

OCTOBRE 2026

POLICY BRIEF

# L'INCIDENT DU VOL FZ1073 DE FLYDUBAI

## vers une nouvelle génération de menaces contre l'aviation civile ?

---

ABDELHAK BASSOU



*L'incident du vol FZ1073 entre Dubaï et Tel-Aviv ne permet encore aucune attribution définitive. Il constitue en revanche un révélateur utile : à mesure que la sûreté aérienne ferme les voies classiques d'intrusion, la menace cherche à emprunter des voies alternatives en exploitant les personnes, les prestataires et les systèmes auxquels l'écosystème aéronautique doit nécessairement accorder sa confiance.*

**ABDELHAK BASSOU**

---

## INTRODUCTION — LES QUESTIONS LAISSÉES OUVERTES PAR L'INCIDENT DE FLYDUBAI

Le 30 septembre 2026, le vol FZ1073 de Flydubai, reliant Dubaï à Tel-Aviv, a été dérouté vers Tabouk, en Arabie saoudite, après un incident violent dans le cockpit. Selon les informations disponibles au 1er octobre 2026, le copilote aurait agressé le commandant et provoqué une descente extrêmement rapide de l'appareil avant d'être maîtrisé ; d'autres pilotes de Flydubai présents à bord auraient ensuite assuré l'atterrissage. Les autorités émiraties ont ouvert une enquête portant notamment sur le caractère prémédité des faits et sur une éventuelle finalité terroriste. À ce stade, le mobile n'est pas établi et aucun lien avec une organisation ou un État n'a été démontré.<sup>1</sup>

Cette réserve est essentielle. L'analyse stratégique ne doit ni devancer l'enquête judiciaire ni transformer une coïncidence chronologique en causalité. Elle peut cependant partir d'un événement encore imparfaitement élucidé pour identifier les vulnérabilités qu'il révèle et les hypothèses qu'il rend pertinentes.

Le cas Flydubai fait ainsi émerger quatre questions. L'aviation civile pourrait-elle redevenir une cible privilégiée de la violence politique sous des formes différentes des détournements des années 1960 à 1980 ? Le contexte de confrontation autour de l'aviation iranienne autorise-t-il, sans permettre encore aucune attribution, à conserver une hypothèse iranienne ? Les organisations terroristes pourraient-elles chercher à infiltrer, recruter ou retourner non seulement des pilotes ou des personnels navigants commerciaux, mais l'ensemble des personnels bénéficiant d'un accès privilégié à l'écosystème aéronautique ? Enfin, la numérisation croissante de cet écosystème ne déplace-t-elle pas une partie du risque vers les systèmes, les données, les prestataires numériques et les chaînes d'approvisionnement technologiques ?

Ces questions ont un point commun : elles invitent à réfléchir non seulement à la protection de l'aéronef, mais aussi à celle de tout l'écosystème qui soutient l'aviation civile et permet son fonctionnement. La sûreté aérienne s'est historiquement construite autour du contrôle des accès physiques ; elle doit désormais composer avec les accès légitimes des acteurs internes et avec l'accès numérique aux fonctions critiques.<sup>2</sup>

### Une histoire de la sûreté faite d'adaptations successives

La lutte internationale contre les actes d'intervention illicite dans l'aviation civile s'est structurée à partir de la forte augmentation des détournements dans les années 1960. Après les conventions de Tokyo, de La Haye et de Montréal, l'Organisation de l'aviation civile internationale (OACI) adopte en mars 1974 les premières normes et pratiques recommandées de l'Annexe 17 à la Convention de Chicago. Cette annexe devient applicable en 1975. Son objectif est de protéger les passagers, les équipages, les personnels au sol et le public contre les actes d'intervention illicite.<sup>3</sup>

---

1. Reuters, 30 sept. – 1er oct. 2026 : Une enquête est ouverte par les autorités émiraties sur le mobile, la préméditation et une éventuelle finalité terroriste ; aucun lien extérieur n'est alors établi.

2. Dans son "Insider Threat Toolkit", l'OACI définit l'insider comme un employé à temps plein ou partiel, un contractant, un temporaire ou un travailleur indépendant du secteur aéronautique dont la fonction lui procure un accès privilégié ou des connaissances relatives à des lieux sécurisés, des biens ou des informations sensibles.

