Aviation companies and European regulators say they will increase documentation and alert procedures about GPS tampering after a recent uptick in incidents near war zones.

Commercial airlines raised concerns after an increase in so-called GPS jamming, when geopositioning signals are blocked so a flight location isn't shown, and spoofing, when a GPS shows a false location, in particular in the Middle East and around Ukraine and Russia.

The incidents highlight cybersecurity risks, although they haven't caused safety issues, said Stuart Fox, director of flight and technical operations at the International Air Transport Association, a trade group that represents airlines.

"It's a global situation," Fox said. "The Global Positioning System or satellite-based systems are very accurate, but you can't just rely on those," he said.

There were reports last year of GPS spoofing near Ukraine, and also in nearby countries such as Poland and Baltic states, and in the Mediterranean and areas around Israel, according to the European Union Aviation Safety Agency.

IATA and EASA said they would take steps to share information about incidents of GPS tampering and make sure pilots and crew can identify when it is happening. Planes must be capable of using backup ground technology systems to navigate when GPS is spoofed or jammed, they said in a statement last week.

"For the longer term, we need to ensure we are involved in the design of future satellite navigation systems. Countering this risk is a priority for the Agency," the statement said.

In some planes, pilots have been able to switch off GPS when they encounter spoofing, but with other types of equipment on planes, that isn't possible because it would be too late to switch to backups, said Todd Humphreys, a professor of aerospace engineering at the University of Texas at Austin, who researches GPS spoofing.

In 2022 and 2023, EASA, the European regulator, warned about an increase in reports of GPS spoofing and jamming incidents taking place in areas surrounding Russia, including in Finland, around the Black Sea and in the Baltic Sea area. In one bulletin, EASA said pilots were forced to reroute planes or change their destinations midflight.

Experts say the increase in GPS spoofing affecting commercial airlines highlights the potential for the issue to cause chaos.

One result of GPS interference could be that pilots don't know exactly where the plane is situated or they could fly over conflict zones inadvertently, and signal a false position to other aircraft, he said. Pilots and other crew members need training to address cybersecurity risks just as they already think about physical safety, said Thomas Hutin, a senior managing director at FTI Consulting.

"Today the aerospace industry is not completely prepared for that because the system hasn't been designed to be able to take this kind of scenario into consideration," he said.

Commercial aircraft can be collateral damage as conflicts escalate and militaries send false GPS signals to try to intercept drones and other aircraft, Humphreys said.

The worst-case effects could be that pilots veer into airspace where they aren't authorized to be and risk their plane being shot down, he said.

Pilots who lose access to GPS navigation can overwhelm air-traffic control systems that need to guide them, he said.

To share more information, data on separate technology platforms must be coordinated, said Fox. IATA runs one such database. EASA, the regulator, said it would send out alerts to manufacturers, airlines and airports about attacks.

The uptick in GPS spoofing and jamming points to security issues that go beyond aviation.

Critical infrastructure in many sectors uses GPS, and there could be huge problems if the technology were falsified, Humphreys said.

"Many of the systems that are in use today have never really met their match in GPS spoofing. This was a wake-up call for aviation, but other systems have yet to be tested," he said.

Credit: By Catherine Stupp

Word count: 645