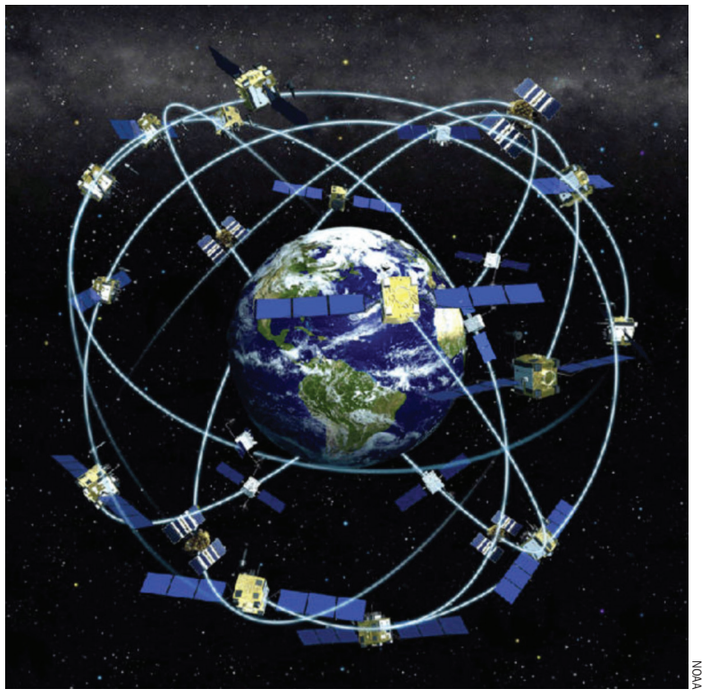
GPS Vulnerabilities

It's become **a utility,** so can GPS afford to be **susceptible to malicious** interference?"

BY **DAVID ESLER** david.esler@comcast.net


NOAA

The current Global Positioning System constellation consists of 24 Block II satellites, 21 active and three spares, rotating the planet at 12,550 sm in medium-earth orbit. New upgraded, more powerful Block III satellites now being launched will form a replacement constellation of 31 units claimed to be more resistant to jamming.

Back in the 1980s, as the U.S. Air Force was testing the first NavStar satellites in research trials that led to today's Global Positioning System (GPS), Charlie Trimble, founder of a small navigation equipment company in Silicon Valley, wrote a pamphlet in which he predicted that GPS would eventually become a "utility," or essential public service.

I recognized that the proposed system with its "constellation" of satellites circling in mid-earth orbit might become a useful navaid for aircraft, missiles and marine vessels but probably not for much else. Furthermore, who among the general public would need a precision navigation device or be able to afford to buy one?

Well, of course, Trimble was prescient — and right — and his little eponymous venture that started by manufacturing Loran-C navigation sets became a pioneer in developing GPS equipment, and today Trimble Inc. employs more than 8,000 people. Meanwhile, GPS has become the basis for a multitude of activities and conveniences, everything from surveying, agriculture, construction, vehicle tracking and autonomous drone operation to digitized map reading and guidance in our cars — and smartphones. It is even making the much-vaunted autonomous (driverless) car possible. In other words, GPS has become that utility Trimble predicted three decades ago and now we're carrying affordable, handheld computers equipped with GPS engines and using GPS guidance and time data routinely.

For aviation, space-based position and navigation enabled 3-D position determination for all phases of flight — even for maneuvering on the ground. GPS provided a repeatable level of accuracy hitherto unavailable. It opened up a raft of new precision approaches independent of ground-based navaids, meaning that airports without conventional (and expensive) guidance infrastructure could now have these procedures. The same was true for en route navigation, especially in remote areas devoid of radio aids including oceanic airspace, since guidance signals were emanating from space and available almost everywhere on the globe (or at least between 80 deg. north and 80 deg. south latitudes).

The Global Navigation Satellite System (GNSS) also made Automatic Dependent Surveillance (ADS) possible, since positioning was so accurate that aircraft could now broadcast their own locations in areas where there was little or no radar coverage. Air traffic controllers could then track them with a "virtual radar" presented on a computer-generated display, based on the GPS-verified ADS transmission. It's not surprising, then, that FAA planners and contractors designed the NextGen ATC system around GPS and its progeny, ADS.

