Why Everyone Needs to Brace for Cyberattacks Disabling U.S. Power Grids

By: Michael Snyder

What would you do if the power grid where you live went down and there was no electricity for an extended period of time?

You might want to think about that, because experts are warning that it is just a matter of time before cyberattacks successfully cripple our power grids. In fact, foreign hackers are working hard to infiltrate critical infrastructure as you read this article. As you will see below, we are extremely vulnerable, and the Russians and the Chinese have both developed highly advanced cyberwarfare capabilities.

When the U.S. ends up fighting a war with Russia or China (or both simultaneously), devastating cyberattacks on our power grids will be conducted. When your community is suddenly plunged into darkness, what is your plan?

The United States and Canada are not covered by a single power grid.

Rather, there are multiple grids that collectively provide the electricity that all of us need. The following explanation comes from Wikipedia:

“The electrical power grid that powers Northern America is not a single grid, but is instead divided into multiple wide area synchronous grids. The Eastern Interconnection and the Western Interconnection are the largest. Three other regions include the Texas Interconnection, the Quebec Interconnection, and the Alaska Interconnection. Each region delivers power at a nominal 60 Hz frequency. The regions are not usually directly

connected or synchronized to each other, but there exist some HVDC interconnectors. The Eastern and Western grids are connected via seven links that allow GW to flow between them. A study by the National Renewable Energy Laboratory found that increasing these interconnections would save energy costs."

Bloomberg is reporting that "US power grids are facing heightened risks of cyber and physical attacks as the election nears," and one expert is warning that there is "a 100% chance" that critical infrastructure will eventually be breached at some point: "I think there's a 100% chance that organizations in the critical infrastructure space at some point will experience some short of breach," said Stephanie Benoit Kurtz, lead cybersecurity faculty at the College of Business and Information Technology at the University of Phoenix. "No longer are the days when organizations can say, 'We'll never be breached.' It's not if, it's when."

Sadly, I believe that she is quite correct.

Breaking News. Spirit-Filled Stories. Subscribe to Charisma on YouTube now!

We should have never exposed our power grids to the Internet, and now we are incredibly vulnerable.

During a recent congressional hearing, FBI Director Christopher Wray publicly admitted that Chinese hackers have been targeting our power grids.

> *FBI Director Christopher Wray said Wednesday that China's hackers are targeting American critical infrastructure, including water treatment plants, pipelines and the power grid, to be able to "wreak havoc" in the U.S. if Beijing ever decides to do so.*
>
> *Testifying before the House Select Committee on the Chinese Communist Party, Wray also warned that there has been too little public attention on the threat that he says China's*

> *efforts pose to national security.*
>
> *"China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if and when China decides the time has come to strike," Wray told lawmakers.*

This is a very real threat.

The moment that China invades Taiwan, the U.S. and China will be at war.

And the Office of the Director of National Intelligence has warned that "If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide."

Most Americans don't realize that the groundwork for such cyber operations is already being laid. For example, last August Chinese hackers specifically targeted the Texas power grid.

> *The report says that, in August, hackers attempted to access the computer systems used by the Public Utility Commission of Texas, or the PUC, and the Electric Reliability Council of Texas, or ERCOT, which operate the state's power grid. Most of Texas is on its own power grid, separate from the grids used by most of the country.*

If you think that our systems are secure, you are just being delusional.

Get your FREE CHARISMA NEWSLETTERS today! Stay up-to-date with current issues, Holy Spirit news, Christian teachings, Charisma videos & more!

The truth is that we are extremely vulnerable, and the North American Electric Reliability Corporation admits that the number of weak spots is growing with each passing day.

> *U.S. power grids are increasingly vulnerable to cyberattacks, with the number of susceptible points in electrical networks increasing by about 60 per day, the North American Electric Reliability Corporation (NERC) said in a webcast on Thursday.*
>
> *The grids' virtual and physical weak spots, or points in software or hardware that are susceptible to cyber criminals, grew to a range of 23,000 to 24,000 last year from 21,000 to 22,000 by the end of 2022, executives with the energy regulator said.*
>
> *"It's very hard to keep pace with addressing all those vulnerabilities," said Manny Cancel, senior vice president of NERC.*

But foreign entities wouldn't even need to gain access through a weak spot if there are already back doors in place.

According to one analysis, "about 90% of software used to manage the U.S. power grid is linked to Russian and Chinese developers":

"Orlando-based Fortress Information Security explained that any 'kid' with internet can contribute their 'block' that then can be developed into software used in America's critical infrastructure. A "block," one of these code components, can risk the whole structure—our energy grid.

"A Chinese agent or a Russian agent can install backdoors into one of these components. And then unbeknownst to a software manufacturer, you grab this component, which has been tampered with and poisoned by Russian or Chinese actor and now they put that component into their software, and it ends up in our electrical grid or, or an oil rig," said Alex Santos, CEO of

Fortress Information Security.

“The company analyzed nearly 8,000 of these open-source components. Thirteen percent had contributions from Russia and China. Fortress found about 90% of software used to manage the U.S. power grid is linked to Russian and Chinese developers—something that can make it three times as likely to contain critical vulnerabilities.”

How in the world did we allow that to happen? Are we really that incompetent? I was floored when I first read that. I had no idea that we were so vulnerable.

Of course, it isn’t just our power infrastructure that is being targeted. According to Politico, Europe has been “inundated” with cyberattacks since Russia invaded Ukraine.

> *Thousands of cyberattacks have inundated Europe’s energy grid since Russia’s invasion of Ukraine, and a top industry leader is calling for help as officials and researchers fret that not nearly enough is being done.*
>
> *“The crooks are becoming better by the day, so we need to become better by the day,” Leonhard Birnbaum, the chief executive of , one of Europe’s largest utilities, said in an interview. “I’m worried now and I will be even more worried in the future.”*

Thank you for visiting . To enjoy the rest of this MyCharisma post, please visit this link:

Michael Snyder’s *new book entitled* “Chaos” *is available in paperback and for the Kindle on , and you can check out his new Substack newsletter right here.*

Join Charisma Magazine Online to follow everything the Holy Spirit is doing around the world!