In the Dark

Industrial control systems have traditionally been kept isolated with limited remote network access. But that's changing—introducing new and potentially damaging vulnerabilities.

Essential personnel have made drastic changes to the way they are working in response to the coronavirus pandemic—including electric grid operators.

In an unprecedented step, the New York Independent System Operator (NYISO)—an independent organization charged with managing the state's electric marketplace—announced on 31 March 2020 that it would sequester a group of its control room operators and support staff to protect their health and safety and maintain grid reliability as COVID-19 cases skyrocketed in New York state.

Thirty-seven people—31 grid operators, two managers, two facilities staff, and two café workers—volunteered to join the sequestration program at two NYISO sites outside of Albany, New York. They would work 12-hour shifts and live in separate trailers for the duration of the sequestration—a workflow that was established to minimize cross-contamination.

"Our primary job is to keep the power flowing in New York," NYISO said in a statement. "Operators are on the front lines, making sure that the amount of power being generated always equals the amount of demand from the state's nearly 20 million residents and businesses. To do that, seven operators work per shift, monitoring dozens of digital displays and directing power generators and distributors to keep energy transmission in balance."

Such steps were necessary to keep NYISO operational because much of the equipment that is used to manage, control, and distribute

ILLUSTRATION BY EVA VÁZQUEZ

electrical power is not connected to a network that can be accessed remotely. This is a control mechanism designed to limit exposure to a cyberattack that could cause a power failure.

But with increasing technological capabilities and the need to access worksites remotely—such as during a pandemic—more utility operators are looking at connecting their operational equipment to the Internet, said Tim Conway, technical director of industrial control system (ICS) and Supervisory Control and Data Acquisition (SCADA) programs at the SANS Institute, in a virtual conference on ICS security earlier this year.

"Critical infrastructure is adding remote connection at an alarming rate," he added. "I don't know if we're going to see this go back down after COVID-19...but we need to improve detection capability if that's the case."

This is because ever since the attacks on Ukraine's electrical grid that shut off power in 2015, threat actors have been increasingly focused on targeting critical infrastructure and the systems used to support its operation. North America is an especially lucrative target, and recent analysis finds that regulators may not fully understand the scope of a massive power outage caused by a cyberattack.

The Landscape

ICS is a term used to describe control systems and their instrumentation, which can include devices, systems, networks, and controls that operate or automate industrial processes. These

Critical infrastructure is adding remote connection at an alarming rate.

These systems are an important component of critical infrastructure, such as manufacturing, transportation, energy, and water treatment.

One type of ICS is a SCADA system, which is used to acquire and transmit data and is often integrated with a human interface to provide centralized monitoring and control for process inputs and outputs, according to multinational cybersecurity and defense company Trend Micro.

"The primary purpose of using SCADA is for long distance monitoring and control of field sites through a centralized control system," Trend Micro explained in a blog post. "In lieu of workers having to travel long distances to perform tasks or gather data, a SCADA system is able to automate this task. Field devices control local operations such as opening or closing of valves and breakers, collecting data from the sensor systems, and monitoring the local environment for alarm conditions."

In 2015 and 2016, Russian-backed hackers used cyber tactics to target Ukraine's electric grid and shut portions of it down during the winter—wreaking havoc and causing authorities around the world to bolster their grid security.

Prior to those attacks, the U.S. Government Accountability Office (GAO) placed the protection of critical cyber infrastructure—including the electric grid—on its High Risk List in 2003. In 2018, Congress asked the GAO to audit the cybersecurity of the U.S. power grid, which is interconnected with Canada's and a small portion of Mexico's.

In its research, conducted over the course of a year and published in August 2019, the GAO found that the electric grid is increasingly vulnerable to cyberattacks—especially those involving any ICS that supports grid operations. Increasing adoption of consumer Internet of Things (IoT) devices and the use of the global positioning system to synchronize grid operations were also contributing to the growing vulnerability of the grid.

"Compounding the risk associated with the increased attack surface, many legacy industrial control systems were not designed with cybersecurity protections because they were not intended to be connected to networks, such as the Internet," the GAO explained. "For example, many legacy devices are not able to authenticate commands to ensure that they have been sent from a valid user and may not be capable of running modern encryption protocols. In addition, some legacy devices do not have the capability to log commands sent to the devices, making it more difficult to detect malicious activity."

