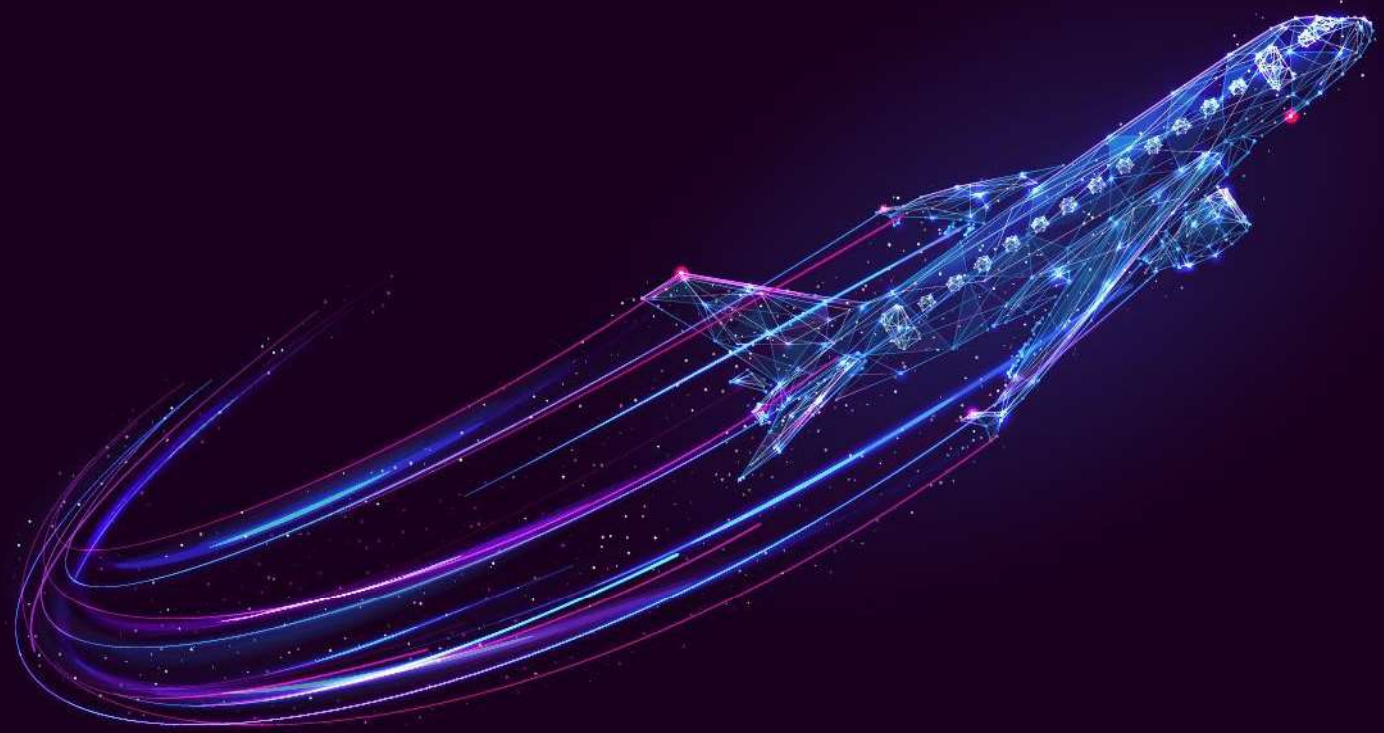


# Détermination du Besoin de Formation à la Cybersécurité pour les Pilotes

Rapport d'expérience



Juin 2023



**Cyber Israel**  
National Cyber Directorate



## Table des matières

<b>I. Introduction</b> .....	<b>3</b>
<b>II. Question de recherche</b> .....	<b>4</b>
A. Hypothèse et contre hypothèse .....	4
B. Compétences attendues .....	5-6
<b>III. Cadre de travail</b> .....	<b>7-8</b>
<b>IV. Description de l'expérience</b> .....	<b>9</b>
A. Détails techniques du vol .....	9
B. Evènements du vol .....	10
C. Cyberattaques simulées .....	11-15
D. Collecte de données .....	16
E. Méthodologie d'analyse de données .....	17-18
<b>V. Résultats</b> .....	<b>19</b>
A. Analyse des résultats par observation directe .....	19-21
B. Analyse des résultats selon la méthode des 3R .....	21-23
<b>VI. Débat</b> .....	<b>24</b>
A. L'efficacité de la formation à la cybersécurité pour les équipages d'avions .....	24
B. Faire face aux différents types de cyberattaques .....	24-25
C. Étendre la formation à la cybersécurité dans l'aviation .....	25
<b>VII. Conclusion</b> .....	<b>25</b>
<b>VIII. Auteurs</b> .....	<b>26</b>