When the full GPS constellation of 21 active satellites and three spares became fully active in 1995, the system's consistent accuracy and reliability even prompted planners in the FAA and Department of Defense (DOD) to consider ultimately decommissioning the huge and expensive network of radio navigation aids — the VORs with their DME adjuncts, NDBs and various instrument approaches — since it was assumed their functions could be provided by GPS with greater accuracy (easily supporting Required Navigation Performance [RNP]) and for less money.

For a while, the FAA and the Pentagon considered retaining the low-frequency Loran-C navigation network as a compatible backup to GPS, both being ground-referenced (i.e., calculating position in latitude and longitude), but it was eventually decided that the U.S and Canadian Loran transmitter chains would be turned off in 2010. Other chains in Europe and Russia followed in 2015. There has been talk among governments of resurrecting a new digitally based Loran system ("enhanced," or eLoran, studied by the U.K. until 2015 when work was halted on the project), but so far no agreements have been finalized.

Thus, at the present, there would be no backup for GPS except inertial reference navigation (with its cumulative error limitation) and existing radio navaids, if for some reason, the system were to go down. For aviation alone, becoming more dependent on GPS every day, such an event would be merely disruptive to devastating.

According to a 2011 FAA assessment, the potential economic impact to aviation from a nationwide GPS interference event would be an estimated $70 billion. "Aviation relies on GPS significantly, and we not only need it but [must] make sure it is protected," Andrew Roy, director of engineering services at Aviation Spectrum Resources, told *BCA*.

But It's Vulnerable . . .

But the truth about GPS is that it is vulnerable to interference, both accidental and malicious.

"Aviation has been aware of GPS vulnerabilities since Day One," confirmed Guy Buesnel at U.K.-based Spirant (pronounced "SPY-rent"), which makes, among other things, GPS simulators for testing of receivers. "The low signal strength, as low as a 40-watt light bulb, transmitted from space, is vulnerable to spoofing and jamming." (The signal comes in below thermal noise, and that had to be accommodated when the system was designed.)

The designed GPS receiver sensitivity level is below 10-14 watts, given the 13,000 sm (20,000 km) distance the signal needs to travel from the satellite to the ground. "So, from a jamming perspective," Roy added, "it isn't that hard to get a higher-power signal onto the L1 operating frequency, which is 1575.42 MHz. If you can get some power into that band, whether deliberate or accidental, it doesn't take that much power to stop the receiver from being able to 'see' the GPS signal. So, it's easy for the signal to be lost — DOD intentional jamming has proven that." [More on those DOD exercises further on.]

Massive areas can be affected in the worst-case scenarios. Not only that, but even local interference over a city block or larger area can be accomplished with a handheld jammer.

For an interesting walk on the wild side, Google "GPS jammers" and see what comes up — and mind you, this is not on the so-called "darknet" but the public platform anyone can access. Easily available, the jammers you will see advertised are "sold as 'personal privacy systems,' and their use is quite widespread," Buesnel observed. The devices — made in China, of course, and in many cases, sold on line from there — can be purchased for less than $125. The smallest can be plugged into the cigarette lighter or USB port of a vehicle. High-powered handheld jammers, some of which are claimed to corrupt all GPS bands, L1 through L5, while covering both tracking and navigation plus cellphone signals, are battery powered and retail for between $200 and $500.

In addition to malefactors blocking GPS signals for malicious purposes or just to create mischief, personal jammers have become especially popular with long-haul truckers or package delivery drivers tracked via GPS by their employers to ensure they're adhering to their schedules. The jammers disable tracking devices installed by the shipping companies on their trucks that calculate GPS location.

The larger problem is that the jammers can disrupt any GPS signal within their range — up to miles away, depending on the unit. Moreover, "It is quite hard to identify the source of jamming," Roy pointed out, "especially if it's coming from a moving vehicle like a truck." Truckers are also using jammers to avoid paying tolls, since the automated toll-takers on highways and bridges operate on GPS tracking, and the big rigs can simply blast through the toll lanes with impunity.

