emergency Response Team heard of about 290 control system cyberincidents. Of those, ICS-CERT attributed 134 to advanced persistent threats, or nation-states. Other threats came from competitors, company insiders and "hacktivist" groups like Anonymous.

But 90 cases were classified as "unknown," marking times the digital trail ran cold.

"A lot of times, we don't know what the root cause is, we don't know the intrusion vector. That's because we don't have any information," Bristow said. "Our team's really good, but they can't make something out of nothing. It's not magic."

Twitter: **@BlakeSobczak** | Email: **bsobczak@eenews.net**