The GAO also found that grid owners and operators may not be able to identify ICS vulnerabilities in a timely manner because conventional IT vulnerability scanning could disable or shut down energy delivery systems. And for those who do identify vulnerabilities, they may not be able to quickly address them because of high availability requirements needed to support grid operations.

"These devices typically need to be taken offline to apply patches to fix cybersecurity vulnerabilities," the GAO added. "In addition, grid owners and operators need to rigorously test the patches before applying them. Security patches are typically tested by vendors, but they can degrade or alter the functionality of ICS, which can have serious consequences for grid operations."

The GAO also found that the supply chain for ICS could also introduce vulnerabilities that make operators more vulnerable to cyberattacks.

"For example, there is a potential for manufacturers and developers to—wittingly or unwittingly—include unauthorized code or malware in industrial control system devices and systems that provides a back door into the equipment or that allows the program to 'call home' once installed," the GAO explained.

Most concerning, however, was the finding that despite federal assessments indicating cyberattacks could cause widespread power outages in the United States, the government lacked an understanding of what the ramifications of such an incident would be.

"We thought federal assessments of the impact had limitations," says Frank Rusco, director of GAO's Natural Resources and Environment Team and coauthor of the report. "In short, assessments didn't always cover the various cyberattack scenarios that should be considered—such as techniques or coordinated attacks on multiple sites at one time. Some of the assessments did not cover as wide a geographic scale as would have been helpful."

For instance, the assessments did not address the ramifications of a widespread power outage that lasted for a long period of time—as opposed to a storm where the grid was damaged but able to resume operations quickly.

Additionally, one of the three assessments that the U.S. Department of Energy (DOE) was relying on covered the Western Interconnection, which extends from western Canada south to Baja California in Mexico, and east to the Great Plains of the United States, but was based on a reduced model of the electric grid from 1980.

"If you're not modeling what's possible in terms of what could happen, but you're also not looking at the system as it is today and how reliant we are on it…you're going to miss it because you haven't modeled what is actually possible," Rusco says, adding that he is not sure why the U.S. Department of Energy (DOE) was relying on that particular assessment. The DOE did not return request for comment on this article.

The GAO's analysis also found that while the Federal Energy Regulatory Commission (FERC), which regulates the interstate transmission of electricity, natural gas, and oil, has approved mandatory grid cybersecurity standards, it does not ensure that those standards address the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The GAO also highlighted that FERC has not considered the potential risk of a coordinated cyberattack on geographically distributed targets.

"Such an attack could target, for example, a combination of geographically dispersed systems that each fall below the threshold for complying with the full set of standards," the GAO said. "Responding to such an attack could be more difficult than to a localized event since resources may be geographically distributed rather than concentrated in the same area. Without information on the risk of such an attack, FERC does not have assurance that its approved threshold for mandatory compliance adequately responds to that risk."

Actors and Methods

In its *2019 Year in Review: The ICS Landscape,* Dragos—a security firm that specializes in ICS protection—found that despite no reported destructive attacks, the "amount of activity targeting ICS increased significantly in 2019."

The report detailed 11 activity groups that are targeting ICS entities around the world, with an increased focus on ICS organizations in critical infrastructure across the United States and the Asia-Pacific regions.

Dragos assessed that there will likely be an increase in cybersecurity activity

A Flaw in the System

Experts and researchers have raised concerns over the past several years about the security of Supervisory Control and Data Acquisition (SCADA) programs—a type of industrial control system (ICS).

In summer 2020, cybersecurity firm Trustwave published a new vulnerability report by Seok Min Lim on two exploits that could be used to target Schneider Electric's Programmer Logic Controller (PLC) software and hardware. PLCs are flexible pieces of hardware used in SCADA programs and operational technology for utilities. One of the exploits was an expansion of a discovery researchers originally made in 2017, but the other was new, says Karl Sigler, senior security research manager for Trustwave, who oversees the research team Lim is on.

The first vulnerability allowed researchers to "intercept, manipulate, and re-transmit control plane commands between the engineering software to the PLC," according to Trustwave's report. "The impact is that a malicious actor can start and stop the PLC remotely without authentication."

The second vulnerability found that free software provided by Schneider—SoMachine Basic—to program and control a PLC did not perform "adequate checks on critical values used in the communications with the PLC," Trustwave said. "The vulnerability can potentially be used to send manipulated packets to the PLC, without the software being aware of the manipulation."