Jammers work by broadcasting noise on the same frequencies generated by the satellites, blocking receivers from picking them up. Think of the jamming signal as a bubble around the jammer that GPS signals can't penetrate. And these jamming bubbles have inadvertently caused a lot of trouble where highways pass in the vicinity of airports or when vehicles containing jammers drive or park near airports or under approach and departure paths.

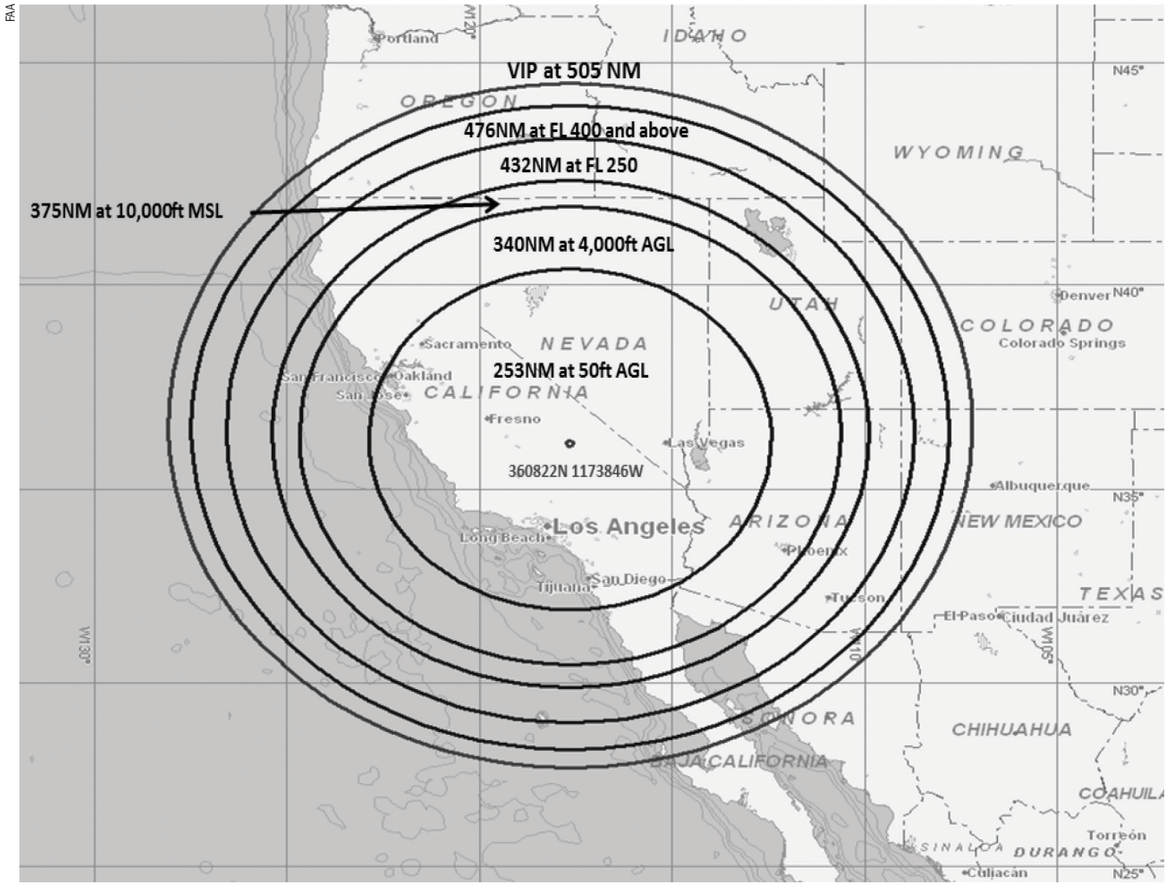
This scenario occurred at Northeast Philadelphia Airport (KPNE), where in 2015 pilots were reporting loss of GPS on approaches, and at Newark Liberty International Airport (KEWR) in 2012, where a jamming device in a parked pickup truck disrupted the airport's GPS Ground Based Augmentation System (GBAS). The driver of the pickup, who claimed he was using the jammer to keep his employer from tracking him, was himself tracked down by Federal Communications Commission investigators and ultimately fined $32,000 for interfering with a critical aviation guidance system. And at business aviation's Teterboro Airport (KTEB), there have been reports of GPS jamming believed to be emanating from truckers plying U.S. Route 46, which passes just north of the airport and Runways 19 and 24.