3. L'Annexe 17 à la Convention relative à l'aviation civile internationale (Convention de Chicago) est le document officiel de l'OACI consacré à la sûreté de l'aviation civile. Elle définit les normes et pratiques recommandées visant à protéger le transport aérien contre les actes d'intervention illicite, tels que les détournements d'avions, les attentats ou le sabotage.

---

Étudier l'Annexe 17 et en saisir l'importance exige de la considérer comme un dispositif évolutif, et non comme un texte figé. L'OACI la révisé régulièrement en fonction des transformations de la menace et des technologies. Son histoire permet ainsi de lire la sûreté aérienne comme une dialectique : une menace révèle une vulnérabilité ; la norme ferme ou réduit cette vulnérabilité ; l'acteur hostile recherche alors un autre point d'accès ; la norme doit de nouveau s'adapter.

- Dans un premier temps, des années 1960 aux années 1980, la menace dominante était celle de l'intrusion.

Un individu cherche à introduire une arme ou un explosif, à prendre des otages ou à détourner un appareil. La réponse privilégie donc le filtrage des passagers et des bagages, le contrôle des accès aux zones réservées, la fouille de sûreté des aéronefs et la protection du fret et des approvisionnements.

- Les attentats du 11 septembre 2001 produisent une rupture supplémentaire.

L'avion n'est plus seulement l'objet du détournement : il peut devenir l'arme elle-même. Aux États-Unis, l'Aviation and Transportation Security Act de novembre 2001 crée la Transportation Security Administration (TSA) et fédéralise le contrôle de sûreté. Parmi les mesures emblématiques figurent le filtrage de 100 % des bagages de soute, l'extension du Federal Air Marshal Service et le renforcement des portes de cockpit. La Federal Aviation Administration (FAA) renforce parallèlement les exigences de résistance du poste de pilotage aux intrusions.<sup>4 5</sup>

- L'Europe suit une logique différente, mais convergente.

Après le 11-Septembre, elle transforme un ensemble de pratiques nationales en normes communes. Le premier cadre communautaire date de 2002 ; le règlement (CE) n° 300/2008 consolide ensuite les règles communes de sûreté et leur contrôle. Il couvre notamment le filtrage des passagers et bagages, la sûreté aéroportuaire, les contrôles des aéronefs, du fret, du courrier, des approvisionnements de bord et d'aéroport, ainsi que le recrutement et la formation des personnels<sup>6</sup>.

Ces mesures ont profondément accru la difficulté d'une attaque classique. Mais leur succès déplace aussi la question : que se passe-t-il lorsque l'auteur potentiel n'a pas besoin de forcer l'accès parce que le système lui a accordé cet accès légal ?

## Flydubai et l'hypothèse iranienne – Conserver la question sans fabriquer la réponse

L'incident intervient dans une séquence géopolitique qui appelle un examen méthodique des hypothèses.

- Le 23 septembre 2026, plusieurs pays de la région ont suspendu des vols iraniens dans le contexte du durcissement des sanctions américaines visant l'aviation iranienne.
- Selon les informations rapportées par Reuters, le même jour, Mohsen Rezaei, secrétaire du Conseil suprême de sécurité nationale iranien, a publiquement averti les pays

---

4. FAA, AC 25.795-1A, Flight Deck Intrusion Resistance, 24 oct. 2008 ; elle remplace la circulaire initiale de janvier 2002.

5. TSA, historique 2001–2006 : ATSA (nov. 2001), fédéralisation du filtrage, 100 % des bagages de soute, Air Marshals et cockpit renforcé.

6. Commission européenne, Aviation Security ; règlement (CE) n° 300/2008, succédant au cadre commun instauré par le règlement n° 2320/2002.

---

voisins des conséquences de leur participation aux restrictions américaines et évoqué la possibilité de perturber le fonctionnement de leurs aéroports.<sup>7</sup>

- Quelques jours plus tard, l'incident touche un appareil d'une compagnie émiratie reliant Dubaï à Tel-Aviv. Cette succession peut conduire à formuler une hypothèse de travail, mais elle ne suffit pas à établir une attribution.

La proximité temporelle, la nationalité de la compagnie, la destination israélienne et les déclarations iraniennes constituent des éléments circonstanciels ; ils ne démontrent ni commandement, ni facilitation, ni même motivation politique de l'auteur présumé.

