The Christian Science Monitor

Opinion: Squirrels are bigger threat than hackers to US power grid

By Space Rogue, Contributor JANUARY 6, 2016

While fresh reports of digital assaults on critical infrastructure facilities have stirred the cyberwar saber rattlers, it's worth remembering that squirrels cause far more destruction to the grid than rogue nation hackers.

The cyberwar drumbeaters have been stoking fears for decades about the potential of cyberattacks causing devastating physical damage. A litany of anonymous government officials quoted in articles regularly warn about coming digital strikes on power plants, gas pipelines, or water treatment plants. The perpetrators, they say, will be rogue nation hackers executing malicious code to pull off some kind of "Cyber Armageddon."

But until recently no such attacks have ever been confirmed and nothing approaching the kind of physical destruction the doomsayers foretell has taken place. And even though two

recently reported incidents – one at a small New York dam and another involving a Ukrainian power plant – may qualify as real cyberattacks on critical infrastructure, recent history suggests we should all be wary of pointing to these incidents as signs that cyberwar is somehow imminent.

Every time stories in the media emerge about computer attacks that cause physical damage – usually supported by anonymous sources – eventually more reasonable people investigate those claims and disprove theories involving destructive cyberattacks.

One of the most commonly cited – yet erroneous – cyberevents involves several blackouts that affected Brazil between 2005 and 2007. The story goes that blackouts were the work of hackers. Even "60 Minutes" repeated that claim. Brazil's National Agency for Electric Energy, however, concluded that sooty insulators caused the power outages.

Then there was the 2008 explosion of the Baku-Tbilisi-Ceyhan (BTC) pipeline in Turkey. No less than four unnamed sources claimed it was a cyberattack despite the fact that the pipeline owner said the valves involved in the blast weren't attached to any network.

Ever since Stuxnet, the computer worm discovered in 2010 that damaged the Iranian nuclear program, many experts have warned that torrent of other computer attacks on critical infrastructure would follow.

They had a smoking gun the following year when Russian hackers broke into a small Illinois water facility. While the plant's control systems were accessed by someone in Russia, that someone was the contractor for the water facility who happened to be on vacation in Russia at the time.

Even though Stuxnet is the only confirmed cyberattack leading to physical damage, a German incident is often lumped into the category of hacks that lead to property destruction.

Many news articles and German government reports suggested that cyberattackers caused "massive damage" at an unnamed steel plant by causing the blast furnace to malfunction. And, again, no one has gone on the record confirming this story and the steel plant remains unnamed. While this event has not been conclusively disproven, there are enough missing facts to raise considerable doubt.

But over the Christmas and New Year's holiday, news stories about two more incidents are once again stirring up the cyberwar hawks.

The first event occurred at the Bowman Avenue Dam near Rye, N.Y., which is about 20 miles north of Manhattan. It actually occurred in 2013 but unnamed officials (surprise) speaking to The Wall Street Journal attributed some kind of breach of the dam's computers to Iranian hackers.

While the facts about what actually transpired at the dam are few, the incident did cause the Department of Homeland Security to investigate. But exactly what DHS discovered the extent of the so-called "attack," or how the incident was attributed to Iran remains unknown. What's more, the dam has no electrical generation capability and its only electronically controlled item is a flood control sluice gate, which dam officials say has never been fully operational.

More facts are available surrounding the Christmas Day attack in Ukraine in which the regional power company blamed malware for turning off substations. Normally, such claims would be met with deserved skepticism from cybersecurity pros. In this case, however, a sample of the malware has been found, which to people who research such things is considered pretty damning evidence. But there's still debate as whether the introduction of the malware into the power company's systems was the work of a nation state, cybercriminals, or simply a random infection that occurs in all kinds of systems daily.

So despite all the hype, fear, uncertainty, and doubt, we still don't have confirmed, indisputable cases of someone causing a power outage, or other major infrastructure damage, as a result of a cyberattack.

In fact, according to a former deputy director of the National Security Agency, the biggest threat to the US power grid isn't a cyberattack at all. It's a squirrel.

Yes, squirrels and other animals cause hundreds of power outages every year and yet the only confirmed infrastructure cyberattack that has resulted in physical damage that is publicly known is Stuxnet.

Perhaps we should focus less on cyberattacks and more attention to these furry adversaries.