Buesnel related that, "Last year, I took a London black cab and saw a GPS jammer in the cigarette lighter. I asked the driver why he was using the device, and he said it was to interfere with Uber, 'because the Uber drivers rely on GPS to meet their customers' at airports and other venues, and this was taking business away from him." Of course, the jammers also mess with the GPS signals that aircraft rely on at the airports.

In August 2017, at Nantes Atlantique Airport (LFRS) in France, a traveler left his vehicle in the car park with a GPS jammer activated in the cigarette lighter port. Meanwhile, he departed on an airline flight for a vacation. The jammer "disrupted the tracking systems of planes arriving and taking off from the airport, leading to delays on several flights before it was located and disabled." The perpetrator was eventually fined €2,000 by French authorities, but there is no report as to the condition of his car when he got it back from the impound lot.

Jammed Up by Jamming

It is illegal in the U.S. to use, sell or manufacture GPS jammers, and according to Kashmir Hill, writing for Gizmodo Media in 2017, every time you turn one on, you're liable for a $16,000 fine from the FCC (see https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-easy-1796778955). Additionally, infractions can be punished by jail time. ASRI's Roy added that "Jamming GPS signals is a fundamental assault on the public spectrum. . . . There is lots of publicity to try and stop it and a crackdown from the FCC on sellers of the equipment."



For six days in 2016, the Department of Defense conducted this GPS "denial-of-service" jamming exercise centered on China Lake, California, and extending outward with a radius of 500 nm and upward from 50 ft. at origin to more than 40,000 ft. at periphery. Note that the outer circle encompassed Class A airspace at San Francisco, Los Angeles, and Las Vegas. Such exercises, which are becoming more common, are announced via notam.

In 2016, the FCC fined a Chinese supplier $34 million for selling 10 GPS jammers to undercover FCC agents. Further, the FCC extended its GPS jamming prohibition to state and local governments and law enforcement agencies when it learned that some undercover cops were using jammers to avoid being tracked in their cars. Some websites marketing jammers have been blocked or taken down, as well, but thousands of the devices remain in the field and in daily use and are often traded on websites like eBay.

Hill relates how small drone users — many of them teenagers — have circumvented manufacturers' "no drone zone" software, which is dependent on GPS signals to know a drone's location in order keep it away from sensitive areas like airports, government installations, even the White House. They do this by employing jammers to confuse the GPS signals, essentially telling the drones they are outside the prohibited areas.

Even practitioners of the highly popular video game Pokemon Go are spoofing GPS signals with jammers. Players download an app to their phones that superimposes creatures, or monsters, over real-world locations named "arenas" and go to them to either "collect" the virtual creatures or defend the arenas from other players. Buesnel said a second app allows gamers to "collect the monsters from a single location and spoof their GPS system so it looks to other players like they're wandering around the map. You can buy these apps that will give a false location of your phone."

Pokemon Go designers have changed the game to neutralize this, but the hackers still have their apps and can simulate a GPS constellation for less than $300. Hill claims that some players are buying multiple jammers and stationing them at the arenas to block competitors from registering their locations in the virtual space, thus preserving their dominance of it. Some of these locations have been near — and even on — airports, thus affecting GPS and aircraft operations.

Unintentional jamming of GPS signals also occurs, as at Hannover International Airport (EDDV) in Germany in 2010 when a GPS repeater was set up in a hangar less than 3,000 ft. from the threshold of an active runway to test GPS receivers on business jets. Airline crews began to experience Ground Proximity Warning System (GPWS) alarms and displaced runway threshold alerts while taxiing for takeoff. In one case, the repeater acted like a GPS spoofer. Subsequent investigations determined that the repeater power level was unnecessarily high for the testing being accomplished and that the hangar door was occasionally left open during testing, increasing the jamming effect.

