Wireless
April 13, 2009 4:00 AM PDT

How secure is the U.S. communications network?

by Marguerite Reardon

A simple snip of a few fiber-optic communications cables left thousands of people in Silicon Valley and throughout parts of the San Francisco Bay Area without phone, Internet, or wireless service for more than 12 hours on Thursday.

The San Jose Police Department is investigating the incidents, which took place in two different locations in San Jose and San Carlos and classified as **acts of vandalism**. Now that the network is up and running again, people are asking how difficult is it to take down the nation's communications network? And should we be more worried about the fiber optic cables that ring our communities and crisscross the country carrying all of our communications?

"A couple of well-placed attacks could do a lot of damage to the communications network," said Sam Greenholtz, co-founder and principal of Telecom Pragmatics, a consulting and research firm specializing in the telecommunications market. "And it's not really that hard to figure out where the fiber optic cables are laid and to get access to them."

That said, Sgt. Ronnie Lopez of the San Jose Police Department said there is no reason yet to suspect terrorism in this case. But the FBI has been briefed on the case.

AT&T is **offering a $250,000 reward** to anyone who can provide information that leads to the arrest and conviction of the vandals.

"We are aggressively working with law enforcement authorities to see that those

responsible for this willful act are apprehended and prosecuted to the fullest extent of the law," the company said in a statement Friday.

AT&T also said in a press release that following the terrorist attacks of September 11, 2001, its networks were declared National Critical Infrastructures, which means that anyone who tampers with, destroys, or disrupts the company's network or its components is in violation of both federal and state laws.

Wondering about vulnerabilities

Still, with recent reports that our nation's electrical grid **has gotten less secure due to technological advances**, incidents such as this one leaves many wondering how vulnerable the communications network really is.

I talked to a few experts about how telecommunications networks are built and how they operate. And I've concluded that while it's somewhat easy to figure out where fiber is laid and to gain access to the fiber infrastructure in the ground, it's much harder to actually cause major damage unless you know what you're doing.

Let me explain. In the AT&T fiber cut case, it was fairly easy for the perpetrator to access the fiber-optic cables that were eventually cut. Sgt. Lopez said that it appeared that whoever cut the fibers simply lifted the manhole cover, went down the ladder, and cut two cables.

But knowing exactly which manhole cover to open and which cables to cut that would cause widespread damage to the network is another story.

Greenholtz, who was a former manager in the Planning and Engineering Group at Verizon where he worked for nearly 28 years, said that causing a network outage of this magnitude was likely orchestrated by someone who not only knew which manholes provided access to AT&T fibers, but also knew which places on the network were most vulnerable and could cause the most damage.

"The manhole covers are not locked," he said. "Anybody can open them and go down there. But most of these networks have redundancy and diversity built-in to the architecture, so if you cut a cable, it reroutes itself and recovers."

Greenholtz explained that someone with knowledge of the network would know the most vulnerable points in the network and could pinpoint those areas.

Built in rings

AT&T declined to discuss specifics of the company's network architecture, but experts say that the Baby Bell phone companies, such AT&T's predecessor SBC Communications, typically built their regional fiber networks in rings. The rings themselves would help provide protection against an outage, because if a line were cut, the traffic could just reverse itself in less than 50 milliseconds and go the other direction around the ring.

But the phone companies also typically ran redundant lines that are spaced some distance apart from each other, so that if one line is cut, there is also a separate fiber carrying the traffic. And to ensure that the redundant line can handle excess traffic in an emergency, most phone companies run these systems at 50 percent capacity.

(Credit: Google Maps)

The fiber-optic cables that were cut in San Carlos, which were owned by Sprint Nextel, appear to have worked in this way. The traffic was quickly rerouted to another path, and service to Sprint's business customers was not interrupted.

Unlike regional networks, which have multiple fiber rings running through and between cities, undersea cables that connect continents do not have this type of redundant architecture because it's much too expensive to build it that way. This means that undersea cables are **particularly vulnerable to fiber cuts**. But because they are deployed beneath the ocean floor, they tend to be more difficult to tamper with. That said, cables are severed and massive outages do occur from time to time.

