SPECIAL NEWS ITEM

URGENT Risks to the U.S. Power Grid: International Threat Landscape Perspectives

China is a focal adversary regarding threats posed to American power grid security.

One resounding theme today from the world of cyber threats centers around China. It seems that, at every turn, we see, read, hear, or experience something that throws the spotlight onto Chinese adversaries leveling yet another attack or exposing yet another vulnerability to our critical infrastructure. So, what are we DOING about it? Not enough. How are we responding? Not quickly or fortuitously enough.

> Speaking to the Washington Post, in December 2023, Brandon Wales, executive director of CISA said, "It is very clear that Chinese attempts to compromise critical infrastructure are in part to pre-position themselves to be able to disrupt or destroy that critical infrastructure in the event of a conflict, to either prevent the United States from being able to project power into Asia or to cause societal chaos inside the United States - to affect our decision-making around a crisis. That is a significant change from Chinese cyber activity from seven to 70 years ago that was focused primarily on political and economic espionage."

> "...cause societal chaos within the United States..."
>
> Brandon Wales
> CISA Executive Director

Earlier this year, FBI Director, Christopher Wray, testified before Congress on the increasing cyber threat that China poses to the U.S. He outlined methods and examples that demonstrate Chinese cyber attacks that target civilian life and national economic stability. He shared a deep concern about situations such as Chinese entities purchasing land in the U.S. that could be used by them for surveillance and other activities to "undermine our national security." Mr. Wray expressed deep concern about the repercussions of waiting until the Chinese leverage the access that they have gained and will continue to gain, if we don't get "left of boom."

Attack Examples

In the ground-breaking documentary film"Grid Down Power Up," several very real and possible threats to America's power grid are featured; the first one being cyber attacks, many propagated by Chinese hackers, on our electric utility infrastructure. These attacks are not just theoretical. They have been carried out in the past. In fact, according to a report from the U.S.-China Economic and Security Review Commission, Chinese hackers were responsible for at least 17 cyberattacks against U.S. power plants and their suppliers between 2012 and 2019. For example:

- **2015 Malware Discovery in Energy Companies:**
  Cybersecurity firms uncovered that multiple U.S. energy companies had been infected with malware traced back to Chinese sources. This software was specifically designed for espionage and could disrupt energy distribution networks.
- **2017 Spear-Phishing Campaign Against Utility Workers:**
  A sophisticated spear-phishing campaign targeted individuals working in the U.S. energy sector. Investigations linked these incidents back to a group associated with the Chinese government, aiming to infiltrate networks and gather intelligence on the U.S. power grid system.
- **2019:**
  On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against APT41 Chinese nationals Zhang Haoran and Tan Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing.

Real Impacts

Why is there such a sense of urgency to act?

- There were 210 deaths attributed to the grid collapse in Texas during the Winter of 2021.
- Taking out just 9 specific power substations across the U.S. will cause a blackout across the **entire country**.
- Life-saving medical devices will shut down.
- Gas pumps & vehicle charging stations will be crippled.
- Grocery stores & other essential operations will close.

In short, life, as we live it today, will cease to continue, and we can only assume that chaos and anarchy will ensue.

This Isn't Dismissible FUD: Hear From the Experts

This is not Fear, Uncertainty, Doubt (FUD), but real demonstrated risks. Time isn't just ticking - it's UP! Cyber attackers have become more and more sophisticated. As a result, our national power grid has become more and more vulnerable. We are not developmentally outpacing the cyber criminals to achieve resilience to their attacks.

Chinese Parts Create Risks

> "Chinese transformers, cranes, inverters, process sensors, etc. are comparably well-made and inexpensive, leading to their continued use in U.S. critical infrastructures. Many of these devices have known hardware backdoors or other cyber security concerns," says Joe Weiss (CISM, CRISC, ISA Life Fellow, IEEE Senior Member, Emeritus Managing Director ISA99). Joe's blog entries on **www.controlglobal.com/blogs/unfettered** focus on risks to Operational Technology (OT) security.

Mr. Weiss has over 40 years of experience in industrial instrumentation controls, and automation, and over 20 years of experience in the cyber security of industrial control systems (ICS). His passion about the urgency for solutions is evident in his work.

Our own resident expert, Jim Frelk (SVP Business Development) was a guest on the February 4, 2024 episode of the America Out Loud podcast, on which he offered his perspectives from the Grid Down Power Up congressional event. Jim previously served as a national security advisor on Capital Hill, and has vast experience with and understanding of adversarial threats; particularly those of a cybersecurity nature. "The Chinese have been playing a long game at this. They've prepositioned a lot of the threats that we're facing today," Jim says on this podcast. "We know there are at least 400 transformers on our grid that have Chinese equipment in there." Jim explains that these transformers have hardware backdoors that can be exploited, very possibly resulting in a regional blackout.

CLICK HERE to listen to this entire podcast episode.

Are We Getting In Our Own Way?

Inaction, hesitation, finger-pointing, and indecision are blocking critically necessary measures that can prevent a terribly impactful event. Suppliers compete with others on pricing, so tight utility budgets compel purchasers to buy from the lowest bidder. A utility leader's authority is limited by the corporate leaders and compliance regulations. Corporate leaders are answerable to federal mandates and guidance, so the merry-go-round keeps spinning.

As authorities within various levels struggle to identify ownership and accountability, individuals are stepping up to offer their voices, and to find solutions that may save some necks (and lives). End-to-end OT cybersecurity is immediately attainable without breaking the bank.

About Us

Blue Ridge Networks is a proven and trusted provider of cybersecurity breachprevention solutions. Our mission is to provide proactive protection of critical infrastructure that eliminates the adverse impacts associated with reactive responses to compromises.

Our unique CyberCloak capabilities secure critical assets and operations in zero-trust IT/OT network architectures. Regulated, Commercial, and Industrial organizations have trusted Blue Ridge Networks for over 20 years to prevent exploits and receive continuous returns on their investments while achieving uninterrupted operational efficiency.

BLUERIDGE®
NETWORKS

1-800-704-5234
sales@blueridgenetworks.com
BlueRidgeNetworks.com

f X in