Since 2013 and to November 2018, more than 250 incidents of GPS disruption have been reported to the Aviation Safety Reporting System (ASRS) by pilots. In Europe and adjoining areas, 815 incidents were reported to Eurocontrol, again, through November 2018. A sampling of incidents from the last three years reveals the ubiquity of suspected jamming incidents experienced by aircraft in flight:

▶ Manila Ninoy Aquino International Airport (RPLL), Philippines, 2016. There were more than 50 reports of GPS interference on approach to Runway 24 during the second quarter. Lapses included total loss of onboard GNSS with GPS-L and -R "invalid" messages appearing on displays; decrease in navigation performance leading to RNP alerts due to increasing lateral error (i.e., actual nav performance deterioration below RNP) leading to missed approaches and GPWS alerts. In some aircraft, nav reverted to IRU or DME/DME, loss of autoland and ADS-B capabilities. According to an International Civil Aviation Organization Information Paper, there exists some suspicion that a cellphone tower on the approach course at 14 nm DME might be the cause of the GPS signal degradation, although this was not verified, and suspicion exists that the GPS signal degradation may have been caused by jamming attacks.

▶ Undisclosed U.S. location, 2017. Pilot reported temporarily losing the GPS signal, saying "GPS loss seemed an illusion." This was supported by ATC radioing that no other aircraft in the area had reported a GPS outage, causing the pilot to assume that he'd encountered a trucker with a GPS jammer on a highway beneath the aircraft. "So I continued into the rain, clouds and turbulence . . . then all hell broke loose: GPS signal failure, ADS-B failure, multiple cascading messages on the GTN."

▶ Fresno Yosemite International Airport (KFAT), California, 2017. Aircraft appeared to crew to turn toward assigned waypoint; however, ATC asked crew to confirm heading. "At that point it appeared the GPS had lost position, and we declared a lost signal to ATC and asked for vectors. We were not able to regain accuracy with the GPS and navigated on vectors and VOR tracking for the remainder of the trip."

▶ Undisclosed U.S. Location, 2017. "I experienced a failure of the WAAS [Wide Area Augmentation System] GPS antenna in flight. The antenna failed in such a manner as to create spurious emissions that caused all other GPS antennas on my aircraft to lose signal."

▶ Cherry Capital Airport (KTVC), Traverse City, Michigan, 2018. Pilot reported that while instructing in vicinity of LADIN intersection he experienced a "GPS anomaly," the receiver displaying scrambled characters that were indiscernible. The event lasted approximately 10 sec., then cleared up.

The Government Jams, Too

Just to make flight crews' lives more interesting and increase cockpit workload and stress, the U.S. DOD, which manages the Global Positioning System through the U.S. Air Force out of Schriever AFB, Colorado, is mandated by presidential directive to train and test U.S. military forces in operationally realistic conditions that include "denial of GPS" through jamming. These events, staged at varying locations throughout the country, have been increasing in frequency in recent years and covering ever larger areas. The DOD conducts intentional GPS interference during these events in coordination with military exercises to ensure weapons systems can operate in a GPS-degraded environment and for research purposes and testing of the GNSS.

The DOD coordinates with the FAA when it schedules these exercises, and the latter publishes flight advisories announcing dates, times and areas covered by them — another reason to plow through the reams of NOTAMs and notes on your computerized flight plan before you fly. As an example of the growing scope of these events, consider the six-day one staged in June 2016 centered on China Lake, California, and extending outward in a 500-nm circle from 50 ft. AGL at the source up to more than 40,000 ft. at the periphery and encompassing the cities — and Class A airspace — of San Francisco, Los Angeles and Las Vegas.

The Radio Technical Commission for Aeronautics (RTCA) in a March 2018 report titled "Operational Impacts of Intentional GPS Interference" concluded that the effect of GPS jamming in the DOD exercises varies on aircraft flying through or near the test zones from total loss of GPS reception to "degraded integrity." Of course, it also causes lapses in ADS-B. In a 2012 event, two airliners flying near one another in an interference zone drifted off course when their GPS receivers lost signal and had to be sorted out by a vigilant air traffic controller, averting a possible midair collision.

