the Mobilist

Follow 4.4K Followers About

Could Your Electric Vehicle Be Sabotaged?

In a silent cyberwar, rival nations are already embedded in each other's power grids

Steve LeVine 15 hours ago · 4 min read ★

In Mumbai, awaiting power so a commuter train can resume. Photo: Anshuman Poyrekar/Hindustan Times/Getty

leading nations appear to be deliberately unmasking their ability to take down each other's electric power systems in catastrophic cyberattacks.

In the latest example, a new report implicates China in a cyberattack that knocked out the power to the Indian business capital of Mumbai. On October 12, amid a four- to five-day attack on infrastructure across India, the power went out for up to 12 hours in Mumbai, closing down commuter trains, offices, the stock market, and hospitals. Immediately after the attacks, Indian media began to quote anonymous officials blaming China, which they said was retaliating over deadly skirmishes on their shared border. Now, the report, released Sunday by the Massachusetts cyber research firm Recorded Future, validates some of the suspicions of China's role without stating flatly that Beijing carried it out.

It's an example of what's going on globally: Russia is already embedded in the U.S. grid, and the U.S. is perched within Russia's. North Korea is also in the U.S. electric system. Iran has been trying to be, and China may be as well. Law enforcement agencies also worry about threats to the U.S. grid by right-wing groups and militants around the world.

All appear to have one idea in mind: To be prepared to inflict the Stone Age on their foes should the right provocation arrive. Short of that, their message is "don't push me around too much—or else."

"We are all familiar with normal war, like World War II and the Cold War. We are now entering a new phase: soft, cold cyberwar," says Stuart Madnick, a professor and cybersecurity expert at the Massachusetts Institute of Technology. "This is all a kind of prodding. It's like, 'See what we can do? Imagine what we could do if we were serious.' They have all tried to keep it not so severe as to [not] prompt the victim to retaliate in a massive way."

One nightmarish potential cataclysm, according to Rand and others including Madnick, would be sabotage that took weeks or months to repair, shutting down communications and business, panicking people, and perhaps igniting social mayhem. Our current age may be particularly susceptible to absolute disorder in such an attack: In this new paper,

Not much thought, however, seems to have been put into what would happen to the movement of people and goods in a new age more reliant on electricity. Over the coming decade, automakers, industry researchers, and governments are forecasting a massive expansion of electric vehicles (EVs) into a mass market; up to 26 million vehicles in annual sales by 2030 or 28% of the U.S. total. But an attack on the power grid would strand the entire fleet. In an announcement today, Volvo became the latest to announce that it would be all-electric by 2030.

"I hope that in the event of an attack on U.S. electrical grids, emergency response teams would have backup options for charging their electric vehicles in the way that hospitals have backup generators," says Ainikki Riikonen, an analyst with the Center for a New American Security.

In the months before the Mumbai attack, China and India had been skirmishing on their border with clubs and rocks in June, leaving dozens dead. Four months later, according to Recorded Future, Chinese hackers began to infiltrate multiple Indian entities in government, the military, and the private sector. The hackers, which the report calls "RedEcho," targeted 10 power generation and transmission organizations across the country, in addition to two seaports. Mumbai was the only apparent live target.

Russia has set the standard for the grid attack: In cyberattacks in 2015 and 2016, Moscow disrupted electric power to neighboring Ukraine. Currently, the Biden administration is said to be readying a response of some nature on Russia over the so-called "SolarWinds" attack, Moscow's suspected incursion into utilities, government agencies, and 100 companies.

Mat Burrows, director of the Foresight, Strategy, and Risks Initiative at the Atlantic Council, doubts China, Russia, or the United States would move to bring down each other's electric systems, simply because they would fear major retaliation. Smaller countries, including U.S. allies, could fall victim. Still, Burrows doesn't expect the United States to want to negotiate rules of the road for how cyber power is used. "My sense is that while decrying how Russia and China use and abuse their cyber reach," Burrows

As Texas showed last month, the electric grid is already fragile. A solar storm, such as one that struck Earth in 1859, could knock out power around the world and keep it down. But humans are worsening the existing threat of natural disaster. One thing that worries MIT's Madnick is hackers getting into a large, digitally connected fleet of autonomous vehicles. "Imagine 100,000 cars all taken control of," he said. "They can recognize people or trucks but are reprogrammed to hit them. Is it technologically feasible — definitely."

Electric Car | Lithium Ion Battery | Autonomous Cars | Cybersecurity | Cyber Warfare