# Aviation security depends on detecting the threats from within

Eyal Tsir Cohen and Larry Maher - 2026-10-16

Original: https://nationalpost.com/opinion/security-depends-on-detecting-the-threats-from-within

Shared by Exigent Foundation with the contributor's permission.

NP Comment

Opinion: Aviation security depends on detecting the threats from within

We've made it harder for an attacker to get through a passenger check-in. But what about insiders who already have permission to be there?

Profile picture of Special to National Post

By

Eyal Tsir Cohen and Larry Maher, Special to National Post

October 16, 2026 at 11:00 a.m.

Last Updated: October 16, 2026 at 1:23 p.m.

On Sept. 30, the co-pilot of a Flydubai flight bound for Tel Aviv attacked the captain with a cockpit crash axe and tried to seize control of the aircraft, according to the United Arab Emirates' prosecutor general. Emirati authorities have described it as an attempted terrorist attack. The investigation must establish the full circumstances, including motive and any outside connections.

Westerners should pay attention. September 11 demonstrated that an aircraft can become a weapon, with consequences far beyond the passengers on board. An attack on a flight to Israel may appear to be a regional security problem. The vulnerability it exposes belongs to the entire aviation system.

We have spent decades making it harder for an attacker to get through the passenger checkpoint. The insider threat starts with someone who already has permission to be there.

Pilots, maintenance workers, baggage handlers and catering staff perform essential jobs. Their access is necessary for aviation to function. It also places a particular responsibility on those who employ them, issue their credentials and evaluate security concerns. A trusted position cannot become a reason to stop asking whether that trust remains justified.

The bombing of Metrojet Flight 9268 is a warning. On Oct. 31, 2015, the Russian airliner was destroyed after taking off from Sharm el-Sheikh International Airport in Egypt, killing all 224 people aboard. ISIS claimed responsibility. Reuters later reported suspected involvement by airport insiders, including a mechanic and a baggage handler; Egyptian officials disputed the reported arrests and suspicions. Those allegations should not be treated as settled fact. Airports must nevertheless examine every route by which an explosive could reach an aircraft, including through workers with trusted access.

Aviation terrorism has never been confined to one country or one people. Air India Flight 182, Pan Am Flight 103 and the 9/11 attacks killed people of many nationalities and faiths. Their perpetrators understood the same thing: bringing down an airliner can spread fear, disrupt economies and change government policy.

Many familiar screening procedures developed in response to particular attacks and plots. Physical screening remains indispensable. But a scanner can detect a dangerous object without telling us whether someone with authorized access is being recruited, coerced or directed by a terrorist organization.

The answer requires two co-ordinated efforts.

The first is intelligence. Security services must identify recruitment, financing, operational direction and attempts to infiltrate airlines or airport operations before an attack reaches the boarding gate. That requires close co-operation across borders. North American travellers frequently use foreign airlines and transfer through foreign airports. Their protection depends in part on information held by partner governments.

The 2017 plot against an Etihad flight from Sydney illustrates the point. ISIS operatives directed a plan to place an explosive device aboard the aircraft. The device never made it onto the plane. Israeli intelligence subsequently helped Australian authorities identify and arrest the plotters. Intelligence sharing exposed a continuing conspiracy after the initial bombing attempt had failed.

The second effort is security throughout an employee's access to sensitive facilities. Background checks at recruitment are essential, but circumstances can change. Credible concerns raised later must reach officials who have both the authority and the responsibility to assess them. Access should be limited to what a person's work requires, reviewed when duties change and withdrawn promptly when that access is no longer needed.

Canada vets its airport workers. Anyone seeking access to restricted areas must obtain a Transportation Security Clearance and a Restricted Area Identity Card, but a clearance is a snapshot taken at the time of hiring. A person's circumstances, associations and loyalties can change long after the background check is complete. A W5 investigation published in May 2026 reported that between 2021 and 2026, more than 7,500 airport workers at Canada's four largest airports were flagged for security concerns and still received clearance, including an individual later charged in the largest gold heist in the country's history. A flag is not proof of wrongdoing, but a clearance cannot be the end of the question. A good system has to keep checking after the first approval.

The United States already has the Transportation Security Administration and recurrent vetting of aviation workers. The practical question is how reliably those systems work together. When an employee changes an airline or airport, can a serious unresolved security concern disappear between institutions? Who reviews new information, and how quickly can access be restricted when the evidence warrants it? Governments and employers need lawful channels for sharing such concerns across borders, with clear responsibility for following them up.

Employees also need a reliable way to report coercion, threats or suspicious approaches without assuming they will be punished for coming forward. An employer that discourages reporting can lose the warning it needs most. Any restriction on access should be reviewable through a fair process.

Artificial intelligence may assist the lawful analysis of publicly available information, helping identify relevant connections and significant changes. It must support trained human judgment. A person's nationality or religion cannot substitute for evidence of a genuine threat. Clear standards, privacy protections and a way to correct mistakes are necessary for a system that depends on public trust.

Security must also reflect the risk of the particular route. Between 2016 and 2019, Eyal worked with Israel's

Ministry of Transport on protections for flights to Israel, including from Turkey, during a period of extensive ISIS activity there. The starting point was that passengers required protection even when the aircraft was foreign. Measures included tighter screening, greater use of technology and stricter control over those handling aircraft and baggage.

That experience underscored the need for co-operation among Israel's external intelligence service, Mossad; its internal security service, Shin Bet; and the Ministry of Transport and Road Safety, including its Civil Aviation Authority and aviation-security officials. These institutions have distinct responsibilities. Intelligence must inform security decisions, while civil aviation authorities address regulatory and operational requirements. Airlines and airports must put the resulting measures into practice. Comprehensive passenger protection depends on their co-operation. A warning must reach the authority able to act on it, with someone accountable for ensuring that it does.

The same principle applies to Americans abroad. The flag painted on an aircraft cannot determine the limits of a government's concern for its citizens.

Passenger well-being includes both safety and the ability to travel with reasonable comfort, dignity and confidence. Long delays, intrusive questioning and repeated checks impose real costs on travellers and the aviation industry. Governments should be able to explain how a proposed measure addresses a credible risk, whether a less burdensome option would work and how its effectiveness will be assessed. Measures that no longer serve a clear purpose should be revised or removed.

Against the backdrop of conflict and tension in the Middle East, Europe and Russia, the pressure to add restrictions can be considerable. The response must remain proportionate. More intensive protection may be warranted for a particular route or a specific warning, without imposing the same burden on every journey. Better intelligence, co-ordination and technology should help focus security where it is needed, while reducing avoidable inconvenience. Privacy and fair treatment are part of a durable security system.

This work needs clear public accountability. Governments must set standards, verify compliance and ensure that airlines, airports and security services act on relevant information. Whether a particular function is performed by public employees or contractors, responsibility for protecting the system remains with government.

There is a diplomatic dimension as well. The Abraham Accords created new connections between Israel and its Arab partners. Terrorists may seek to damage those relationships by frightening passengers and disrupting air travel. The motive in the Flydubai case remains under investigation, but the broader risk is clear.

The response should strengthen those connections through better intelligence and security co-operation. Passengers should be able to keep flying with confidence. Airlines and governments must earn that confidence by addressing the threat wherever it originates, including inside their own systems.

Special to National Post

Eyal Tsir Cohen was a top-level director at Israel's leading intelligence agency at the Prime Minister's Office and is a former fellow at the Brookings Institution in Washington, D.C. Larry Maher is CEO of The Exigent Foundation.