On April 14, 2016, the FAA released a priority message indicating that an Embraer Phenom 300 had experienced a yaw damper failure following loss of GPS signal while cruising through a DOD interference zone. The GPS loss precipitated a cascade event causing subsequent failure of AHRS, autopilot, ventral rudder and yaw damper, instituting a Dutch roll and triggering a stall warning protection system fault — all at high airspeeds.

The FAA priority message stated that "Further analysis revealed that GPS constellation signal instability in the flight area leading to loss of both GPS information data and causing the event. . . . The AHRS continuously calculates and applies altitude and heading measurement updates to correct gyro-integrated altitude and heading during flight maneuvers and, in normal operation, the AHRS relies upon GPS, air data system, and magnetic field measurements supplied by the magnetometer to maintain primary AHRS operation mode."

The FAA subsequently urged pilots of Phenom 300s to avoid DOD GPS jamming areas and closely monitor flight control systems due to potential loss of GPS signals. Embraer responded with a statement that the government's GPS testing shouldn't affect the normal operation of the Phenom and that the aircraft flight manual specified how to fly the aircraft under the conditions described in the FAA's priority message.

How could a GPS signal failure possibly cause an aircraft's flight controls to become erratic? It has to do with how GPS attributes are harvested from the satellites' signals for purposes other than navigation. Roy at ASRI explains that "There are three core attributes to GPS: position, velocity and timing. Each attribute relies on receiving an appropriate quality of GPS signal, with even small variations in signal quality — from signal reflections, signal propagation, satellite movement or orientation, your hand blocking some of the signal, and so forth — affecting the accuracy of each attribute." (Just as a footnote, this explains the reason why you see a blue circle constantly varying in size when using GPS mapping on your smartphone, as the GPS receiver

constantly adjusts to the changing signal quality to give you the best accuracy it can.)

"The reason why jamming is an issue for aviation is because the GPS receiver receives the three parameters," Roy continued, "and therefore it is a key reference point for an airframe because it can be allowed to operate for both navigation and functionally for other aircraft systems, depending on how the OEM designs the aircraft. This can be troublesome if the timing signal is used for something critical for flight."

Jamming as a Weapon

We are engaged in a war right now in which the weapons are not guns, bombs, poisonous gas or biological agents but cybernetic attacks on infrastructure. Compared to conventional warfare, the cyber equivalent can be waged for magnitudes less in funding and by considerably fewer players than those serving the major powers. In addition to probing of telecommunications networks, malicious manipulation of social media and theft of intellectual property through the internet, other forms of infrastructure can be targeted, as well, including GPS and its aviation users.

At last year's Air Transport IT Summit in Budapest, Societe Internationale de Telecommunications Aeronautiques, better known as SITA, estimated that more than 60% of cyberattacks on aviation targeted "critical assets," the most common being IT systems, airport and airline websites, and air traffic control and navigation systems — the last constituting GPS and representing 12% of attacks. Given the role that GPS plays today in terms of en route and terminal guidance and as a key component of ADS-B, it is easy to accept that targeted attacks on the GNSS signals could be disruptive to aviation — and the general economy of any nation that relies on it.

It has been documented that GPS jamming and spoofing have occurred near the airspace of Western powers adversaries Russia, North Korea, Iran and other Middle Eastern countries. Here are three examples of GPS interruption that were suspected to have been caused by jamming from sources within these nation states or regions:

▶ Middle East near Israel, 2017. Departing Ben Gurion International Airport (LLBG), Tel Aviv, this airline crew saw "ADS-B Out R" on their aircraft's EICAS. Performing the checklist, the pilots received an "ADS-B Out L" message, followed 5 min. later at FL 300 with "Unable RNP," "Runway Sys," "Terr Pos" and "GPS" additional messages. RNP showed 2.75 nm right of course. The crew contacted Nicosia Center to verify position and used VOR for navigation. Operations returned to normal when passing into Greek airspace where all nav systems returned to normal. "Everyone involved seemed to believe we were being jammed by possible military aircraft."

