THE HILL

GETTY IMAGES

The escalating threats to infrastructure confirm our need to harden electric grid

By Suedeen Kelly

• It's official: The U.S. Department of Homeland Security and the FBI confirmed this month that our nation's nuclear, energy, water, aviation, and critical manufacturing sectors as well as some government entities have been the targets of repeated cyberattacks dating back to at least May 2017.

In a "joint technical alert" circulated by email, the agencies said that attacks had compromised some of the targeted networks, but they did not describe the extent of the infiltration or damage or identify any specific victims.

The existence of these threats is no surprise — a confidential report made public in June detailed a narrower set of activities aimed at the nuclear, energy and manufacturing sectors that U.S. authorities had been monitoring for months.

But this new report — and widely circulated warning — provides insight into a much larger, escalating threat.

DHS described the attacks as "a multi-stage intrusion campaign" designed to infiltrate low security and small networks to gain access and then move laterally to the networks of "major, high value asset owners within the energy sector." DHS said it is confident that the campaign is ongoing, and hackers are actively pursuing the long-term objective of being able to access and manipulate the computer networks of their targets.

Central to any scheme to damage industries and handicap the U.S. economy is the ability to manipulate or control our national power grid – the vast, highly inter-connected network of power plants, wires, poles, transformers and cables that deliver our nation's lifeblood — electricity — to hundreds of millions of homes, businesses and critical service organizations every minute, every day. We need look no further than the massive impact of recent hurricanes in Florida and Puerto Rico to understand the price of being without power.

The unfortunate reality is that the national electric grid is vulnerable to a variety of potential attacks, natural and man-made, and every U.S. president since 1990 has acknowledged that fact and pledged to promptly address the looming potential risks. But little has been done at the federal level to develop the kind of comprehensive policy, process and financing mechanisms that are necessary to ensure the grid is made as robust and resilient as today's threat demand.

To be fair, many entities have been working to make grid improvements over the last decade, including electric utilities, which own and maintain much of the grid, as well as system operators and state and federal regulatory agencies. But those efforts need to expand exponentially, and they need to be well-coordinated and funded on a national scale. Absent cohesive, focused leadership and funding, scatter-shot grid upgrades will likely only achieve limited success over an extended period of time.

What we now need to do is establish a large-scale public-private partnership that brings together the necessary expertise — utilities, system operators and technology companies — and financing — Congress, regulators and the private markets — to focus on making the electric grid more robust and resilient in the near-term.

Improving the grid also supports and ensures resilience in the other key infrastructure areas that we now know are being targeted by cyberattacks — the nuclear, water, aviation, and key manufacturing sectors — all of which rely on an adequate and reliable supply of electricity to perform their critical functions.

The good news is that advanced technology — physical and digital — is making grid improvements easier than ever before. What we now need to do is establish a large-scale public-private partnership that brings together the necessary expertise — utilities, system operators and technology companies — and financing — Congress, regulators and the private markets — to focus on making the electric grid more robust and resilient in the near-term.

Developing that partnership, and creating a national grid enhancement program that meets our current and future needs and challenges, will require four components:

• An independent, thorough and candid assessment of exactly where improvements and upgrades are needed, in order of priority, to be completed as soon as possible;

• Development of a collective national plan based on the independent assessment and codified by Congress, with oversight from the federal regulatory agencies with infrastructure responsibility, to drive key short- and long-term grid improvements;

• Regulatory reform, including the development of improved, uniform standards for the North American bulk power system that rise to the level of detail and rigor required to meet the threats we face; and,

Identification of public and private funding mechanisms, including the potential use of tax-exempt government bonds, to raise the necessary financing in an equitable manner.

The time for government and the private sector to work together to produce a meaningful plan that addresses this imperative is now. As DHS and the FBI just warned, the threats are increasing every day, and the consequences of inaction are unacceptable and unnecessary. We have the expertise and the technology, and we must now marshal the national will.

Suedeen Kelly served as a member of the Federal Energy Regulatory Commission from 2003-09. She provides regulatory counsel to Protect Our Power, a not-for-profit organization whose mission is to strengthen the reliability and resilience of the U.S. electric grid.