Truckers' Jammers Threaten Move to GPS-Based Aviation Navigation

By Alan Levin March 19 (Bloomberg) -- Two years ago, a new global positioning system-based system guiding jets to runways at Newark Liberty International Airport began switching off without warning. The culprits, according to government documents, were drivers on the adjacent New Jersey Turnpike who were using cheap, illegal GPS jamming devices to prevent their employers from locating them. The devices, whose signals are as much as 1 billion times more powerful than GPS transmissions, were also blanking out the airport landing system. That passing vehicles could so easily cripple airport navigation illustrates one of the U.S. Federal Aviation Administration's obstacles in its $42 billion effort, known as NextGen, to convert the nation's air-traffic control away from radar to a reliance on GPS. Wireless networks, financial institutions and power grids are also vulnerable to GPS disruption, according to studies commissioned by the U.S. government and academic experts. "The interference threats to GPS are very real and promise to get worse," the National Space-Based Positioning, Navigation and Timing Advisory Board, which is appointed by the government, said in a 2010 report. So-called spoofers may be a greater threat than jammers. They mimic signals from space and can trick a receiver into displaying the wrong location, Todd Humphreys, an assistant engineering professor at the University of Texas, said in phone interviews. "The mischief makers are looking for opportunities to prick us in our soft spots," he said. "This is a soft spot and a pretty glaring one."

Gaming Markets

Jammers and spoofers probably can't make commercial aircraft veer out of control and crash because planes have backup navigation systems, Humphreys said. A carefully calibrated attack might be more successful steering private planes and ships off course, he said. Iranian officials claimed they used this technique to capture a U.S. spy drone in December. It may also be possible to subtly alter the times in computer systems used for high-volume trading, which rely on GPS for accurate time, Humphreys said. An attacker could game the markets or to sow unrest similar to the May 6, 2010, flash crash, which briefly sent stocks tumbling, he said. NYSE Euronext, which operates the New York Stock Exchange and other global markets, has enough backups to ward off an attack, Andrew Bach, senior vice president and global head of network services, said in a phone interview.

Critical to Infrastructure

The GPS system is easily disrupted by jammers that deliberately broadcast on the same frequency and sell for as little as $25.99 on the Internet, according to government documents. Using or selling the devices is illegal, according to the Federal Communications Commission. After traveling 12,000 miles from space, the GPS signal is as weak as a 60-watt light bulb in New York would be to someone in Los Angeles, according to the U.S. government's GPS advisory board. The FCC last month vowed to block a proposal by LightSquared Inc. to create a high-speed data network that President Barack Obama's administration said would interfere with GPS devices. In 2007, the Navy accidentally jammed GPS in San Diego, knocking out wireless telephone base stations and a first- responder pager system, according to a report by the Institute for Defense Analyses, an Alexandria, Virginia-based nonprofit that does research for the U.S. Defense Department.

Jamming Widespread

In Britain, teams monitoring roadways found scores of drive-by jamming cases, according to a February presentation by Chronos Technology Ltd., which conducted a study for the U.K. government. The study estimated there are between 50 and 450 jamming cases per day across the country. Jamming against ships caused malfunctions of radar, satellite phones and other onboard systems embedded with GPS, according to studies led by David Last, a former president of the London-based Royal Institute of Navigation. Satellite navigation in aviation is less expensive to operate than existing landing systems and will save airlines money with shorter routes and fewer delays. The signal disruptions set the program in Newark back at least a year as Honeywell International Inc., which makes the system, and the FAA wrestled with how to overcome the jamming, according to an agency summary obtained by Bloomberg. The first shutdown occurred on Nov. 23, 2009, according to the document. FAA and FCC employees tracked someone using a jammer during a two-day stakeout on the turnpike in April 2010 and confiscated it. Eight days later, another jammer shut down the system, according to the FAA document. The system is running again without interference after shielding antennas from the highway, according to e-mailed statements issued by the FAA. Flight tests with the system are to resume in the summer, according to the statements.

Layers of Backup

Any new program must work through such issues in testing, Chris Benich, a vice president for aerospace regulatory affairs at Morris Township, New Jersey-based Honeywell, said in a telephone interview. The protections, while marking an improvement, can't prevent jamming, Logan Scott, a GPS consultant in Fort Collins, Colorado, said in a phone interview. The FAA is keeping layers of backups to let planes fly without GPS, according to the agency's statement. Traditional navigation beacons and radars can help guide planes in an emergency. The agency also said it is considering "various alternatives" to create a GPS-like navigation backup system.

More Enforcement

The Homeland Security Department, concerned that "U.S. critical infrastructure sectors are increasingly at risk," created a review panel in 2010 to study the issue, according to documents on the Space-Based Positioning Navigation & Timing National Executive Committee's website. The panel is charged with protecting GPS use by the U.S government. Homeland Security is developing a network of monitors for jammers and other GPS interference, according to the documents. The department didn't provide additional information. The FCC has begun more aggressive enforcement, it said in a March 6 statement. Penalties should be increased on violators caught selling or using jammers, Tom Stansell, who helped develop the GPS system starting in 1960, said in a phone interview. As a backup to GPS, the government also should resurrect a radio-navigation system known as LORAN, which Obama canceled in 2010, Bradford Parkinson, a Stanford University professor emeritus who formerly headed the GPS program at the Defense Department, said in a phone interview. The system for now remains exposed, the University of Texas' Humphreys said. "I see it as a gaping vulnerability and so do others," he said.

--Editors: Bernard Kohn, Michael Shepard; To contact the reporter on this story: Alan Levin in Washington at +1-202-624-1928 or alevin24@bloomberg.net; To contact the editor responsible for this story: Bernard Kohn at +1-202-654-7361 or bkohn2@bloomberg.net