

Editor's Note

BY JOY FINNEGAN
EDITOR-IN-CHIEF

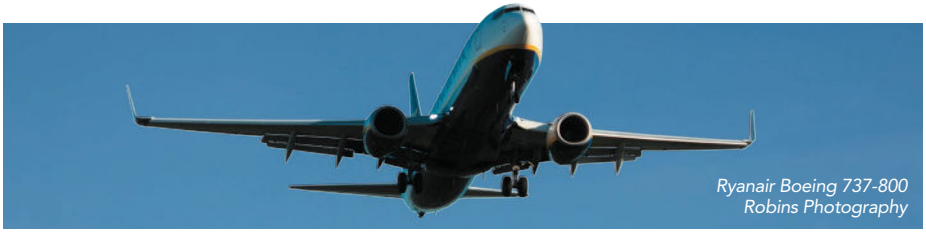
If It's Not One Thing, It's Another

There have been so many huge aviation security stories recently that I've been reminded of the classic Saturday Night Live character, Roseanne Roseannadanna, who used "If it's not one thing, it's another!" as her catchphrase. It has truly been a period of one thing after another.

First, we had the flydubai incident. I won't go into that much here as we have our editor emeritus, Philip Baum, taking an in-depth look at the events of Flight 1073. He looks at insider threats, pilot radicalization and gives some history of how we ended up here with a locked cockpit door and a pilot with ready access to a crash axe who was focused on killing all aboard, as well as people on the ground and martyrdom.

The Boeing 737 MAX plunged over 17,000 feet in less than a minute and approached the speed of sound. Another miraculous data point was that the airframe proved its ability to survive a descent rate exceeding 30,000 feet per minute and land safely even with a severely damaged rudder.

That incident and the quick thinking of all involved turned out to be a true miracle as all aboard survived. The captain — Smit Machchhar, a plumber named Yaniv Hayoun, who helped subdue the attacking first officer and stabilized the aircraft, the relief crew that just happened to be aboard and who jumped into the cockpit and flew the disabled aircraft, as well as the passengers who rushed to help, are all heroes. This is an extraordinary event. For more on the flydubai incident, please read Philip Baum's piece starting on page 14.



Ryanair Boeing 737-800
Robins Photography

Bomb Threat Hoaxes

Next, there has been a striking cluster of bomb threats against commercial airlines in recent weeks, particularly in Europe and on flights involving Israel. On November 3 alone, at least four passenger flights were targeted by reported bomb threats across Europe, prompting diversions, aircraft evacuations, military fighter escorts, airport closures and extensive security searches.

The incidents raise an important aviation security question: Are we seeing unrelated hoaxes, a coordinated campaign intended to disrupt commercial aviation or a new form of intimidation targeting airlines?

There were a few isolated bomb threats in October. But in early November, they revved up. On November 2-3 there were nine bomb threats causing diversions and airport closures which impacted a diverse array of airlines that included Wizzair, El Al, Ryanair, SAS and LOT Polish Airlines, among others. Reported numbers vary but subsequent waves targeted around 18 commercial flights on November 5 and around 18 flights on November 6. The total was 45 targeted aircraft (these numbers vary). In addition, multiple newsrooms in Europe and thousands of schools in Italy, the U.K. and Ireland were also subjected to bomb threats. No explosives were found in any of the incidents.

An actual bomb isn't necessary to cause a significant disruption. An anonymous email, telephone call or social media message can trigger an aircraft diversion, security response, flight delays and potentially airport closures.

This type of widescale bomb threat is not unheard of. In October 2024, Indian carriers experienced an extraordinary wave of threats. More than 120 flights were targeted in less than two weeks. In total, there were 728 hoax bomb threats that targeted airlines in India during 2024. Eventually, 13 people were arrested in connection with those threats, but authorities suspected many more were involved. The vast majority of the threats were sent using encrypted email services, Virtual Private Networks (VPNs) and anonymous social media accounts routed through foreign servers, so the authorities said most of the perpetrators were never caught.

Some threatening emails received at airports in Rome and Sofia were signed by purported members of "Male State," a name associated with a Russian ultranationalist, misogynistic movement. It was reported that the movement's founder, Vladislav Pozdniakov, denied involvement and said the organization had ceased operating in 2021. European intelligence services are also reportedly examining a possible Russian connection, according to reporting attributed to the Financial Times.

European Transport Commissioner Apostolos Tzitzikostas said on November 11, 2026, that arrests had been made in several cities in connection with the wave of bomb threats against European commercial flights. At the time of his statement, the commissioner did not identify the suspects, specify how many people had been arrested, or name the cities or countries where the arrests occurred. The arrests were publicly acknowledged, but their precise connection to individual threatened flights remains unclear.