La bonne méthode consiste donc à maintenir plusieurs hypothèses concurrentes : acte individuel sans motivation politique ; radicalisation individuelle ; action inspirée par un groupe ; action organisée avec des complices ; enfin, action facilitée ou commanditée par un acteur extérieur. L'hypothèse iranienne appartient à cette dernière catégorie et exige, par définition, le niveau de preuve le plus élevé.

Cette prudence renforce plutôt qu'elle n'affaiblit l'analyse. Même si l'enquête excluait tout lien iranien et toute finalité terroriste, l'incident conserverait sa valeur pour l'analyse d'une vulnérabilité : une personne bénéficiant d'un accès légitime à une fonction critique peut potentiellement contourner des barrières physiques conçues principalement contre les acteurs extérieurs.

## De l'intrusion à l'infiltration – La menace interne concerne tout l'écosystème

L'amendement 17 de l'Annexe 17, adopté en 2019 et applicable en 2020, a renforcé les dispositions relatives à la menace interne : vérifications d'antécédents, évaluations de vulnérabilité, partage d'informations et filtrage des personnes autres que les passagers. Ces dispositions visent notamment les risques associés à des personnes bénéficiant d'un accès légitime aux zones de sûreté à accès réglementé.<sup>8</sup>

- Cette approche ne se limite nullement à la compagnie aérienne. Il s'étend à tout l'écosystème de l'aviation civile. Les pilotes et les personnels navigants commerciaux (PNC) en constituent une composante visible, mais la même logique concerne les personnels d'escale, de maintenance, de nettoyage, de restauration à bord, d'avitaillement, de manutention des bagages et du fret, les fournisseurs, les prestataires techniques, les opérateurs informatiques et, plus largement, toute personne dont la fonction ouvre un accès physique, informationnel ou numérique à une fonction critique de l'aviation civile.
- Trois mécanismes peuvent contribuer à la menace interne :
  1. L'infiltration consiste à faire entrer intentionnellement une personne dans cet écosystème.
  2. Le recrutement consiste à obtenir la coopération d'une personne qui s'y trouve déjà.
  3. La radicalisation ou le retournement peuvent conduire une personne disposant initialement d'un accès légitime à utiliser contre le système les privilèges que celui-ci lui a accordés.

---

7. Reuters, 23–25 sept. 2026 : suspensions de vols iraniens et avertissements de Mohsen Rezaei. Élément de contexte, non preuve d'un lien avec Flydubai.

8. OACI, Amendement 17 à l'Annexe 17 : adopté en 2019, applicable en 2020 ; renforcement des mesures contre la menace interne.

---

L'organisation hostile n'aurait alors plus nécessairement à « faire entrer un terroriste dans l'avion » ; elle pourrait chercher à faire entrer, ou à recruter, un acteur dans la chaîne qui rend possible l'accès à l'avion.

Le cadre européen illustre déjà cette extension du périmètre de sûreté. Le règlement (CE) n° 300/2008 impose des contrôles d'accès, prévoit des vérifications d'antécédents pour les personnes disposant d'un accès non escorté aux zones de sûreté et soumet les personnes autres que les passagers à des mesures d'inspection/filtrage. Il couvre également les fournitures destinées à l'aéroport et à l'aéronef, précisément parce que la sûreté d'un vol implique largement les chaînes logistiques extérieures au cockpit.<sup>9</sup>

Le problème devient alors celui de la confiance dans la durée. Le système aéronautique ne peut fonctionner sans accorder des droits d'accès. Un mécanicien doit intervenir sur l'appareil ; les personnels de restauration doivent y introduire des approvisionnements ; les agents de nettoyage doivent y pénétrer ; les bagagistes et les personnels de fret doivent intervenir dans des zones sensibles ; les pilotes doivent évidemment contrôler l'aéronef. La vulnérabilité potentielle est donc inséparable du fonctionnement normal.

