INCORPORATING BORDER SECURITY REPORT

WORLD SECURITY REPORT

Official Magazine of
International Association of CIP Professionals

MAY/JUNE 2017
www.worldsecurity-index.com

COVER STORY

GPS DISRUPTION AND CRITICAL NATIONAL INFRASTRUCTURE

GPS disruption and Critical National Infrastructure

Evidence of growing GPS jamming threats near Airports shows the need for increased vigilance

In 2013 pilots reported 11 incidents of GPS interference or malfunction through NASA's Aviation Safety Reporting System (ASRS); in 2014 the number jumped to 24; in 2015, it was 28, and 28 incidents were also reported in 2016.

That amounts to 91 occurrences of GPS disruption in aviation in four years – each sufficiently serious to justify professional pilots reporting them to a voluntary, anonymous database. In the majority of these incidents a GPS-based navigation system either experienced a total loss of signal or – more seriously – misreported the aircraft's position. What's more, these reports only represent the incidents that flight crew have reported to the ASRS database, so the actual number is undoubtedly higher.

Unknown causes

In many of these cases there is no immediate explanation provided for the malfunction. Many reports simply say the signal was lost for a time and then returned – with flight crew either falling back on other navigation techniques or asking air traffic control for guidance. For example, a Cessna pilot reporting an unexplained incident in 2014 wrote:

"While established on the localizer for the approach to Runway 22L in Boston, the GPS signal was lost numerous times (more than 3) from 20 miles out from the runway to 5 miles out. Each time the GPS failure message remained for approximately 10-15 seconds before signal returned. The weather was VFR and navigation was not affected."

Military exercises

The remaining reports provide better insight into the source of the disruption, with around 20 of them specifically citing nearby GPS jamming exercises by the US military.

These tests are vital to the effective operation of the US military, and are usually either testing how military equipment copes with signal jamming, or are used to train military personnel to work in hostile environments where an enemy might be jamming navigation signals. They are conducted in open-air ranges over a wide geographical area, so can have a

significant impact on private and commercial aviation in nearby airspace.

Even though advance notification of the exercise is normally given, it can still cause problems, as in the following example:

Early in 2016 a private jet pilot received an advisory Notice to Airmen (NOTAM), requesting him/her to avoid a wide swathe of air space in the southwestern United States during a military jamming exercise, and it triggered this response:

"… The coverage area of this test effectively grounds all GPS-equipped aircraft in the Southwest flying IFR since they may experience unknown signal loss… At the time that ground based Navaids are being decommissioned and our government is promoting GPS based systems as primary navigation sources, the repeated interruption of GPS signals by our military [is] threatening the safety of our aviation system."

Judging from the reports in the database, military testing does cause widespread problems, and not only for aviation. In 2015, agricultural businesses in Idaho were knocked out of operation for several hours by a military exercise they had not been made aware of.

Disruption near airports

Another growing source of interference to commercial and private aviation comes from ignorant, or even malicious, use of widely available pocket-sized jamming devices. These are widely used by car thieves, road toll evaders, tracker evaders, lorry drivers bypassing commercial mileage limits as well as those wanting a short respite from the fleet operator's vigilance – as suggested by the following advertisement from the web:

"If you are sales personnel and delivery drivers, this GPS tracking jammer is a very popular item for you to take lunch or make a personal stop outside of your territory or route off the radar!"

As major airports and ports (and other critical infrastructures such as finance, grid and telecoms) are often situated near to major road networks, they can be vulnerable to interference caused by these devices

This sort of jamming is typically indiscriminate and can be both moving and stationary. It may be fairly low power – something like a 500m bubble that blocks any GPS receiver or transmitter that might be used to identify location – but still be as effective as hiding in an underground car park. In any case, a car thief is unlikely to be concerned with managing power levels to minimise risk to other GPS users.

The Aviation Safety Reporting System (ASRS) includes several reports of signal disruptions experienced by pilots landing at several airports that suggest an intermittent presence of a nearby jammer.

