Cybersecurity

Powering Through Requires Securing the Grid

The U.S. energy sector has a bullseye on its back. Whether it's nation-state hackers or domestic terrorists, the level of malicious activity directed against the sector has reached an all-time high, and we would do well to heed the threat. As the threat grows, some federal cybersecurity officials and others are sounding alarms about potentially "catastrophic" budget cuts proposed by some lawmakers.

In December 2015, Russia's cyberattack against the Ukrainian electricity sector caused a blackout affecting 230,000 people. A year later, Russia perpetrated a second attack against Ukraine. These incidents marked a turning point, demonstrating for the first time that cyberattacks can have significant impact on a nation's electricity infrastructure.

COMMENTARY

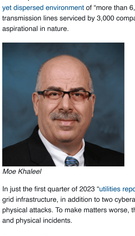
Fast forward to 2023 and Ukraine is not alone in this. Its NATO allies, including the U.S., have been the victims of malicious Russian cyber events including ransomware attacks suspected of being influenced by Russian intelligence services.

The U.S. and our allies have been put on notice to stand ready in case the crosshairs shift our way. The 2023 Annual Threat Assessment produced by the Director of National Intelligence warned "Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States."

Threats to the U.S. grid are both real and varied. They come in all sizes, shapes, and flavors, from nation-states to non-state actors. They span the gamut from supply chain, insider threats, to cyberattacks on information technology (IT) and operational technology (OT) systems. From 2020 to 2022 the average number of weekly cyberattacks alone on utilities (gas and electricity infrastructure included) increased 118%.

Threats From China

China's cyber capabilities have also increased in sophistication and malicious intent. Recent reports have provided that China has implanted malicious code in the power-grid networks that support U.S. military bases located stateside and overseas as well as civilian communities. This portends that China could interfere with U.S. military operations and cause harm to Americans more broadly.



Frank Cilluffo

Notably, China now tops the list of sophisticated cyber actors, and it is clearly watching Russia's activity in Ukraine with Taiwan in mind. The 2023 Annual Threat Assessment by the Director of National Intelligence stated: "China almost certainly is capable of launching cyberattacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems."

Physical Threats

In the meantime, physical attacks against the grid are not going away. To the contrary, domestic violent extremists have set their sights on it, according to the DHS Office of Intelligence and Analysis. The recently released DHS 2024 Homeland Threat Assessment noted critical infrastructure will continue to be a potential target of terrorist cyber and physical attacks, due to the belief this would significantly impact Americans' daily way of life.

The temptation to attack domestic critical infrastructure stems from a variety of motives, including striking the target-rich yet dispersed environment of "more than 6,400 power plants, 55,000 substations, and 450,000 miles of high-voltage transmission lines serviced by 3,000 companies" to achieve their goals. This kinetic threat is far from being purely aspirational in nature.

Moe Khaleel

In just the first quarter of 2023 "utilities reported 60 incidents they characterized as physical threats or attacks on major grid infrastructure, in addition to two cyberattacks." At that rate, 2023 may well top 2022's record of 164 major cyber and physical attacks. To make matters worse, the numbers could be understating the reality due to imperfect reporting of cyber and physical incidents.

Many Bad Actors

There is no shortage of bad actors willing to exploit our vulnerabilities and do us harm. Our goal must be to thwart them.

We must bring together experts in academia, government and the corporate world to work together and share information rather than working at cross purposes. We must cut through red-tape and find solutions quickly, before we face a new threat. We must see this threat holistically and not as a series of unconnected events.

As an example of building partnerships, the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University and Oak Ridge National Laboratory (ORNL) have joined forces to address these challenges. Though our critical infrastructure has withstood attacks to date, we cannot wait to protect it from future, potentially catastrophic, attacks. As former President John F. Kennedy said, "The time to repair the roof is when the sun is shining." And, in this case, while the lights are on.

—Frank J. Cilluffo is Director of the Auburn University McCrary Institute for Cyber and Critical Infrastructure Security and is a former Special Assistant to the President for Homeland Security and Commissioner on the Cyber Solarium Commission. Moe Khaleel is the Associate Laboratory Director for National Security Sciences at Oak Ridge National Laboratory.

Dec 18, 2023
by Contributed Content

POWER is at the forefront of the global power market, providing in-depth news and insight on the end-to-end electricity system and the ongoing energy transition. We strive to be the "go-to" resource for power professionals, offering a wealth of information on innovative business practices, sound safety measures, useful productivity enhancements, and much more.