La sûreté change ainsi de nature. Contrôler un passager est une opération ponctuelle ; apprécier dans le temps le risque associé à des milliers de personnes autorisées relève d'une logique de sécurité du personnel, de culture de sûreté, de supervision, de signalement et de réévaluation continue. Cette surveillance peut notamment s'appuyer sur les journaux d'accès physiques et numériques, les anomalies de comportement et les usages inhabituels de systèmes.<sup>10</sup>

## De la menace interne à la cybermenace — Protéger la chaîne de confiance numérique

La dernière évolution prolonge la précédente. Si l'acteur extérieur cherche à contourner le contrôle physique et si l'acteur interne exploite un accès professionnel légitime, la cybermenace ouvre la possibilité d'agir sur certaines fonctions de l'écosystème sans présence physique à bord.

Il convient toutefois d'éviter les représentations spectaculaires. Rien ne permet, jusqu'à présent, de présenter comme capacité terroriste établie la prise de contrôle intégrale, à distance et depuis Internet, d'un avion de ligne moderne. La cybermenace aéronautique est cependant réelle parce que l'aviation civile repose sur un ensemble toujours plus dense de systèmes interconnectés : exploitation des compagnies, maintenance, communications, navigation, gestion du trafic aérien, aéroports, bases de données, fournisseurs et chaînes logicielles.

L'OACI a déjà intégré cette évolution. L'Annexe 17 comporte la norme 4.9.1 et la pratique recommandée 4.9.2 relatives à la cybersécurité ; l'Organisation a développé une stratégie, un plan d'action et des documents de gestion du risque cyber pour l'ensemble du secteur aéronautique. Cette prise en compte institutionnelle souligne l'importance de la menace : la protection contre les actes d'intervention illicite n'est plus exclusivement une affaire de portiques, de badges et de portes.<sup>11</sup>

---

9. Règlement (CE) n° 300/2008 : accès, antécédents, personnels, fret, courrier, approvisionnements de bord et fournitures d'aéroport relèvent du dispositif commun.

10. OACI, Insider Threat Toolkit, 2022 : approche multicouche associant culture de sûreté, vérifications, contrôle des accès, supervision et surveillance.

11. OACI : Annexe 17, norme 4.9.1 et pratique recommandée 4.9.2 ; Cybersecurity Strategy, Action Plan et Doc 10213 Global Cyber Risk Considerations.

---

La menace interne et la cybermenace peuvent d'ailleurs se rejoindre. Une personne autorisée peut exploiter ses identifiants, introduire un équipement, détourner un accès distant ou faciliter l'action d'un acteur extérieur. Inversement, une compromission numérique peut exploiter la confiance accordée à un fournisseur, à un logiciel, à une mise à jour ou à une connexion considérée comme légitime.

La menace interne exploite donc la confiance accordée à une personne ; la cybermenace exploite la confiance accordée à un système, une identité numérique, un fournisseur ou une connexion. Dans les deux cas, l'attaquant ne cherche plus nécessairement à briser la barrière : il cherche à se présenter au système de contrôle sous la forme de ce que ce système a appris à accepter.

---

## **CONCLUSION — DE LA PROTECTION DE L'AVION À LA RÉSILIENCE DE L'ÉCOSYSTÈME AÉRONAUTIQUE**

L'incident de Flydubai restera peut-être un cas isolé. L'enquête peut encore conclure à une motivation individuelle, sans organisation terroriste, sans complicité extérieure et sans rapport avec les tensions entourant l'aviation iranienne. Une telle conclusion invaliderait certaines hypothèses appliquées au cas précis ; elle n'annulerait pas les vulnérabilités que ce cas permet d'interroger.

Depuis les grandes vagues de détournements, la sûreté aérienne s'est renforcée par couches successives. Le filtrage a répondu à l'introduction d'armes et d'explosifs ; la protection du cockpit a répondu au risque de prise de contrôle de l'appareil ; le contrôle des personnels et des zones réservées répond à la menace interne ; la cybersécurité répond désormais à l'interconnexion numérique croissante. Les États-Unis, l'Europe et l'OACI ont suivi des voies institutionnelles différentes, mais convergent vers une même logique : élargir progressivement ce qui doit être protégé.

Il serait donc erroné de parler d'échec de la sûreté aérienne. Son efficacité contre certaines menaces explique en partie l'intérêt que peuvent acquérir d'autres modes de contournement. La dynamique pourrait être résumée ainsi : intrusion, infiltration, pénétration numérique.

