# Damage to our power grid could be our biggest threat

March 2, 2017
Randy Bright

It hardly seems possible that so much time has passed that I can say that if you are in your early twenties or older, you might remember all of the chaos and concern that took place for a few years before the passage of the year 1999 to the year 2000.

Y2K was the acronym that was used to describe the year 2000 and the work that had to be done to prevent a complete nationwide meltdown.  Predictions of rampant riots in the streets and starvation were expected because most computer systems were programmed with the thought that they would no longer exist in 2000, and their internal clocks would cause the computers to malfunction if they were not reprogrammed in time.

When nothing happened at 12:00:01, everyone breathed a sigh of relief and went on with life as if nothing had happened, and there were those that thought that it had all been nothing but a farce.  The truth is that billions of dollars had been spent by corporate and private citizens reprogramming computer systems so that nothing would happen.

The point is, the threat was quite real, and we did something about it.  Unlike the myth of global warming, there was good science behind the warnings that Y2K was actually a serious threat and that preemptive actions were warranted.

Now there is another threat that we need to give our attention.

Most of us have heard of an EMP bomb, essentially a nuclear weapon that is detonated at a very high altitude, producing an electromagnetic pulse.  The EMP has the potential of knocking out almost all of our computers, including those that run our cars, aircraft, and the power grid itself.  While this is entirely possible, I don't fear that this is likely to happen, and the reason is simple – there is a much easier way for a terrorist to take out our power grid.

Ted Koppel, in his book Lights Out, explains how.  His entire book is worth reading, but here are some excerpts from the book and an abbreviated explanation.

"One hot summer afternoon in August 2003, a high-voltage power line in northern Ohio brushed against some overgrown trees and shut down… As system operators struggled to diagnose the problem, three other lines failed in the same way, forcing the surrounding grid to take on additional current. In just an hour and a half these overburdened lines fell like dominoes, resulting in the largest blackout in North American history.  Fifty million people lost power for up to two days in an area that spanned southeastern Canada and eight northeastern states."  The cost of repairs was $6 billion and 11 people died as a result of the outage.  But the system worked – the repairs were made and power was restored.

In 2013, a terrorist attack at the Metcalf Transmission Substation owned by Pacific Gas and Electric Company. A little before 1 a.m. on April 16, terrorists opened a metal vault and cut the fiber-optic telecommunications cables it contained. Using AK-47's over a 19-minute period of time, the terrorists then began shooting at the substation and caused enough damage to knock out seventeen giant transformers. An obvious planned attack, the terrorists left just one minute before police arrived, and were never caught.

Despite the damage, the attack did not succeed, and may have been simply a test. Power was rerouted to avoid a large blackout, so the system worked. They were able to continue to provide power for the twenty-seven days it took to make repairs and get the substation back online.

During the George W. Bush administration, an attack code named Olympic Games was launched against several thousand nuclear centrifuges in Iran. The centrifuges were located at Natanz, Iran's main uranium enrichment center. These centrifuges spun at very high speeds, refining the uranium so that it could be used in nuclear reactors or for bombs.

It is rumored that the operation was a joint effort between the United States and Israel in order to slow down or destroy the centrifuges. There was no physical attack on the facility, only the introduction of a computer worm code-named Stuxnet.

Stuxnet caused the centrifuges to spin at rates that caused them to self-destruct: "The genius of the U.S.-Israeli attack lay in its ability to conceal the sabotage." According to David Sanger, who reported on Olympic Games for the New York Times, Stuxnet "also secretly recorded what normal operations at the nuclear plant looked like, then played those recordings back to plant operators…so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart."

These incidents may seem unrelated, but I will pull them all together in next week's article.



Randy W. Bright, AIA, NCARB, is an architect who specializes in church and church-related projects. You may contact him at 918-582-3972, rwbrightchurcharch@sbcglobal.net or www.churcharchitect.net. ©2017 Randy W. Bright