The recent surge in airline bomb threats raises a serious concern about complacency. When repeated threats prove to be hoaxes, there is a risk that airline personnel, airport security teams and law enforcement may become desensitized, potentially underestimating

a genuine threat. This phenomenon, often called alert fatigue, can undermine vigilance and decision-making. Aviation history, including the Richard Reid shoe-bomb attempt and the attempted bombing of Northwest Airlines Flight 253, demonstrates that explosives can evade security screening and reach aircraft. The challenge for aviation security is to maintain a consistently high level of vigilance without allowing repeated false alarms to overwhelm resources or compromise operational efficiency. Every threat requires a credible, proportionate assessment, regardless of how many previous warnings have proved false.

Repeated bomb hoaxes present aviation security agencies with a difficult balancing act. Authorities must respond decisively to credible threats while avoiding unnecessary disruption and the desensitization that can accompany frequent false alarms. Training, intelligence sharing, standardized procedures and security audits help maintain vigilance, but the true test is whether personnel can assess the next warning objectively, regardless of how many previous alerts have proved false.

Aviation security analysts have suggested several possibilities, including copycat threats, a coordinated effort by individuals or groups, or attempts to destabilize aviation operations through so-called hybrid warfare. Authorities have not confirmed any of these explanations.

These incidents underscore the importance of intelligence sharing, standardized threat assessments and coordinated international responses to protect passengers while minimizing unnecessary disruption.

And thankfully, just as abruptly as they started, the hoax bomb threats ended.

Nationwide Ground Stop

On November 13, the United States experienced something that should give everyone involved in aviation safety and security serious pause. The Federal Aviation Administration (FAA) ordered a nationwide ground stop after a telecommunications failure disrupted air traffic control operations across parts of the country. Thousands of flights were affected, passengers were stranded and the aviation system experienced a disruption of extraordinary proportions.

The remarkable thing is that this apparently wasn't a cyberattack, an act of terrorism or a coordinated attempt to sabotage American aviation. It appears to have been triggered by routine telecommunications modernization work.

Think about that for a moment.

According to the FAA, the failure affected 17 of the nation's 22 en route air traffic control centers. Investigators identified network equipment at facilities in Arkansas and Texas as possible sources of excessive traffic that overwhelmed portions of the system. The contractor responsible for the FAA's telecommunications network, L3Harris, was performing upgrades as part of the transition from aging copper connections to fiber-optic infrastructure. A relatively localized technical problem had nationwide consequences.

To its credit, the FAA acted conservatively. Aircraft already airborne were allowed to continue to their destinations, and controllers safely managed those flights while additional departures were suspended. From a safety standpoint, limiting traffic during a widespread communications failure was a defensible decision.

But why did the failure become so widespread in the first place?

We routinely hear about the redundancy built into aviation systems. Aircraft have backup instruments, multiple communications capabilities and carefully engineered protections against individual equipment failures. Pilots train extensively for abnormal and emergency situations. The aviation industry has spent decades developing a safety culture built around anticipating failures before they become catastrophes. Shouldn't we expect the same philosophy to govern the infrastructure supporting the entire National Airspace System?

The FAA has backup communications equipment, alternative frequencies and established contingency procedures. Yet this incident demonstrates that redundancy is only as effective as the architecture supporting it. Multiple backup systems offer limited protection if they depend on shared infrastructure vulnerable to the same failure. That is a fundamental resilience issue, and one that deserves a thorough, independent investigation.

There is also the question of contractor oversight. L3Harris operates the telecommunications network and was involved in the modernization work associated with the disruption. The company is cooperating with investigators, and responsibility for the failure has not been established. Nevertheless, we should ask whether the FAA has sufficient independent oversight of critical network changes and the ability to identify and isolate problems without depending entirely on its contractors.

Then there is the money. Following the disruption, Transportation Secretary Sean Duffy called for an additional $50 billion to modernize America's air traffic control system. That comes after Congress approved $12.5 billion in modernization funding in 2025.

Few would dispute that the system needs substantial investment. Much of its infrastructure is decades old, and modernization has been delayed through multiple administrations.

But the Government Accountability Office has identified significant weaknesses in the FAA's modernization planning, including the absence of a comprehensive lifecycle cost estimate and integrated master schedule.

Before committing tens of billions more, taxpayers deserve to know precisely what will be purchased, when improvements will be delivered and how success will be measured. Money alone will not fix a system whose vulnerabilities are poorly understood.

The November 13 disruption should also prompt a broader discussion about how we define transportation security. We tend to associate security with preventing deliberate threats: terrorism, cyberattacks, sabotage and unlawful interference. But infrastructure resilience is equally essential. An accidental technical failure can produce operational consequences comparable to those of a malicious attack.

The aviation industry rightly celebrates its extraordinary safety record. That record reflects rigorous training, engineering discipline, redundancy and a willingness to learn from failures. We should apply those same standards to the systems on the ground.

The question is not simply how quickly the FAA can replace aging equipment. It is whether the next generation of air traffic control infrastructure will be sufficiently resilient to prevent one localized malfunction from disrupting an entire nation.

We should not need another nationwide ground stop to find out.