Electronic Warfare Spooks Airlines, Pilots and Air-Safety Officials; Hundreds of daily flights around the world are running into GPS spoofing, a hazard that poses new risks for pilots and passengers

Tong, Adrienne; Churchill, Carl

FULL TEXT

American Airlines Capt. Dan Carey knew his cockpit equipment was lying to him when an alert began blaring "pull up!" as his Boeing 777 passed over Pakistan in March—at an altitude of 32,000 feet, far above any terrain.

The warning stemmed from a kind of electronic warfare that hundreds of civilian pilots encounter each day: GPS spoofing . The alert turned out to be false but illustrated how fake signals that militaries use to ward off drones and missiles are also permeating growing numbers of commercial aircraft, including U.S. airlines' international flights.

"It was concerning, but it wasn't startling, because we were at cruise altitude," Carey said. Had an engine failure or other in-flight emergency struck at the same time, though, the situation "could be extremely dangerous."

Pilots, aviation-industry officials and regulators said spoofed Global Positioning System signals are spreading beyond active conflict zones near Ukraine and the Middle East, confusing cockpit navigation and safety systems and taxing pilots' attention in commercial jets carrying passengers and cargo.

The attacks started affecting a large number of commercial flights about a year ago, pilots and aviation experts said. The number of flights affected daily has surged from a few dozen in February to more than 1,100 in August, according to analyses from SkAI Data Services and the Zurich University of Applied Sciences.

Modern airliners' heavy reliance on GPS means that fake data can cascade through cockpit systems, creating glitches that last for a few minutes or an entire flight. Pilots have reported clocks resetting to earlier times, false warnings and misdirected flight paths, according to anonymized reports shared with government and industry groups.

Aviation-safety officials said spoofing has disrupted some flights but hasn't posed major safety risks. While pilots are trained on how to use non-GPS navigation systems as a backup, managing the bogus GPS signals and alerts risks dividing pilots' attention if a more serious problem strikes.

"If we lose an airplane because of workload issues because of these problems we're encountering, compounded with an emergency, that is going to be a horrendous event," said Ken Alexander, the Federal Aviation Administration's chief scientist for satellite navigation, during a pilot union forum this month in Washington, D.C.

Airlines are huddling with aircraft makers, suppliers and air-safety regulators to develop short-term workarounds and longer-term fixes. Equipment standards designed to harden civilian aircraft against spoofing won't be issued until next year at the earliest, according to people familiar with the matter.

Pilots are meanwhile getting preflight briefings about how to identify potential spoofing and respond—which may at times include turning off certain features or ignoring false "pull up!" commands from a safety system heralded for sharply reducing crashes.

Pilots in some cases have pulled up unnecessarily, according to industry officials. Other aircraft systems, including pilot messaging services, have been thrown off when cockpits draw false time and position data from spoofed signals.

Researchers said the volume of faked GPS signals has surged over the past six months. Most spoofing attacks

come from powerful electronic-warfare transmitters in Russia, Ukraine and Israel , said Todd Humphreys, a professor of aerospace engineering at the University of Texas at Austin. Hand-held devices can also spoof GPS signals in a smaller area.

Civilian flights apparently haven't been targets, though that is little comfort to commercial pilots flying through some of the world's busiest air corridors.

"These pilots are doing double duty in the cockpit," Humphreys said, citing pilot reports. He said the industry and regulators should fast-track work to harden planes against spoofing before one has an accident. "This is embarrassing for the airline industry, for the carriers and for the FAA," he said.

The variety of attacks across different locales have caused a range of problems, according to anonymized reports collected by OpsGroup, an aviation-safety organization that includes pilots, dispatchers and other airline staff.

A spoofed GPS signal in September 2023 nearly sent a private Embraer jet into Iran without clearance, a misdirection that could have led the plane into hostile airspace. The crew of an Airbus A320 departing from Cyprus in July reported a "severe map shift" in the cockpit and the failure of a separate navigation system. A Boeing 787 the same month aborted two landings, one of them 50 feet above the ground, after the loss of a GPS signal kicked off a series of instrument problems.

The FAA said it knew of no spoofing events in the U.S., though industry and government officials said there have been sporadic reports in recent years of possible spoofing or other types of GPS interference that can cause similar disruptions.