▶ Norwegian and Finnish airspace, September 2017 and November 2018. In the 2017 period, Widderoe and SAS airline flights experienced GPS disruption. During the 2018 period, GPS signal again deteriorated but this time during NATO exercise "Trident Juncture." The pilots reported loss of GPS while flying into airports in northern regions of Finnmark and Lapland. Norwegian aviation authority Avinor issued a NOTAM of irregular navigation signals over eastern Finnmark between Oct. 30 and Nov. 7. "Altogether GPS signals were jammed five times in 17 months," Buesnel said. It was subsequently reported that Finland summoned the Russian ambassador to answer allegations that Moscow was behind jamming of GPS signals in Lapland during NATO exercises.

▶ Near North Korean airspace, 2018. A Boeing 777 crew received EICAS message "ADS-B L Out," confirmed a few minutes later by the ADS-B itself. "I wrote both of them up," the captain reported, "and we then started discussing if this was a GPS jamming event, since we were just north of North Korea. The FO and I referenced the B777 GPS jamming update, and our situation was the first example listed."

Could the anomaly have been jamming generated by the North Koreans? Kashmir Hill had this to say in her Gizmodo article: "North Korea periodically interferes with GPS using jammers mounted on trucks that it drives close to the South Korean border, causing navigational problems for airplanes, ships and drones in the area — not to mention any GPS guided missiles headed in its direction." Would it be too much to assume they'd do the same along or near their northern border, especially knowing that international airlines fly there?

Another threat to GPS, and thus to aviation, is "spoofing," which is defined by the RTCA as "the surreptitious replacement of a true satellite signal with a manipulated satellite signal that can cause a GPS receiver to output an erroneous position and time." Spoofing "is a newer source of interference with advancing technology," Roy said. Much of that advancement has been spurred by open-source software, where users constantly make improvements to the code — all for free.

"Unfortunately, you don't even know you are being spoofed," Roy continued, "as a malicious user could send signals to slowly trick your GPS into moving you off target. The receiver does not know that the malicious signal is false, so it's insidious, like someone shouting at you at a higher volume than the one you want to hear. It can change or delay signals. Especially vulnerable is the older GPS equipment; the newer equipment — 'multi-constellation receivers' — is more robust and can receive signals from other satellite networks like GLONASS and Galileo."

Nation states are engaged in spoofing, Buesnel claimed, "trying to fool you, broadcasting replica GPS signals to deceive the receivers and steer you off position or spoof the time/date function backward or forward. And smugglers have been trying to spoof border-surveillance drones. Commercial aviation is well aware of this, and it would be difficult to spoof a commercial-level aircraft equipped with backup systems and operated by well-trained pilots." Spoofing is not as big a threat as jamming, he believes, but since the advent of Pokemon Go, it has become more prevalent in the larger community.

No Silver Bullet . . . But There Are Strategies

Can it be stopped, and if not, can we protect aviation from jamming and spoofing? First some background on GPS and how it works. A GPS receiver needs to receive signals from a minimum of four GPS satellites to report a position (three for position, and a fourth for timing information). The more satellites the receiver can see — and this could be up to 14 when cruising at high altitudes — and the more spread out they are across the sky relative to the aircraft, the better the information the GPS receiver has to specify an accurate position. Modern receivers — and this is important when considering local jamming and especially spoofing — can also receive similar signals from other countries' nav satellite systems to provide even more accuracy, *e.g.,* Russia's GLONASS, Europe's Galileo and, maybe, China's BeiDou.

The system has to take into account relativity considerations from the satellites moving at 8,700 mph (14,000 km/hr.) in medium earth orbit (MEO) at 12,550 sm (20,200 km) altitude, each circling the earth twice a day, or end up hundreds of miles off the intended course or target. Thus, even the slightest variance can mean a significant error in a GPS device's performance.

"Fortunately," Roy said, "modern receivers can account for the multitude of effects that can cause errors, including use of additional geostationary satellites that provide correctional data [in other words, the GPS WAAS in the U.S.]. The best performing receivers are used by surveyors and agriculture to gain accuracy to within 1 cm horizontally and 2 cm vertically."

