NEWS AUG 8 2016, 3:36 AM ET

GPS Under Attack as Crooks, Rogue Workers Wage Electronic War

by MIKE BRUNKER

Once the province of hostile nations, electronic warfare has arrived with little fanfare on U.S. highways and byways.

Criminals, rogue employees and even otherwise law-abiding citizens are using illegal "jamming" devices to overpower GPS, cellphone and other electronic signals over localized areas. The devices are small and mobile — a common variety plugs into a vehicle's cigarette lighter — making it difficult for law enforcement to identify the culprits.

And experts say the threat to the Global Positioning System (GPS) — the critical space-based navigational, positional and timing network — is escalating as potentially more destructive "spoofing" devices become readily available.

Trucks and cars creep along on Chicago's Kennedy Expressway.
Scott Olson / Getty Images file

"We're highly dependent on (GPS) in pretty much every part of our economy and security, yet it's very easy to disrupt," said Dana Goward, president and executive director of the Resilient Navigation and Timing Foundation, which is urging the federal government to move quickly to better protect GPS and to develop a backup system. "... I think the general consensus is that any outage of more than an hour or two would be pretty unpleasant."

Experts have been warning for years about the vulnerabilities of GPS, a global network of 36 U.S. satellites that provides timing data for a wide array of critical infrastructure, including telecommunications, the energy grid and financial markets, as well as everyday applications like smart phone mapping and ride-sharing services like Uber.

"If there were an airline crash or a wide-scale, long-duration interruption of GPS, say in New York City, that affected the stock exchanges there, you can bet there would be a lot of people wagging their fingers and saying, 'I told you so,'" said Todd Humphreys, associate professor at the Radionavigation Laboratory at the University of Texas at Austin and a leading authority on GPS security holes.

Humphreys was referring to predictions that a widespread outage of GPS — either due to natural phenomena like solar flares or a major electronic warfare attack — would immediately cause serious slowdowns in all types of transportation, with the impact spreading through other sectors if service could not be quickly restored.

Protecting the system is difficult, as GPS signals from 12,000 miles in space are extremely faint and susceptible to interruption by jamming (interference by transmitters operating at or near the same frequency) or spoofing (tricking GPS receivers into reporting they are somewhere they are not or producing an incorrect time signal). The U.S. military, which developed GPS, uses a separate frequency band with encryption and other measures that render it more secure.

A car using a dashboard GPS device passes a speed radar sign on Highway A25 in France. Philippe Huguen / AFP/Getty Images - file

Predictably, criminals have found ways to profit from GPS weaknesses with illegal jamming devices. The devices, once available only to those with considerable technical savvy, are now widely advertised on the internet for $50 or less and require no expertise to operate.

"You put a battery in it or plug it in and turn it on. That's it," said Peter Soar, business development manager for military and defense for the Canadian firm NovAtel, which supplies positioning and timing components to a wide range of industries.

Addition to the criminal 'Armory'

As a result, experts say, the devices — which typically disrupt GPS and sometimes other frequencies over areas ranging from about 980 feet to more than 5 miles, according to one test — have become almost standard issue for villains engaged in certain kinds of serious crime like cargo theft and drug trafficking.

"Any respectable criminal involved in that kind of (cargo) hijacking is going to employ jammers as part of their armory," David Last, professor emeritus at the University of Bangor in Wales and past president of the Royal Institute of Navigation, told NBC News. "There is no reason why they shouldn't and every reason why they should."

Charles Curry, managing director and founder of the British firm Chronos Technology, cited a case in which an organized crime group used jammers to protect surreptitious shipments of stolen high-end cars to Uganda for resale.

A stolen Range Rover recovered by authorities in the U.K. in a jammer-protected cargo container. National Vehicle Crime Intelligence Service

"You must have been a really well-organized crime gang to be doing that kind of business, stealing top-end Jaguar Land Rovers from the streets of the U.K., shipping them via France (and the) Middle East to Mombasa in Kenya and then overland to Uganda," he said. "That isn't a petty criminal."

Drug traffickers also regularly use them to try to foil electronic surveillance by law enforcement or rival gangs, Last said.

Last, who frequently testifies as an expert witness in GPS jamming cases in Britain, recalled one recent incident in which the courier meeting a flight of illicit drugs from Germany at a small general aviation airport in England deployed a "very serious kit" in a suitcase, with eight antennas that jammed GPS, mobile phones, Bluetooth, Wi-Fi and the frequency used by stolen vehicle recovery systems such as LoJack.

A sophisticated eight-antenna jamming device built into a suitcase. One such "serious kit" was recently used by crooks

"I don't know if you've ever been around when Air Force One lands, but nothing electronic works for several hundred meters around," he said. "It was quite like that."

Stealing jewels with a garage-door opener

But Last said far less sophisticated crooks also are using jamming, citing a case in which "a couple very low-tech criminals" used a garage door opener to prevent a jewelry courier's key fob from locking the vehicle. They then made off with goods left inside while the courier was in a store making a delivery.

"So there's quite a mom-and-pop level of criminality that uses jammers and doesn't even know quite how they work," Last said.

U.S. authorities are generally tight-lipped about the criminal use of jamming devices, but an industry advisory issued by the FBI's Cyber Unit in October 2014 indicates they take the problem seriously.

smuggling drugs from Germany into the U.K. to knock out a variety of communications signals. Chronos Technology Ltd.

The advisory said an industry security group had reported 46 instances of car thieves' using jammers to try to avoid detection of stolen vehicles in shipping containers bound for China.

It also referred to a theft in Florida in which the thieves used jamming devices after stealing a refrigerated truck trailer filled with pharmaceuticals, in case any tracking device was hidden in the cargo. The thieves were caught by the Florida Highway Patrol during a routine vehicle stop, it said.

Separately, the shipping security firm FreightWatch reported last year that there have been at least four failed cargo thefts in which jamming devices were recovered, saying the attempted heists were the work of Cuban cargo thieves operating along the Eastern Seaboard.

That may just be the tip of the iceberg.

"We often don't know, based on what law enforcement tells us, whether a GPS jamming device facilitated and enabled (a particular) cargo theft to happen," said John Wislocki, the information manager and publisher with the American Trucking Associations' Safety Management and Transportation Security councils.

(The FBI declined an interview request from NBC News, directing inquiries to the Federal Communications Commission, the agency primarily tasked with enforcing anti-jamming laws. The FCC also declined an interview, instead pointing to a jammer enforcement web page and a 2013 forfeiture notice imposing a $32,000 fine on Gary Bojczak, a New Jersey engineer whose illegal jamming device inadvertently interfered with a test of a GPS landing system at Newark Liberty International Airport in New Jersey.)

Hiding from 'the boss'

The use of jammers has been well documented in Britain in a 2012 study known as the Sentinel Project, which used a network of detection sensors around the country to measure the frequency of the illegal activity. The BBC reported at the time that 20 roadside monitors detected 50 to 450 occurrences of jamming in the country every day.

The problem has only grown worse since then, according to Curry, whose company conducted the study with government and industry support.

In addition to documenting use of jamming devices, the study found that the overwhelming majority of them — about 9 out of 10 — were employed by fleet drivers or truckers trying to avoid monitoring by the fleet-tracking systems "because they don't want the boss to know where they are," Curry said.

That observation was bolstered by a March 2014 experiment in the United States by Rohde & Schwarz, which manufactures radio testing and measurement equipment. An instrumented van parked near a major highway adjacent to Portland International Airport in Oregon found that "about

every third or fourth truck" was radiating at or near GPS frequency, according to a presentation by GPS and communications consultant Logan Scott.

Related: North Korea Jams GPS Signals to Fishing Boats: South

Despite such anecdotal evidence, Brian Lagana, executive director of the trucking associations' safety and security councils, said he has seen no evidence that truckers are using the devices in significant numbers to defeat tracking or manipulate driving logs.

"I think, in general drivers, are well aware of the regulatory requirements ... and they're also very well aware of the penalties they could receive for use of a jamming device," he said.

In fact, Britain's Sentinel study found that many jamming culprits were at the wheels of smaller vehicles, including service and delivery vehicles and taxis.

It also documented instances of civilians with no ill intent using jammers. In one account that has become something of a legend in GPS security circles, an employee of a U.S. government agency with a mobile jamming detection device was surprised when it began alerting while he was at church.

"He went up to the priest after the service and said, 'Father, I think there's a GPS jammer in the church here somewhere,'" said Goward, who knows the official. "The father says: 'Yeah. You're darn right. I bought it to jam GPS and the cellphones because I was tired of people texting during the sermon.'" (The official declined an interview request from NBC News and requested anonymity.)

Spoofing concern growing

While use of illegal jammers appears relatively common in the field, spoofing — tricking GPS receivers by faking satellite signals — so far appears to be largely confined to electronic battlefields (Iran reportedly spoofed a U.S. reconnaissance drone that it captured in 2011) and laboratories. But that may be changing.

The closest thing to official confirmation of a criminal spoofing incident came when a Homeland Security Department official said at a security conference in December that Mexican drug cartels were trying to jam and spoof GPS signals to interfere with U.S. government drones patrolling the border.

"The bad guys on the borders have lots of money, and what they're putting money into is ... spoofing and jamming of GPS," Timothy Bennett, a DHS science-and-technology program manager, said at the Center for Strategic International Studies conference.

In an interview with NBC News in July, however, Bennett said DHS has no evidence that the cartels have actually used spoofing and that his comments were based on "what is happening in the field (and) what I know about how other people are using jammers in the United States."

Todd Humphreys, associate professor at the University of Texas at Austin. University of Texas

Humphreys, the University of Texas expert who is often consulted by law enforcement and other government security experts, said there are likely other incidents that have not been made public.

"When I get interviewed by the FBI, they often guardedly allude to incidents where jamming and even spoofing have been carried out ... but of course they don't reveal details to me," he said.

Humphreys famously demonstrated how spoofing can be used to take control of a vehicle using GPS for navigation. In June 2012, he and several graduate students demonstrated the technique for DHS officials by commandeering a civilian drone; the following year, they went after larger game — a 213-foot superyacht — and tricked its GPS navigation system into sending the vessel hundreds of yards off course in the Mediterranean Sea without raising any on-board alarms.

Those demonstrations required considerable effort and expense, Humphreys said, estimating that it took "five years and a bunch of Ph.D.s" to develop the device capable of simulating and then overpowering real GPS signals.

But that changed dramatically last year when Chinese technology experts demonstrated at the Defcon hacker conference how anyone can use a $300 software-defined radio to spoof GPS.

"There is now the capability of downloading something that's available online onto an off-the-shelf ... radio frequency card and making your own spoofer," Humphreys said. "It would be something that would only takes a few hours for someone who has a little bit of experience with radio frequency work."

Humphreys estimates that, as a result, "the difficulty of mounting a spoofing attack has dropped by maybe a factor of a hundred since 2012," when he first raised the alarm.

While jamming as practiced "in the wild" is often a nuisance crime — causing GPS to black out briefly or cell towers to drop calls when one is nearby — spoofing is potentially much more dangerous in the wrong hands.

As Soar, the NovAtel executive, puts it: "The snotty kid in the bedroom is now probably our worst nightmare."

Hoping for a small 'crisis'

Law enforcement is starting to fight back. Jamming detection devices manufactured by Chronos Technology, for example, have been available for about a year and are "starting to find their way into standard use," Curry said.

A device used by authorities to detect truckers using jammers. Chronos Technology Ltd.

The U.S. government also is slowly working to address broader GPS vulnerabilities.

The multi-agency Space-Based Positioning, Navigation and Timing Executive Committee, known as ExCom, has been working for years on a GPS backup solution that would make jamming and spoofing of GPS much harder.

It is now developing requirements for a backup timing system — the GPS function most important to critical infrastructure — to be followed by navigation and positioning requirements. The commission is expected to issue recommendations in the fall of 2017, said Nancy Wilochka, a spokeswoman for the U.S. Transportation Department.

Manufacturers of GPS navigation devices also are beginning to incorporate anti-jamming and anti-spoofing measures — such as inertial sensors and antennas that draw from multiple Global Navigational Satellite Systems (GNSS) or can determine the direction from which signals are arriving — into their designs to at least improve the chances that they can withstand a malicious attack or GPS outage.

"It's an arms race of giving enough protection," Soar said.

That is encouraging to experts like Humphreys, but he can't help wondering whether the improvements will arrive soon enough — and be strong enough — to prevent a disaster.

"My hope is the first crisis, if it comes, is just large enough to really wake us into action but small enough that nobody gets killed or that there isn't a great deal of economic damage done," he said.