A CLOSER LOOK

ANALYZING THE NEWS THAT MAKES A DIFFERENCE

Russia's Jamming of GPS at Ben Gurion

CAN MOSCOW HACK YOUR AIRPLANE FLIGHT?

BY YOSSI KRAUSZ

For the last few weeks, there have been reports that the GPS systems that airplanes use to land at Ben Gurion Airport have been failing. According to reports, that's not a simple technical issue. It's a military decision made by a foreign country.

Since last year, commercial aircraft flying in some areas above the Middle East have noticed a problem with their GPS positioning systems, finding either that they were not working at all or that they were showing the aircraft to be in a different position from its actual one.

There was one major suspect in the strange anomalies: Russia. With multiple military bases in Syria, Russia has been engaged in an attempt to control the skies over that war-torn country. One of those ways was to fool GPS, which could lead enemy drones or other aircraft to their targets.

That may have become more urgent for the Russians after an incident in January 2018, in which a swarm of drones attacked Hmeimim Air Base in western Syria. The Russians blamed the attack on the US, which denied it. Several similar drone attacks occurred throughout 2018—and it was then that the GPS problems started occurring.

This kind of GPS jamming or spoofing is something that Moscow had reportedly carried out in Ukraine and elsewhere, as well. The think tank C4ADS issued a report earlier this year detailing almost 10,000 instances of GPS interference that Russia appears to have been involved in.

Those problems had not reached into Israel until very recently. But on June 25, the International Federation of Air Line Pilots' Associations issued a statement noting that multiple pilots had experienced loss of their GPS signal near Ben Gurion. And the interference has reportedly been reaching farther, even as far as Cyprus. According to some experts, that may mean that the Russians have started using a transmitter at a higher altitude for the interference, with a longer range around the curvature of the earth.

What does this mean for safe flight to and from Israel—or anywhere around the world?

DENIALS AND THE VIEW FROM SPACE

Russia, for its part, has denied having anything to do with the GPS problems. The Russian Embassy in Israel told the Times of Israel that the idea was "fake news" and that they couldn't "respond seriously" to it.

The IDF was coy about naming a source for the interference, but anonymous Israeli officials have told the media that it was the Russians.

Furthermore, Prof. Todd Humphreys of the University of Texas, who studies satellite navigation and related issues, told multiple media outlets that he has been able to trace the disruption to Hmeimim Air Base by several methods, including using sensors on the International Space Station.

"[The signal] is so strong that I can see it from space," he said.

BY YOSSI KRAUSZ

One important note is that Russia itself doesn't use the GPS system for navigation. It has an alternate satellite network called GLONASS. (China, the EU and Japan also have alternate systems.) So fooling with GPS comes at no cost to Russian navigation.

JAMMING OR SPOOFING

Experts say that Russia has been using some of the most sophisticated methods to interfere with GPS signals.

Jeffrey C. Price is a professor at Metropolitan State University of Denver and the owner of Leading Edge Strategies, an airport management training company. He is also an expert in airport safety and security.

He told *Ami* by email: "Military aircraft have had the ability to jam and also project false images on enemy radar for a few decades now. The methods of attack are relatively similar. For example, to jam a radar or radio wave, the jamming source essentially starts broadcasting noise over a range of radio or radar frequencies, which renders the frequencies unusable; think of a million people trying to use their cell phones at once and going through just a single cell-phone tower.

"To intercept a frequency, the radio unit quickly scans a broad range of frequencies until it finds the ones the aircraft is using, then begins transmitting its own data to the plane."

Aircraft flying into Ben Gurion, in fact, have been experiencing this second, more complicated kind of interference, with the apparently Russian transmitters "spoofing" GPS.

Prof. Price noted that, there, the GPS system has a built-in way for the Russians to attack it.

"The GPS technology used in commercial aviation today is supplemented by ground-based augmentation facilities, known as wide-area augmentation or ground-based augmentation [depending on the facility]," he said. These are essentially land-based transmitter stations that know their exact location on the planet. When an aircraft is using GPS for landing guidance, these ground-based stations compare their position information with the information coming from the GPS satellites, then correct for any GPS errors to increase the accuracy of the GPS signal.

"The same technology that is used to improve the accuracy of a GPS signal can also be used to create errors within that signal. This is a cyber-attack that we've been warning the industry about for years."

"Without getting overly technical, the same technology that is used to improve the accuracy of a GPS signal can also be used to create errors within that signal. This is a cyber-attack that we've been warning the industry about for years. With increasing reliance on satellite-based navigation systems, aircraft are more susceptible to cyber-attacks of this nature."

He said that this isn't really a new capability per se.

"Military forces around the world have used this type of technology for many years. Some militaries, such as the US military, have aircraft that just do radar and radio-wave jamming types of attacks.

"The hacker industry has already demonstrated its ability to intercept and send false information to vehicle and cell-phone GPS signals."

Israeli aviation officials have suggested that this isn't a very dangerous threat to landing at Ben Gurion, because aircraft have other instruments that they can use for landing. How dangerous does Prof. Price consider this situation?

"It really depends on the aircraft," he said. "The more the plane relies on electronics, the more it relies on GPS for much of its information. Many modern avionics rely on GPS, but aircraft still have backup systems such as magnetic headings from a normal compass, an altimeter, airspeed and altitude indicators that don't rely on the GPS system. Pilots also still have charts and in-flight procedures for things like failure of the navigational or communications systems.

"From an en route perspective, there is the potential to put aircraft at the same altitude on opposing headings [i.e., so they would crash into one another] but even then, most pilots would wonder why they were given a certain altitude that they know is not normal for that block of airspace based on the directions they hear other aircraft are receiving.

"Landing is the most critical phase of flight. If the aircraft was relying just on the GPS for landing, in bad weather and with poor visibility, but the pilots are receiving an erroneous reading, such as being 100 feet higher than they actually are, then the potential for a crash is higher.

"Even then, there are proximity warning devices in the plane that don't rely on GPS to alert pilots if they are too low on an approach. So these types of 'attacks' definitely increase the danger for an airliner, but not as much as if you fired a missile at one."

Prof. Price said that this story illustrates the "delicate nature of flight," adding, "The more we rely on the Internet of Things, satellite-based technology, and technology that does things for us, the more vulnerable we are to cyber-attacks." ●