FEATURE

Catastrophic cyber attack on U.S. grid possible, but not likely

Anything is possible in the cat-and-mouse game of probing and protecting the online weaknesses of the nation's critical infrastructure. But security experts say the U.S. grid is resilient enough to make a "cyber Pearl Harbor," highly unlikely

CSO

By Taylor Armerding | Follow

CSO | Apr 15, 2016 3:45 AM PT

Warnings about U.S. critical infrastructure's vulnerabilities to a catastrophic cyber attack – a cyber "Pearl Harbor" or "9/11" – began more than 25 years ago. But they have become more insistent and frequent over the past decade.

Former Defense Secretary Leon Panetta warned in a 2012 speech of both a "cyber Pearl Harbor" and a "pre-9/11 moment."

They have also expanded from within the security industry to the mass media. It was almost a decade ago, in 2007, that the Idaho National Laboratory demonstrated that a cyber attack could destroy an enormous diesel power generator – an event featured in a 2009 segment on the CBS news magazine "60 Minutes."

How to respond to ransomware threats

Late last year, retired "Nightline" anchor Ted Koppel warned in his book "Lights Out" of possible catastrophe – thousands of deaths – if the U.S. grid is ever taken down by a major cyber attack.

And just this month, the FBI and Department of Homeland Security (DHS) launched a national campaign to warn U.S. utilities and the public about the danger from cyber attacks like the one last December that took down part of Ukraine's power grid.

The worst-case scenario, according to some experts and officials, is that major portions of the grid could go down for months, or even a year.

Yet, nothing close to that has happened yet – the damage over the past decade from natural disasters like hurricanes, tornadoes and earthquakes has been much more significant than any cyber events.

All of which raise the obvious question: Why? If a hostile nation state like Iran could deal the "Great Satan" a crippling blow, why wouldn't it?

[ALSO ON CSO: Defining the threat in the energy sector]

There are several theories to explain it. One is that even countries like Iran or a rogue state like North Korea would not want to take down the U.S. economy because it would have a drastic negative effect on the world economy.

"The same interdependencies that exist in the global economy could have unintended global consequences, were any nation to suffer widespread disruption to foundational systems," said Anthony Di Bello, director of strategic partnerships for Guidance Software.

Anthony Di Bello, director, strategic partnerships, Guidance Software

Another is that hostile nation states are more interested in espionage than an attack, in the hope that knowledge of U.S. infrastructure systems will give them some leverage in foreign policy disputes, or prevent a country like the U.S. from ever attacking them with conventional weapons.

Yet another is that if other countries are inside U.S. systems, the U.S. must be inside of theirs, which creates the equivalent of a cyber "balance of terror" – the U.S. could do as much or more damage to them in response to an attack.

As Jason Healey, senior fellow at the Atlantic Council, put it, "cyber deterrence is working. They (hostile nation states) haven't attacked our cyber systems for many of the same reason they haven't sent nuclear-tipped missiles: They have no reason to unless the world is in a serious crisis, not least because they know there would be a dangerous counterattack from the U.S."

Indeed, there is general agreement that destructive cyber attacks are unlikely unless hostile nations are heading into war – an armed conflict.

"If any large country truly becomes a national security threat to another large country it may well be far more likely than it would be in today's climate," Di Bello said. "Barring that, it would be unlikely."

For that reason, major cyber attacks are much more likely in areas where there is already armed conflict, or the potential for it. Robert M. Lee, cofounder of Dragos Security and a former U.S Air Force cyber warfare operations officer, noted that the attack on Ukraine's grid, widely attributed to Russia, was, "simply an extension of what was going on with the military.

Jason Healey, senior fellow, the Atlantic Council

That, he said, would increase the likelihood of attacks between countries like North and South Korea, or between Iran and Israel – "traditional conflict areas," as he put it.

Of course that leaves out terrorist organizations that don't represent any nation state and which give no indication that it would trouble them at all to take down the world economy.

[MORE: Protecting vital electricity infrastructure]

But Lee and other experts said this week that smaller organizations – even lethal terrorist groups like ISIS – don't have the same capability as nation states. They say while the U.S. grid and other industrial control systems (ICS) have significant weaknesses – and U.S. adversaries are constantly probing those weaknesses – launching an effective, sustained attack is not as easy as some people, including high government officials, suggest.