In October 2022, GPS interference disrupted air traffic at Dallas Fort Worth International Airport. Some planes went off course, and one got too close to another aircraft on final approach in a minor violation of federal rules that keep planes safely apart, according to a government official. Pilots had to rely on conventional navigation systems for their approaches for about two days.

The FAA earlier this year said it found no proof of intentional interference and was continuing to examine the cause.

GPS spoofing has disrupted operations in Europe but hasn't endangered flights, said Florian Guillermet, executive director of the European Union Aviation Safety Agency. Pilots have had to divert to airports they weren't intending to land at, and earlier this year an airline temporarily halted operations to an Estonian airport that wasn't equipped with ground-based navigation as a backup for GPS.

"The risk is growing in terms of the number of occurrences," Guillermet said in June.

Industry and government officials are weighing how to address the immediate risks.

Carriers including United Airlines and American Airlines have been discussing new procedures that would allow pilots to reset cockpit circuit breakers when confronted with false GPS data.

Airlines and regulators are generally reluctant to let pilots reset systems using circuit breakers, a step that could require them to stand up or introduce other risks such as electrical issues. Boeing hasn't endorsed the procedure on its 777 aircraft, people familiar with the matter said. The FAA declined to comment on the procedures.

Boeing said manufacturers, carriers and regulators globally are contributing GPS expertise for solutions to ensure safety. Boeing and Airbus are working with airlines to help develop procedures to assist pilots, the companies said.

United and American said their pilots are equipped with several ways to navigate with precision, even with GPS interference. American said it hasn't experienced disruptions or significant safety concerns from GPS interference.

Industry officials are urging pilots to stick to manufacturers' and regulators' procedures, given the absence of uniform guidance. "We don't want a do-it-yourself approach," said Andy Uribe, an aviation-security expert with the Air Line Pilots Association union, during a panel discussion last week.

Christopher Behnam, who retired in August as a Boeing 777 captain at United, said he frequently encountered GPS interference flying into the Middle East.

"We are trained for these things, so you stay calm and you just follow the procedure," Behnam said. Still, he said, when pilots rely on GPS to land in low-visibility conditions, spoofing "could get very, very, very alarming."

Write to Andrew Tangel at andrew.tangel@wsj.com , Drew FitzGerald at andrew.fitzgerald@wsj.com , Adrienne Tong at adrienne.tong@wsj.com and Carl Churchill at carl.churchill@wsj.com

Credit: By Andrew Tangel and Drew FitzGerald | Graphics by Adrienne Tong and Carl Churchill

DETAILS

Subject:	Aviation; Public officials; Pilots; Airlines
Business indexing term:	Subject: Airlines; Corporation: Airbus SAS; Industry: 48111 : Scheduled Air Transportation
Location:	Middle East; United States--US; Ukraine
Company / organization:	Name: Airbus SAS; NAICS: 336411, 336412, 336413; Name: Federal Aviation Administration--FAA; NAICS: 926120; Name: American Airlines Inc; NAICS: 481111
Classification:	48111: Scheduled Air Transportation
Publication title:	Wall Street Journal (Online); New York, N.Y.
Publication year:	2024
Publication date:	Sep 23, 2024
column:	Business
Section:	Business
Publisher:	Dow Jones &Company Inc.
Place of publication:	New York, N.Y.
Country of publication:	United States, New York, N.Y.
Publication subject:	Business And Economics
e-ISSN:	25749579
Source type:	Newspaper
Language of publication:	English
Document type:	News
ProQuest document ID:	3107820363
Document URL:	https://ezproxy.lib.utexas.edu/login?url=https://www.proquest.com/newspapers/electronic-warfare-spooks-airlines-pilots-air/docview/3107820363/se-2?accountid=7118
Copyright:	Copyright 2024 Dow Jones &Company, Inc. All Rights Reserved.

Full text availability:	This publication may be subject to restrictions within certain markets, including corporations, non-profits, government institutions, and public libraries. In those cases records will be visible to users, but not full text.
Last updated:	2024-09-23
Database:	Latin American Newsstream,ABI/INFORM Global

LINKS

Find it @UT