## I. Introduction

Les avions de ligne modernes devenant de plus en plus numérisés et connectés, la surface des cyberattaques s'accroît en conséquence. Ce qui n'était autrefois qu'une menace futuriste est aujourd'hui une menace réelle. Les constructeurs, les exploitants et les autorités chargées de réglementation redoublent d'attention et d'investissements pour améliorer la cybersécurité des avions, mais aucun système n'est infaillible et aucune défense n'est incontournable. Les hackers utilisent eux aussi des techniques de plus en plus avancées et il faut donc partir du principe qu'une cyber-attaque sur un avion commercial n'est qu'une question de temps. Le moment venu, les pilotes pourraient se retrouver en dernière ligne de défense.

Dans son plan d'action pour la cybersécurité<sup>1</sup> l'OACI a demandé aux États membres et à l'industrie de définir des exigences appropriées en matière de formation à la cybersécurité dans l'aviation pour chaque fonction, à tous les niveaux de leur organisation (CyAP 7.2). Compte tenu du rôle clé que jouent les pilotes dans l'aviation, il est essentiel de les associer à cet effort. Plus précisément, les pilotes peuvent être confrontés à des cyberattaques qui se manifestent à bord de l'avion et peuvent entraîner un risque accru pour la sécurité, comme l'ont démontré des travaux antérieurs<sup>23</sup>. Cependant, comme l'ajout de tout type de formation pour les pilotes est un investissement conséquent pour les compagnies aériennes, il faut aborder ce concept de manière réfléchie et examiner attentivement l'efficacité de la formation à la cybersécurité pour les pilotes, ainsi que le type de formation qui serait le plus approprié.

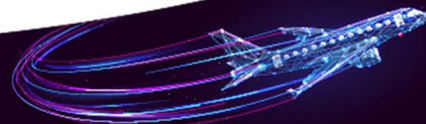
Ce rapport résume une expérience menée par les autorités de l'aviation civile d'Israël (CAAI) et de France (DGAC), la Direction nationale israélienne du cyberespace (INCD) et ASL Airlines France, visant à examiner la nécessité d'une formation à la cybersécurité pour les

---

<sup>1</sup> <https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.EN.pdf>

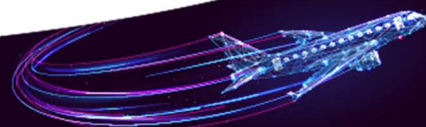
<sup>2</sup>Safety vs. Security: Attacking Avionic Systems with Humans in the Loop; Matthew Smith, Martin Strohmeier, Jon Harman, Vincent Lenders, and Ivan Martinovic; Department of Computer Science, University of Oxford; <https://arxiv.org/abs/1905.08039>

<sup>3</sup>Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior; Patrick Gontar, Hendrik Homans, Michelle Rostalski, Julia Behrend, Frédéric Dehais, Klaus Bengler; <https://www.sciencedirect.com/science/article/abs/pii/S0969699717300510>



## Détermination du besoin en formation à la cybersécurité pour les pilotes

pilotes. Elle a pour but d'apporter un éclairage supplémentaire sur ce sujet important, afin d'aider les parties prenantes de l'aviation dans leur processus de prise de décision en la matière.



## II. Question de Recherche

Dans le cadre de cette expérience, les organisations ayant participé ont cherché à répondre à la problématique suivante :

**Existe-t-il un écart de performance dans la manière dont les pilotes font face aux incidents de cybersécurité à bord de leur avion et, si oui, comment une formation préalable peut-elle contribuer à combler cet écart ?**

### A. Hypothèse et Contre-Hypothèse

**Hypothèse** : il est possible d'aider l'équipage à apporter des réponses appropriées aux cyberattaques par le biais d'une formation spécifique à la cybersécurité.

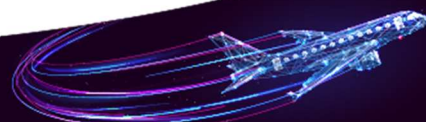
**Supposition** : le savoir-faire générique actuel et la formation des équipages sont insuffisants pour permettre une gestion adéquate des cyberattaques.