"It is significantly more difficult to do a high-confidence attack on ICS than people think," Lee said "It doesn't just involve the cyber component – it's the engineering piece as well."

Al Berman, president of Disaster Recovery Institute, agreed. He said one reason is that, over the past decade, there has been "tremendous sharing" about threat information among utility companies. The ICS ISAC (Information Sharing and Analysis Center) is "enormously strong," he said.

A second is that most ICSs are not completely automated. "The big ones still require manual intervention," he said. "There are manual bypasses occurring all the time – people are manning centers around the clock."

That, he said, makes it more difficult for attackers to get control of a system remotely.

Third, he said, is that most utilities are privately owned and have different software, applications and system designs. That diversity makes it much more difficult to launch a coordinated attack on multiple systems.

Dr. Paul Stockton, managing director at Sonecon, made that point in a recent paper titled "Superstorm Sandy: Implications for designing a post-cyber attack power restoration system."

He wrote that the diversity of systems would likely impede recovery efforts after a major attack, but would also have the benefit of making large-scale attacks much more difficult in the first place.

> "The enormous diversity of ICS software and control system components among utilities greatly complicates the task of conducting a 'single-stroke' attack to black out an entire interconnect or the U.S. grid as a whole," he wrote.
>
> And according to Lee, even with all that diversity, critical infrastructure systems are relatively simple to defend. "They are among the few networks on the planet that are defensible," he said.

Dr. Paul Stockton, managing director, Sonecon

Added to that, said Lila Kee, chief product officer at GlobalSign, is that utility providers are very much aware of the threats, and highly motivated to defend against them.

“Grid providers don’t want to be any more regulated than they are, and they understand if they don’t address cyber security vulnerabilities, the government will do it for them,” she said. “It’s also important to note that grid providers have a self interest around protecting generation and transmission systems.”

Lila Kee, chief product officer, GlobalSign

Berman contends that “the mundane things – like cable backhoes – cause us more problems than cyber.”

While the risks are real, “I spend a lot of time with utility people,” he said, “and they are dedicated and understand where attacks are taking place. I tend to be an optimist – I’m not so sure we’re as ill-prepared as everybody thinks.”

All this, experts hasten to add, does not mean that ICS defenses are adequate. As has been noted many times, they were not originally designed to face the Internet. And the interconnection of ICS networks to gain automation and efficiency has simply expanded the attack surface.

And, as both Lee and Stockton note, if there is a major cyber attack, responding to it will be much more complicated than to a natural disaster like Superstorm Sandy. In that case, other providers who came to assist those that had been damaged by the storm, knew they would not confront the same storm themselves.

With a cyber attack, as Lee put it, “the adversary will be fighting your responders,” in much the same way that terrorist groups sometimes detonate one bomb, wait for others to rush in to assist victims, and then detonate another one.

The most crucial point, Lee said, is that, “everything that everyone is talking about is speculation, because we’ve never seen it (a major attack).”

Another problem he sees is that there were no collective, international warnings to the perpetrators of the Ukraine attack.

“We didn’t even have to say we knew who did it,” he said, “but we should have said that whoever did it, be warned that this is an unacceptable act that will bring severe consequences.

“This was an attack on a completely civilian infrastructure, and now it is seen as permissible. It’s going to embolden attackers.”

Stockton also warns that while terrorist organizations may lack the capability to launch a crippling cyber attack now, that may not always be true.

“They have access to Dark Web and zero days to increasing extent,” he said. “And they are becoming increasingly sophisticated. We’re in an arms race. We continue to strengthen resilience, but we need to accelerate our efforts to defend and respond.”

Lee agreed, saying that while things are improving in securing critical infrastructure, “it’s not happening nearly as fast as it should be.”

Taylor Armerding

Insider: Survey: With all eyes on security, talent shortage sends salaries sky high

View Comments

You Might Like

Forget The iPhone 7. Next Apple Sensation Leaked
The Motley Fool

Pennsylvania: Drivers Are Stunned By This New Rule
Provide Savings Insurance Quotes

Ron Paul Issues Warning On Gold
Stansberry Research

Sports Bras That Are Actually Cute (With Extra Support Too!)
Fabletics

There Are 7 Types of Irish Last Names - Which One Is Yours?
Ancestry

7 Outrageous Credit Cards If You Have Excellent Credit
NextAdvisor

Worst Exercise For People Over 35
MAX Workouts Fitness Guide