For instance, one flight crew operating into Manila International Airport in the Philippines, reported

"…..Complete GPS loss of signal as we crossed the coast in point to RPLL. Signal was lost for remainder of flight. Also on takeoff from RPLL we had a complete loss of GPS signal until coast out. No notice on NOTAMs viewed. No notices on RPLL ATIS."

In other words, this crew reported a total loss of the GPS signal on both their arrival and departure from this airport.

Another flight crew operating into Mexico City reported GPS jamming on approach into the international airport:

"Finally, we received an approach clearance and set the lower altitude in the window. At this time we were now addressing the route discontinuity and as we were verifying that everything looked OK, we descended below the published altitude, but not before we received notice that our GPS was being jammed, first one side, and then the other."

In another report, the user almost landed at the incorrect airport due to an issue with his GPS device:

"The android tablet had frozen and was showing the aircraft approx. 10 nm to NW of JVY. The PIC visually identified what he mistakenly thought was JVY and proceeded to fly Southbound towards the field. The PIC flew to LOU and the

table remained intermittent. The PIC entered a pattern at LOU at approx 1500 MSL and noted the runway configuration did not appear consistent with the airport of intended landing"

In the following report intermittent interference was traced to a jammer in a truck in a car park near North East Philadelphia Airport:

"… they were losing GPS satellite coverage on the RNAV (GPS) RWY 33 approach within the last mile of the approach. This would happen intermittently with different aircraft, and different avionics… A Federal Communications Commission Enforcement Bureau agent located a GPS jamming unit in a truck located within one mile from the approach end of Runway 33. The truck was in a parking lot, henceforth the intermittent interference; when the truck left the area, the GPS approach was normal… The driver had no idea he was using a device that was illegal. He was using the jammer to disable a tracking device that was placed in his vehicle by a vendor, to hide his location."

Disruption near other Critical National Infrastructures

At a United Nations Committee for the Peaceful use of Outer Space) (COPUOUS) sub-committee meeting in February 2017 it was revealed that there had been a complaint from a cell provider in Florida that its cell phone tower sites had been experiencing interference: Forfeiture Order affirms proposed $48,000 forfeiture against a man for using a cell phone signal jammer in his car while commuting to and from work on a Florida highway over a 16-24 month period.

Also an Australian Transport Safety Board (ATSB) bulletin released in March 2016 revealed that the crash of a drone in 2015 that occurred whilst it was filming a major event at the Melbourne Cricket Ground was most likely caused by Radio Frequency interference. Luckily the drone crash landed on a road outside the stadium and there were no injuries.

Understanding and addressing the risks

The good news is that in all of these reports everyone involved was able to work around these failures and avoid serious damage. But, as our Critical National Infrastructures become reliant on GPS for obtaining precise positioning and/or timing data, the scope for disruption can be seen to be growing. Aviation is a particularly good source of reports referring to GNSS interference, not because it is affected more by, or is more vulnerable to, GNSS interference but due to the voluntary, non-attributable reporting system that is available for flight crews.

This all means it is essential for manufacturers, commercial airlines, private operators, airport authorities, and other ground-based GPS-reliant businesses to gain a better understanding of the risks – whether financial or safety-related – and how to implement appropriate mitigation strategies.

There are three obvious ways to improve that understanding. The first is to model test cases for GPS devices and flight management systems. The tests need to replicate the sort of real world conditions described in the ASRS reports. That would be a daunting task were it not for the availability of sophisticated test solutions designed specifically to make it easy to simulate every sort of operating environment and condition under controllable laboratory conditions.

The second approach is to continuously monitor the RF signal environment around critical infrastructures such as airports or ports to understand where and when interference is occurring. There are very accurate interference detectors available (such as the Spirent GSS200D) that will automatically monitor and record results around the clock and – potentially – inform not only on what interference to expect but also provide data to help identify the source of the problem.

Thirdly, there is a need to share our experience and keep each other up to date with current threats, risks and effective workarounds. A good start would be to sign up for the GNSS Vulnerabilities LinkedIn Group.

Guy Buesnel
PNT Security Technologist- Robust Position, Navigation and Timing
Spirent Communications