> "There is no silver bullet to solve this in one hit . . . But conducting risk assessment of equipment is **the most important part of a jamming protection strategy."**

Receivers have had significant development to ensure that aviation-certified units used for RNAV operate within known parameters that provide a consistent level of performance. Aircraft receivers can still experience interference, given the low power signal they are trying to see, but will also warn the pilot when they cannot achieve necessary performance. This is also reflected in the ADS-B system, which combines the aircraft position data with metrics for both GPS integrity and accuracy (known as NIC and NAC), so that en route traffic controllers know if position data is valid. "While INS can compensate for loss of GPS signals for short periods," Roy said, "aircraft will not be able to comply with many RNP requirements without GPS."

Buesnel insists that, "There is no silver bullet to solve this in one hit. Before you think about enforcement, first you have to monitor the signal near airports. We [Spirent] have a detector that detects and sounds an alert when it sees interference. It allows a 'picture' to be made of the areas where jamming is occurring so troubleshooting can take place within them and an intelligence picture built to determine the nature of the problem and when and where jamming is happening. NOTAMs to pilots can then be generated."

That "intelligence picture" will contain what type of jamming or wave form is happening, as these events leave a unique footprint, the timestamp of jamming events to know when they show up, even the type of jammer used, and whether the event is intentional or a leakage accident like the one at Hannover.

"With this information, you can test your equipment and take action," Buesnel said. "But you need the intelligence — the quantifiable data — first. With the data, you can then influence the standards board to make the equipment on aircraft more robust. Enforcement is great but it is difficult due to the resources needed. You have to do the risk assessments to gain the intelligence picture."

But conducting risk assessment of equipment is the most important part of a jamming protection strategy. "We don't do enough of it," Buesnel said. "GPS is a utility we all depend on. The U.S.'s NextGen and ADS are good examples. So risk assessment is essential. It has to be repeated every few years, as things change."

The third generation of GPS satellites — the so-called "Block IIIs" — are promised to offer some resistance to signal jamming. First, there will be more of them, as the full constellation was to constitute 32 satellites. Secondly, their signals will be more powerful than those of their Block II predecessors, and there will be more frequencies generated, including the new L5 band (1176.45 MHz) designed specifically for aviation use (although other disciplines will be able to access it). Furthermore, the U.S. Air Force claims the Block III satellites will be equipped with defenses against jamming but has not indicated what they are.

These improvements should make the system more robust, Buesnel believes, "but it will not be totally free from interference or spoofing, and we still will need to protect it." The first Block III satellite was launched from Cape Canaveral by Space X in December. As of last September, nine more satellites were in production by Lockheed-Martin, whose contract for the first 10 units is valued at $10 billion.

Backups Always Necessary

So the new system will be better, more defensive, but as advanced as it is, the practitioners of jamming and spoofing will continue to advance their malicious technology, and the Block IIIs will still be vulnerable to cyber-tampering. And while the industry has developed standards to support robustness in GPS receivers, high levels of integrity in the GNSS as a whole, and augmentation for it on the ground, there is an understanding that backups will continue to be necessary.

As Buesnel points out, pilots tend to be very conservative, and this is reflected by the fact that airline and business aviation aircraft continue to carry backup nav equipment, and the aviation-support infrastructure retains legacy facilities like radio navaids, including VOR/DME, ILS, etc. The additional GNSS constellations (GLONASS, Galileo and BeiDou) could also serve as backups for each other during cyberattacks on one of them. "All this is good for us," Buesnel insists. "The International Committee on GNSS out of the U.N. has been doing a lot of work on interoperability and has developed the common standard, or L1."

"We can never underestimate the randomness of GPS interference," Roy warned. "Even a bad comm radio can cause an outage in rare cases, emitting radiation on the GPS band. Always report an outage to ensure we can monitor and maintain the integrity of GPS everywhere."

But whatever the threat, aviation will be living with and relying on GPS and its counterparts elsewhere in the world for a long time. "GPS is the only system I've ever worked on that has surpassed expectations," Buesnel admitted. "We talk about its vulnerabilities, but it is in such wide use that we need to be more aware of the risks. Get quantifiable data, and do your risk assessments, and you will be fine." **BCA**