Le véritable changement de paradigme est peut-être ailleurs. Pendant plusieurs décennies, la sûreté a surtout cherché à protéger un objet : l'aéronef. Elle s'est efforcée de le faire en contrôlant ceux qui pouvaient l'approcher ou y entrer. Elle doit désormais protéger un système : l'écosystème aéronautique composé d'hommes, d'organisations, de prestataires, de chaînes logistiques, de données, de logiciels et de réseaux auxquels il est indispensable d'accorder des degrés variables de confiance. Le tableau ci-après résume cette évolution et les réponses apportées aux différentes menaces.

---

## Évolution des menaces et des mesures de sûreté

| Type de menace                                                    | Vulnérabilité recherchée                    | Réponse emblématique                                                    |
|-------------------------------------------------------------------|---------------------------------------------|-------------------------------------------------------------------------|
| Détournement classique (années 1960 à 1980)                       | Accès physique à bord                       | Filtrage des passagers et des bagages, contrôle des accès               |
| Utilisation de l'avion comme arme (à partir du 11 septembre 2001) | Prise de contrôle du cockpit                | Renforcement des portes du cockpit, TSA, agents de sûreté à bord        |
| Menace interne (risque interrogé par l'incident de Flydubai)      | Accès professionnel légitime                | Vérifications d'antécédents, filtrage des personnels, culture de sûreté |
| Cybermenace (risque actuel et évolutif)                           | Systèmes, données, fournisseurs, connexions | Cyberrésilience et protection des fonctions critiques                   |

La question stratégique soulevée par l'incident de Flydubai dépasse ainsi ce seul cas : comment protéger une activité mondiale dont le fonctionnement repose précisément sur des milliers d'accès légitimes, physiques et numériques ? C'est probablement autour de cette gestion de la confiance, davantage encore que du seul renforcement des barrières, que se jouera une part importante de l'évolution de la sûreté de l'aviation civile.

## À PROPOS DE L'AUTEUR



### ABDELHAK BASSOU

Abdelhak Bassou est Senior Fellow au Policy Center for the New South. Ancien préfet de police, il fut investi de plusieurs responsabilités au sein de la Direction Générale de la Sûreté Nationale Marocaine dont chef de la division de la police des frontières de 1978 à 1993 ; Directeur de l'Institut Royal de Police en 1998 ; Chef des Sûretés régionales (Er-Rachidia 1999-2003 et Sidi Kacem 2003-2005) et également Directeur Central des Renseignements Généraux de 2006 à 2009. Il a également participé aux travaux de plusieurs instances internationales dont le Conseil des Ministres arabes de l'intérieur de 1986 à 1992, où il a représenté la Direction Générale de la Sûreté nationale dans plusieurs réunions. Abdelhak Bassou est titulaire d'un Master en études politiques et internationales de la Faculté des sciences juridiques, économiques et social d'Agdal à Rabat sur un mémoire intitulé « L'Organisation Etat Islamique, naissance et futurs possibles ».

## À PROPOS DU POLICY CENTER FOR THE NEW SOUTH

Le Policy Center for the New South: Un bien public pour le renforcement des politiques publiques. Le Policy Center for the New South (PCNS) est un think tank marocain dont la mission est de contribuer à l'amélioration des politiques publiques, aussi bien économiques que sociales et internationales, qui concernent le Maroc et l'Afrique, parties intégrantes du Sud global.

Le PCNS défend le concept d'un « nouveau Sud » ouvert, responsable et entreprenant ; un Sud qui définit ses propres narratifs, ainsi que les cartes mentales autour des bassins de la Méditerranée et de l'Atlantique Sud, dans le cadre d'un rapport décomplexé avec le reste du monde. Le think tank se propose d'accompagner, par ses travaux, l'élaboration des politiques publiques en Afrique, et de donner la parole aux experts du Sud sur les évolutions géopolitiques qui les concernent. Ce positionnement, axé sur le dialogue et les partenariats, consiste à cultiver une expertise et une excellence africaines, à même de contribuer au diagnostic et aux solutions des défis africains.

Les opinions exprimées dans cette publication sont celles de l'auteur.

### Policy Center for the New South

Rabat Campus of Mohammed VI Polytechnic University,  
Rocade Rabat Salé - 11103  
Email : [contact@policycenter.ma](mailto:contact@policycenter.ma)  
Phone : +212 (0) 537 54 04 04  
Fax : +212 (0) 537 71 31 54



[www.policycenter.ma](http://www.policycenter.ma)