By contrast, some networks in highly trafficked regions or networks that service critical customers have even more redundancy built into them. Michael Howard, a principal analyst at telecommunications research firm Infonetics Research, said that

carriers such as Deutsche Telekom have begun building meshed networks so that there is a third path for traffic if fibers are cut or there is some other disruption on the network.

"The more traffic there is on the route, the more redundancy the carrier provides," he said. "There are usually two aspects to a backup plan for networks. One is providing a diversity of virtual routes for the traffic, but the other is providing physically separate routes on separate fibers. I'd have to say the outage that occurred in Silicon Valley seems odd, given the traditional network architecture."

An inside job?

Indeed, AT&T's network failure seems to suggest that at least one other path that would have rerouted the traffic was also damaged or cut. Given that the police indicated that the incidents occurred in only two locations, San Jose and San Carlos, it seems likely that there was already some damage or issue happening on AT&T's network at the time the fiber was cut or the vandals managed to cut the ring in two places.

Of course, neither I nor any other expert could know this for sure. But the fact is that fibers are cut all the time in regional networks, and rarely do they cause massive outages that shut down entire regions for hours. Most of these incidents are accidents. Someone might be landscaping a yard and a back-hoe severs a cable. Or another utility worker accidentally damages a cable while working in the same manhole where communication cables are located.

"Fiber cuts happen more often than people realize," said Crystal Davis, a spokeswoman for Sprint Nextel. "It happens by accident all the time when someone is drilling or digging up a street. Or they're doing regular maintenance. We know this, and that's why traffic can be quickly rerouted."

This is also why Greenholtz believes that the AT&T fibers were likely cut by someone who knew the network and its potential weaknesses.

"If there was an ongoing maintenance issue on one side of the fiber ring that hadn't been addressed," he said. "And then the other side is cut, it would cause a major outage like the one AT&T experienced. But in order to cause that much damage, someone

would have to know that. Otherwise, it was just a very lucky vandal."

More theories

This line of thinking has caused some bloggers to suspect that the vandal was a disgruntled former or current AT&T employee.

And some have even gone so far as to suggest that the perpetrator could be an unhappy union worker. AT&T is currently in contract negotiations with its largest union the **Communications Workers of America**, which represents some 80,000 workers at AT&T. Workers have already voted to strike if a new contract can't be agreed upon. So far, no date has been set for a strike, and Candice Johnson, a spokeswoman for the union said that the two sides are still negotiating.

But Johnson also said that the union was not involved in the vandalism and that claims that its members might be involved are unfounded.

"There is no basis for speculation that our members were involved in this act of vandalism," she said. "We are cooperating with authorities. We are currently at the bargaining table with AT&T management, and our workers are on the job. Our goal is to get a contract renewed."

Sgt. Lopez from the San Jose Police Department said that it's still too early in the investigation to talk about suspects or motives.

Regardless of whether the cables were cut by disgruntled employees or random vandals, the recent incident highlights the potential for such an attack to be undertaken on a broader scale by foreign terrorists, who may infiltrate our nation's telephone companies or gain access to information about the country's communications network. But Greenholtz and other experts say that because these networks have always been built with redundancy in mind, it would take a massive coordinated effort to target individual manholes and to cut fibers.

"If you really want to take down the communications network and cause damage, you'd probably target a central office," Greenholtz said.

A central office is the nerve center of a telecommunications network. It houses all the

switching equipment and billing data for a particular region of the network. As an example, Greenholtz said that if a terrorist was able to damage Verizon's central office on 38th Street in Manhattan, communications services on Wall Street could be wiped out not just for a few hours, but likely for days, weeks, or even a month. Because these facilities are so critical, he said all the major phone companies have tight security.

"Those places have tons of security," he said. "You'd probably need Jack Bauer (of the TV show '24') to help you get in there."

Marguerite Reardon has been a CNET News reporter since 2004, covering cell phone services, broadband, citywide Wi-Fi, the Net neutrality debate, as well as the ongoing consolidation of the phone companies. E-mail Maggie.

Topics: **Corporate & legal**

Tags: **AT&T**, **outage**, **Silicon Valley**, **fiber cut**, **security**

Related

From CNET

AT&T increases bounty on fiber vandals to $250K

AT&T fiber cut disrupts service in Silicon Valley

From around the web

AT&T Increases Reward to $250,000 for In... AOL News

2 European Carriers Agree to Share Networks The New York Times