Trustwave reported the vulnerabilities to Schneider, which has since released patches for them. But the exploits show how these programs and systems are increasingly vulnerable to cyberattacks because of flaws in the system and the organizational and operational cultures that many grid operators have.

"It can be a bit of a hardship—a lot of these organizations, specifically in the SCADA realm, are change averse," Sigler says. "They are not the most agile when it comes to patching; they generally follow the if it's not broke, don't fix it approach. They're dealing with extremely critical systems, and if you install a patch on a SCADA system and it crashes components, you can be talking about causing more damage than the patch was supposed to fix."

Sigler also adds that Trustwave's findings are similar to other vulnerabilities that have been reported in the past decade after the Stuxnet cyberattack became public, explaining that vendors' responses are encouraging because it reflects a mind-set change that simply preventing hackers from gaining access through air-gapped networks is not enough to protect systems.

"We've seen a lot of these vulnerabilities in the past," he says. "I think that all these vendors are quickly coming around to the realization that they need to be better—having their own software that's internally secure and not relying on external controls to prevent exploitation."

directed towards critical infrastructure and industrial entities as geopolitical tensions rise. It identified similar tactics during summer 2019 among the United States, Saudi Arabia, and Iran.

Dragos also analyzed that the threats to ICS are becoming increasingly numerous and sophisticated as threat actors invest resources to obtain the ability to disrupt critical infrastructure. For instance, the activity group XENOTIME (which was behind the TRISIS malware that targeted Schneider Electric's Triconex safety instrument system) engaged in a pattern of attempting to gather information and network resources associated with U.S. and Asia-Pacific electric utilities.

"XENOTIME expanded its probing activity to include electric utilities, using the same techniques previously deployed against oil and gas entities," according to the report. "Additionally, as identified in previous Dragos reporting, XENOTIME has targeted, and in some cases successfully compromised, original equipment manufacturers, potentially impacting the entire industrial supply chain."

The report also identified an increase in malware infections, such as ransomware, at industrial companies in 2019.

"The malware and ransomware incidents largely target enterprise networks," according to the report. "However, like Dragos has observed multiple times, incidental infections within the OT due to poorly segmented or misconfigured networks, or infections disrupting IT software or services required for operations—like data, fleet, or production management software—can have operationally disruptive effects."

Along with new and developing tactics, threat actors are also using common and popular tactics to gain access to their target's ICS, such as password spraying—when adversaries target numerous accounts using common passwords to attempt large-scale authentication to gain access.

We thought federal assessments of the impact had limitations.

"Although password spraying is a relatively common technique attackers use to gain access to enterprise resources, organizations are often vulnerable to these types of attacks because of poor account management and authentication policies for external resources," according to the Dragos report.

The report also identified instances of threat actors using phishing campaigns to target ICS entities. For instance, actors used LinkedIn direct messaging to send "project proposal" lures. "LinkedIn can be a useful phishing route for an adversary as it can bypass email security filters and attackers can leverage users' network connections to appear as a legitimate contact," the report explained. (See "The Cost of a Connection," *Security Management*, February 2019)

Impact

In response to some of GAO's grim assessments, the U.S. government and North American regulators have taken action to increase grid security.

In early 2020, U.S. President Donald Trump signed an executive order to enhance security of the U.S. bulk-power system. A primary focus of the order was limiting foreign supply of the system's electric equipment, a measure that would address in some part the supply chain threat identified by the GAO.

Under the order, operators are prohibited from purchasing or installing bulk-power system electric equipment where the transaction involves any property that a foreign country or national has interest in and poses an undue risk of sabotage or catastrophic effects on the security or resiliency of U.S. critical infrastructure or the economy of the United States.

The order also grants the authority to the U.S. secretary of energy to create criteria for recognizing equipment and vendors as prequalified for purchase and installation into the U.S. electric grid.

In the GAO report, auditors recommended that the DOE develop a plan to implement a federal cybersecurity strategy for the electric grid and include a full assessment of cybersecurity risks to the grid.

DOE agreed with this recommendation and said in a statement included in the GAO report that it is working with the National Security Council to develop a National Cyber Strategy Implementation Plan.

