RUSSIA'S POWER TRIP

- 15.06.2017

Slate (15 June 2017)
Russian hackers have developed a cyberweapon that can disrupt power grids, according to a report widely publicized this week. In fact, the tool is nothing new □□□ has been around in various forms for a decade—but its implications are every bit as frightening as the headlines suggest.
The first test of such a weapon, its worth noting, was devised by the United States government. On March 4, 2007, the Department of Energy conducted an experiment □□□□□□ the Aurora Generator Test □□□ see whether a hacker could destroy a physical object through strictly cyber means. The test was the brainchild of Michael Assante, at the time the chief security officer for American Electric Power, which delivered electricity to millions of customers throughout the South, Midwest, and mid-Atlantic.

A few years earlier, as a Navy officer, Assante had worked on government commissions studying the vulnerability of the nations critical infrastructure □□□□□□□ and finance, transportation, telecommunications, gas and oil, water supply, and, yes, electrical power. The workings of these assets were increasingly run by automated control systems, which several commissions had warned were vulnerable to cyber attack.

When Assante joined American Electric Power and informed his new colleagues of this danger, they didnt believe him. Yes, they said, someone could hack into a power plant or grid and cause a brief blackout, but a technician would replace the circuit breaker and the power would be restored. Assante devised a test to prove them wrong. He installed a 2.25-megawatt power generator, weighing 27 tons, inside a chamber at the Idaho National Laboratory. An IT technician wrote a piece of malware □□□□ 21 lines of code □□□ typed it into a digital relay. The code opened a circuit breaker in the generators protection system, then closed it just before the system responded, throwing its operations out of sync. Almost instantly, the generator shook, some parts blew off, it belched out a puff of white smoke, then a huge cloud of black smoke. The machine was dead. Several officials in Washington monitored this test, and, thanks to YouTube, the rest of the world could watch it too.

Get Slate in your inbox.

This test took place shortly before Stuxnet, the joint U.S. □□□□□□□ operation that destroyed the centrifuges in Irans Natanz nuclear reactor by hacking into the control system and then speeding up or slowing down the rate at which they spun. The Aurora Generator Test was what convinced several skeptical officials that a cyberattack □□□ simple insertion of malware □□□□□ not only manipulate a computer but destroy an object that the computer controls.

The Russian tool □□□□□ as CrashOverride, Industroyer, or Electrum □□□□□□ work in precisely the same way as the malware in the Aurora Generator Test. In some applications, the Russian version sends commands that open circuit breakers when they should be closed; in others, circuits are de-energized through a variety of means.

Russia launched such an attack against the power grid in western Ukraine, first in 2015 and more recently this past December. The modern bit is that, in the decade since Aurora and Stuxnet, the Russians □□□ presumably a few other nations, including the United States □□□□ figured out how to hack into these systems through a number of routes, in case the first one they try is blocked. The basic idea, though, is the same, and this sort of vulnerability pervades all systems that are run or monitored by automated controls □□□□□ almost all the systems that make up our critical infrastructure.

One bit of good news, sort of, is that nearly every nation with advanced technology has followed the same path that we paved in embedding these controls into the foundations of our socioeconomic life. Michael Assante, who is now a director at the SANS Institute, a cybersecurity training organization, told me, The majority of power systems rely on the same control system technologies available through global vendors. Even older, locally built components, he says, typically perform the same way and usually share the same vulnerabilities as the standard market-based solutions.

In other words, whereas 20 years ago Americans were nearly the only people on Earth living in digital glass houses, now much of the world lives in them too □□□□□□□□□ Russians (and the Chinese and, as we learned with Stuxnet, Iranians). As a result, without anyone making a strategic decision about this, we have all entered into a state of mutually assured destruction when it comes to major cyberattacks. As with the decadeslong nuclear standoff, if Side A attacks Side B, then Side B will strike back at Side A—and therefore both sides might be deterred from attacking each other.

The Russians shut down western Ukraines power grid, in part, because they knew that Ukraine had no ability to strike back. That wouldnt be the case if the Russians shut down a stretch of Americas power grid. But that isn't cause for relief. Unlike missile attacks, where the trajectorys arc can be traced precisely, cyberattacks can be hard to pin down; it may take a while to figure out where the attack came from, and even then its not always clear who launched it. Before firing off a retaliatory attack, it would be good to know the proper target. Big wars have grown out of small misunderstandings. Then theres the problem of rogue actors □□□□□□□□□□ criminals, or mischief-makers □□□ simply want to disrupt the existing order and have a fairly good idea of how to cover their tracks.

Meanwhile, 10 years after the Aurora Generator Test (which only confirmed the reports of commissions formed 10 years before then), too few of the private companies that own and operate our critical infrastructure have taken steps to guard against these sorts of attacks. Some sectors have taken enormous steps, chief among them banks □□□□ for good reason: Banks need your money and your trust, and they have the money to hire large teams of cybersecurity specialists. Cyberattacks are an everyday occurrence, and cybersecurity is a central piece of their business model. This is not the case with electrical utilities, whose executives see cyberattacks as a hypothetical danger. Many of them have also calculated that the cost of preventing an attack is almost as large as the cost of cleaning up after an attack □□□□ the preventive measures might not really prevent one—so why bother to make much of an investment?

When the fear of cyberattacks first materialized, President Bill Clintons cybersecurity adviser tried to impose mandatory cybersecurity regulations on critical infrastructure companies. These attempts were quashed by lobbyists and by White House economic advisers. Now we are living with the consequences □□□□ a new form of risk that too many of those in charge are ignoring at their, and our, peril.

Kaynak/Source: