Redacted DHS Report Details Privacy Jammer Risks

DEE ANN DIVIS

Small GPS jammers, particularly the "personal privacy devices" readily available on the Internet, pose one of the greatest risks to the nation's critical infrastructure, according to a now public Homeland Security assessment.

The devices, also called PPDs, rank among the three most likely causes of GPS disruption, according to researchers from the Department of Homeland Security's Homeland (DHS) Infrastructure Threat and Risk Analysis Center (HITRAC). Of those three, however, only the scenario incorporating multiple PPDs was identified as being both among most likely to happen and the most potentially damaging to the operation of industrial infrastructure.

If you've not heard this perspective previously, it may be because it is scattered across the 200+ pages of a limited-circulation report called *National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions.* The report was prepared in 2011 at the request of the National Executive Committee for Space-Based Positioning, Navigation, and Timing (PNT ExCom) and released the following year on an "official use only" basis — that is, strictly within the federal government.

Although a very brief, process-focused fact sheet about the study was made public in 2013, it was not until last year that a redacted version of the full report was obtained and released by Government Attic, a Freedom of Information Act organization. Despite its aging, the report's content remains remarkably relevant and timely.

Expert Insights

To conduct the study, HITRAC convened panels of GPS and infrastructure experts to rank the likelihood and potential impact of eight types of GPS disruption in the United States. (See accompanying sidebar, "National Risk Estimate — Disruption Scenarios"). The study also weighed the likelihood and impact of a wide range of other events, such as solar flares, hacker attacks, the sudden loss of GPS satellites to old age, and even the intentional, malicious manipulation of other international PNT systems. These events, while potentially devastating, were considered unlikely, however, and not covered deeply — at least not in the released portion of the report.

Brandon Wales, then-director of DHS HITRAC summarized some of the findings in November 2011. He told the National Space-Based PNT Advisory Board that spoofing was judged to be of higher consequence than jamming because of the length of time it might take to discover signal tampering. Even so, he said in his charts, jamming was far less technically challenging and therefore seen as more likely to occur.

Of the eight scenarios HITRAC looked at, two potentially involved PPDs. Scenario B looked at the impact of a single low-power jammer while Scenario D comprised multiple low-power jammers on the ground. These jammers were described as both stationary and mobile, with some only intermittently active. Between them they caused sporadic tracking and acquisition disruptions across a metropolitan area.

The experts agreed that the likelihood of interference from multiple PPDs was high "based on the increase in commercially available jammers, the ease of acquiring them (such as through the Internet), and their falling cost," wrote the researchers. Documented examples of such interference supported the conclusion, in particular an incident at Newark Liberty International Airport (EWR) four years ago where hard-to-find PPDs interfered with operations.

"During a 127-day period in 2011, there were 127 events of (radio-frequency interference) at EWR attributable to PPDs," the report said. Another study

Dee Ann Divis has covered GNSS and the aerospace industry since the early 1990s, writing for *Jane's International Defense Review*, the *Los Angeles Times*, *AeroSpace Daily* and other publications. She was the science and technology editor at United Press International for five years, leaving for a year to attend the Massachusetts Institute of Technology as a Knight Science Journalism Fellow. She has won numerous journalism awards for her *Inside GNSS* articles.

National Risk Estimate — Disruption Scenarios

Scenario A: A stationary interference source is causing continuous unintentional disruption. Ground receivers within a 30-kilometer ground-to-ground (GTG) radius are affected, and airborne receivers within radio line-of-sight (radio LOS) are affected.

Scenario B: Continuous jamming disruption from a single low-power, stationary jammer. GPS receiver tracking is affected within a 500-meter GTG radius and a 20-kilometer radio LOS radius. GPS receiver acquisition is affected within an 800-meter GTG radius and a 30-kilometer radio LOS radius.

Scenario C: Continuous jamming disruption from a single high-power, stationary jammer (e.g., mounted on a tall building or hilltop). GPS receiver tracking is affected within a three-kilometer GTG radius and a 230-kilometer radio LOS radius. GPS receiver acquisition is affected within a four-kilometer GTG radius and a 350-kilometer radio LOS radius.

Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some continuous and others intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.

Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm (G4 or higher). Tracking threshold of GPS is reduced significantly.

Scenario F: Continuous pinpoint spoofing attack against a single target receiver. The spoofer walks off the time and position reported by the target receiver without raising alarms.

Scenario G: Sophisticated, coordinated, continuous pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position reported by its target receiver without raising alarms.

Scenario H: Continuous attack whereby a strategically placed high-power transmitter generates GPS-like spoofing signals after an initial interval (several minutes) of jamming. Receivers within a three-kilometer GTG radius and a 230-kilometer radio LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.

found as many as five events per day, possibly from PPDs. Aviation receivers, said the researchers, suffered "unintended, collateral damage."

Anecdotal evidence from pilot forums, the authors added, indicated "that low-level flight above certain stretches of roadways (such as along I-95 and I-35 near certain convenience stops) typically results in loss of GPS satellite tracking in small aircraft. PPDs are a suspected cause of the disruptions."

"The aviation experience seems to indicate a higher prevalence of PPDs in the United States," said the researchers, "as well as a larger jamming radius for common cigarette lighter styles than previously assumed."

Moreover, some of the panelists said they fully expected the problem to get worse.

"The (subject matter expert) from the (Federal Aviation Administration) noted that in the near term, possibly within the next 12 to 24 months, this sort of scenario could become the most frequently occurring because of the increasing numbers of mobile jammers and our current lack of mitigation options," wrote the authors in 2011 .

Not only have the laws regarding PPDs not changed since the panels met — they are still legal to buy and own, although not to use — but new developments may drive demand for the devices even higher.

The use of PPDs, also called pocket jammers, has largely been associated with workers trying to avoid minute-by-minute oversight of their company vehicles. Whether its a delivery person stressed by demands for more productivity, a lunch-time Romeo (or Juliet) hiding a tryst, or a trucker hoping to avoid restrictions, many of the examples of the use of privacy jammers are, anecdotally, linked to commercial activity. Criminals are also suspected of using the jammers to thwart the tracking of stolen vehicles and generally undermine GPS-based surveillance.

But market forces arising since the report was finalized may be conspiring to drive up demand in the general population. For example, mandatory road-usage fees, determined with the help of GPS, are being suggested as a way to address declines in gas tax revenues caused by a shift to higher-mileage cars and electric vehicles. Experience with efforts to spoof electronic toll collection systems in some European nations suggests that these are credible concerns.

Insurance companies are also increasingly incorporating options for car monitoring, which can include location tracking, into their rate setting models. Although such tracking is currently voluntary and advertised as a way to lower rates, it could be used to raise the rates of those whose driving patterns are seen as more risky — perhaps someone on the overnight shift who does most of their driving at night. Eventually the consensual aspect of such monitoring may be replaced by mandatory requirements if refusal to be tracked comes to be seen as a warning sign of a risky driver, an expert told the Washington Post.

"When such programs become more common, opting out could serve as a "red flag" to insurance companies, according to Renee Stephens, vice president of U.S. auto quality for J.D. Power and Associates.

The prospect of new fees and higher insurance premiums may drive more people to seek out and PPDs. The panelists anticipated such an increase in privacy concerns and even postulated a possible public backlash against GPS. They suggested a study of the factors motivating people to disrupt GPS and how prevalent it might become.

Dire Consequences

Having looked at the likelihood of different kinds of GPS disruptions, the study authors then assessed the impact of such interference. The greater the chance of a type of disruption occurring, and the higher its potential impact, the higher its overall risk.

To better understand what could happen if GPS signals were degraded or there were signal outages, DHS looked closely at how GPS is integrated into 4 of the 16 infrastructure sectors deemed critical to the nation by the agency. These four sectors — communications, emergency services, transportation (all types) and energy — were picked because GPS PNT is used to support or fulfill their core missions.

While the operations of all four sectors could be seriously undermined by at least two of the eight scenarios, Scenario D — the one incorporating two or more personal privacy devices — was the only one of the eight that made the high-impact list for every single sector.

Transportation. The transportation sector was divided into air and surface/marine modes for analysis. For aviation, the impact of PPDs would most likely be seen as isolated instances of GPS signal degradation, with problems continuing for more than a month, most of the experts agreed. This, however, would be more of a nuisance and a capacity issue because the nation's air traffic control system has layers of redundancy.

If pilots and air traffic controllers come to see GPS as unreliable, however, it could seriously undermine efficiently and capacity over time, the experts said. And if the problem is not dealt with by the time the new NextGen air traffic control system is implemented, the overall problem would become serious. The nation cannot absorb the nation's projected growth in air traffic without NextGen, and NextGen depends on GPS.

The panelists could not agree on the extent of the impact of GPS interference and spoofing on maritime and surface transportation. Some suggested it would be isolated degradation while others believed there could be widespread adverse effects and even outages. Maritime services would become less efficient as they shift to conventional methods of navigation, but overall marine and land transportation would be fairly resilient.

Problems could arise, however, where modes of transportation meet. For example, the unloading of shipping containers at a port for the next leg of delivery was recently halted for hours when a driver with a pocket jammer drove into the cargo trans-shipment area and the cranes lost their GPS lock.

Energy. The energy sector "depends on GPS for providing electrical power system reliability and grid efficiency, synchronizing services among power networks, and finding malfunctions within transmission networks," according to the researchers. GPS is a key component of wide area power distribution monitoring systems, phase monitoring units, and disturbance monitoring equipment.

Operators use phasor measurement units (PMUs) that rely on the precise, ubiquitous timing information in the GPS signal for extremely accurate time stamping, which is correlated with sampled voltage and current inputs. "Collecting and collating these measurements," explained the authors, "provides powerful techniques for monitoring and modeling power networks."

As with transportation the panelists were divided on how long PPD-triggered problems would last and whether or not they would be more isolated. The electrical grid also would likely take a hit to its overall efficiency as synchronization can be lost if a jamming incident lasts longer than 15 seconds. Energy exploration, which increasingly uses GPS to synchronize seismic monitors, could also be effected.

Communications. Communications infrastructure, of which there are many

types including wireless, cable, satellite and broadcasting, use timing signals derived from GPS-disciplined oscillators (GPSDOs) — that is, clocks that maintain their accuracy through continuous reference to a GPS time source.

But communications firms have long factored in national disasters and accidental disruptions and, as a result, are generally prepared for problems. If a timing system loses lock on the GPS signal, it goes into holdover mode, relying on its internal clock to slow degradation of timing accuracy. The duration and level of performance of the system depends on the quality of the non-GPS timing source.

The dependence of other sectors on efficient and reliable communications, however, makes this sector particularly important, and disruptions of communications infrastructure could have far wider consequences than is the case for other sectors, according to the DHS report.

Emergency Services. Emergency Services appears to be the sector most vulnerable to even short-term GPS disruptions. First responders use GPS to navigate to incidents and, as with the overall communications sector, they stay in touch with each other over networks that often rely on GPS-disciplined oscillators.

"If a first responder's radio network architecture pivots around GPS Timing, there is no readily available backup if the GPS component is compromised," says the DHS report. "While dispatchers may still be able to communicate with individual first responder units, there could be debilitating effects on radio signals or untimely delays in communications voice radio systems using simulcast technology."

Falling back on older technology could create chaos, the researchers said, if, for example, an entire department had to rely on one communications channel.

Without GPS E911 services also would be compromised and computer-aided dispatch systems would be hampered, making it harder to locate accidents and stolen vehicle and dispatching fire, medical, and police. "While this Sector has not reached the point of total dependency on GPS services," wrote the researchers, "the use of GPS improves the ability of the sector to perform damage mitigation and assist in timely rescue response."

Not So Rosy Future

The particular vulnerability of the emergency services sector is probably captured best when the study looks ahead 20 years to how trends will strengthen or undermine its operations. When DHS researchers described the best case for future first responders during a GPS disruption, they deemed it a "learning experience" nicknamed "As Good As It Gets."

Unfortunately for emergency personnel in 2016, that best case is still a good

ways off. It assumes the United States has put a backup for GPS in place — a long-debated proposition that has yet to come to pass. Though the PNT ExCom put its stamp of approval on the ground-based eLoran system, which would be a completely independent alternative for timing, no federal money has been allocated as yet for its creation or support.

So what name did DHS give the no-backup future for emergency services? That depends on how completely first responders come to rely on satellite navigation. If they have not utterly lost their pre-GPS chops for locating and then navigating to those in need, the future was deemed a "Should Have Known Better" scenario. If dependence on GPS grows and no alternatives emerge, said DHS, a disruption will be the preparedness equivalent of bringing a "Knife to a Gun Fight."

As for the other sectors, researchers said signal diversity would greatly improve the future prospects of the energy sector, which could otherwise be facing intermittent outages and energy shortages. To support this approach, the report says, DHS could encourage GPS receiver manufacturers "to make multi- system/multi-frequency receivers."

Fortunately receiver manufacturers, if they haven't already developed multi-GNSS chip sets, are chomping at the bit to do just that. Unfortunately the availability of reliable, usable signals from other constellations is unclear. The only non-GPS constellation completed so far has been the Russian GLONASS system, which has suffered some technical problems. The other global constellations — Europe's Galileo and China's BeiDou — will come fully online soon enough, but questions remain about the permissibility of using their signals in the United States for official purposes such as supporting E911.

The Europeans applied to the Federal Communications Commission for approval more than a year ago but are still waiting for an answer. Bureaucratic foot dragging on the part of the United States has now raised doubts about American access to PRS, Galileo's encrypted, jam-resistant signal — a service that could prove useful for countering problems like PPDs.

The trend appears similar for both the transportation and communications sectors. Without government action the sectors will be drawn to GPS because it is reliable and free, becoming increasingly vulnerable as their dependence on satellite navigation grows.

The needed government action, underscored by the panelists and the HITRAC team, is deployment of a backup for GPS. It is the key difference, according to the report, between a smooth-running future and a dystopian outcome for all four sectors.

This is a rather surprising assessment to find in a years-old DHS report given that DHS has yet to fulfill its 11-year-old mandate to help develop a GPS backup. In fact the Coast Guard, which is part of DHS, continued dismantling the infrastructure essential to eLoran until 2014, when it was finally ordered to stop by Congress.

"Unfortunately," wrote the researchers in what may prove to be their most prescient forecast, "it may take a major GPS disruption to prompt investment in these types of initiatives." IG