The North American Electric Reliability Corporation (NERC) also released a suite of cyber standards for some—but not all—grid operators to comply with over the course of the past decade (CIP-002 through CIP-011). NERC is the international regulatory authority that develops and enforces reliability standards, assesses seasonal and long-term reliability, and monitors the bulk power system in the United States, Canada, and the northern part of Baja California, Mexico. It is overseen by the FERC and Canadian government authorities.

Howard Gugel, vice president of engineering and standards for NERC, says that the regulator began developing a suite of cyber standards using a risk-based approach and assessment methodology to help operators determine what their risk was and apply controls to reduce it. This resulted in several standards, along with a recent revision of a standard: CIP-008-6, *Cybersecurity—Incident Reporting and Response Planning*.

The previous standard only required operators to report all compromises to their systems. It did not require operators to report attempts to compromise, which meant there was a lack of understanding of the threat landscape, Gugel says.

"These standards have been in place for years, so it was time to say, 'Let's start looking at some attempts—maybe we can reduce some shots on goal,'" he adds.

Under the updated standard, which goes into effect on 1 January 2021, subject grid operators will be required to report all cybersecurity incidents. NERC defines an incident as "any malicious act or suspicious event that compromises or was an attempt to compromise the electronic security perimeter or physical security perimeter of a critical cyber asset, or disrupts or was an attempt to disrupt the operation of a critical cyber asset."

The SANS Institute's Conway says that having terms like "incident" defined and a set scope of regulations addressing cybersecurity is a benefit to the electric operator community.

"Previously, asset owners and operators could define what a reportable incident was," Conway explains. "If someone broke into a control center and disrupted the [system], that's a cybersecurity incident. But if it didn't cause any effect on power generation, dynamic response, any type of situational awareness, or control center functions, it wouldn't have been reportable."

Operators must also provide evidence collected on the incident, including documentation that demonstrates maintenance of each incident response plan in accordance with the standard. Owners must then notify the Electricity Information Sharing and Analysis Center (E-ISAC) of the incident.

U.S.-based operators are further mandated to report this information to the U.S. National Cybersecurity and Communications Integration Center (NCCIC). There is no similar requirement for Canadian-based operators.

Additionally, all subject operators are required to provide continuous updates about the incident within seven days of learning something new. They must also detail what the functional impact of the incident was, for instance what the threat actor was likely targeting.

Penalties for noncompliance with the updated standard will be determined on a case-by-case basis, Gugel says.

"We do an assessment of the situation with our compliance and enforcement folks, take into account the scenarios that occurred, mitigating effects put into place—that's all evaluated," he explains. "If determined there's a penalty, then that's developed and put forward. There is not a cookie cutter automatic fine."

Gugel says he is not aware of any other regulatory authorities that have adopted similar standards for electric grid operators, but many countries are using NERC's standards as a model for what they would like to implement.

"Our standards are the minimum requirement; we expect entities to do at least that," Gugel says. "Our entities put other controls in place. These are just the ones that we say have to be done."

Based on its analysis, the GAO recommended that FERC consider adopting changes to its approved cybersecurity standards to more fully address the NIST Cybersecurity Framework.

The GAO also recommended that FERC evaluate the potential risk of a coordinated cyberattack on geographically distributed targets and determine if it needed to change the threshold for mandatory compliance with its full set of cybersecurity standards.

FERC Chairman Neil Chatterjee responded to the recommendations in a statement and said he considered them "constructive" and has directed staff to take appropriate steps to implement them.

Rusco says that FERC, as of *Security Management*'s press time, was conducting studies on applying the NIST Cybersecurity Framework to its standards and on effects of coordinated cyberattacks. But despite these actions, regulators, government agencies, and operators will need to remain focused on cybersecurity across the grid.

"You are only as strong as the weakest link," Rusco says. "Given that everything is becoming more and more interconnected, you're going to have to massively train everyone who uses equipment that's vulnerable to watch out for hacks. Or you're going to have to have systems that are able to expand into a broader and broader landscape where everyone has more devices that are Internet connected and connected to other things. We're heading into unchartered waters." ■

MEGAN GATES IS SENIOR EDITOR AT *SECURITY MANAGEMENT.* CONNECT WITH HER AT *MEGAN.GATES@ASISONLINE.ORG.* FOLLOW HER ON TWITTER: *@MGNGATES.*