**Test de l'hypothèse** : deux groupes d'équipages (test et témoin) sont confrontés aux mêmes scénarios en vol qui incluent des cyber-attaques.

**Validation de l'hypothèse** : les équipes formées seraient plus à même d'adopter le comportement escompté que le groupe témoin, et seraient donc prêtes à faire face aux cyber-attaques.

#### **Contre-Hypothèse :**

- 1) Le savoir-faire dont disposent les équipages "standard" (compétences aériennes, compétences génériques en matière de CRM, de prise de décision, de conscience de la situation, etc.) leur permet de faire face aux cyber-attaques de manière satisfaisante
  - a. La performance dans la gestion des situations pourrait être la même face aux difficultés rencontrées par le groupe test et le groupe témoin
  - b. Les deux groupes ne présenteraient pas de différence significative dans les trois types de comportements recherchés (données quantitatives et qualitatives)
  - c. L'identification de l'origine malveillante sera faible ou inexistante pour le groupe test
- 2) La formation dispensée n'améliore pas de manière notable les performances du groupe test



## B. Compétences Attendues

Les compétences résultent des interactions entre : (i) connaissances, (ii) des séquences d'action routinières et (iii) des cadres d'activités spécifiques. Les compétences sont développées par la formation et l'expérience.

L'hypothèse proposée suppose que les compétences acquises par un équipage pourraient être améliorées pour faire face aux cyber-attaques si la sensibilisation à la cybersécurité est assurée par une formation sur ordinateur dispensée à l'équipage.

Les contre-hypothèses supposent respectivement que :

1) Les compétences générales seraient suffisantes pour détecter, identifier et élaborer une réponse appropriée à une cyber-attaque. Les réponses des deux groupes seraient alors équivalentes avec un haut niveau d'efficacité. Les composantes des compétences déjà acquises seraient transposées à la situation de cyberattaque (connaissances, routines et cadre spécifique).

2) La formation dispensée n'est pas suffisante pour améliorer les compétences du groupe test, et un niveau de compétences aussi faible serait observé pour les deux groupes. Nous devons garder à l'esprit qu'il peut s'agir d'un manque de connaissances, de routines inappropriées ou d'un cadre d'activité spécifique mal identifié.

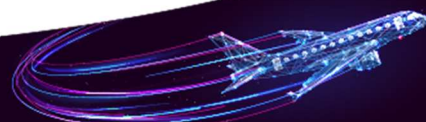
Les comportements sont évalués en fonction des trois étapes suivantes (modèle de « sensemaking ») :

- 1) Détection d'une attaque
- 2) Identification de la nature et des conséquences de l'attaque
- 3) Élaboration d'une stratégie d'adaptation et d'un processus décisionnel

Leur degré d'adaptation aura pour objectif la collecte des données suivantes :

- Quantitative pour chaque étape : temps de réaction, temps de mise en œuvre, origine et nombre de prises de parole, etc.
- Qualitative : précision et clarté des descriptions de chacune des étapes, consensus au sein de l'équipe, efficacité et suivi des actions, etc.

Il convient de noter que le protocole et le nombre de pilotes disponibles pour l'étude ne permettent pas d'atteindre un degré élevé de statistiques significatives. Par conséquent, ce document présente une expérience qualitative plutôt que quantitative. Néanmoins, l'objectif

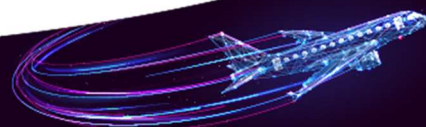


## Détermination du besoin en formation à la cybersécurité pour les pilotes

reste de réaliser une étude "propre", robuste et donc opposable à d'autres données possibles.

Cet objectif sera atteint si plusieurs critères de robustesse sont satisfaits :

- Utilisation d'une approche "empirique" (vérification "structurée" de modèles comportementaux connus). Les tendances et les effets observés confirmeront ces modèles et fonderont les conclusions et les comparaisons avec d'autres travaux réalisés ou études à venir.
- Répétabilité du scénario (traçabilité, transparence, exhaustivité des explications).
- Pertinence et validité des données collectées et de leur traitement.



### III. Cadre de travail

Cette étude vise à tester l'utilité d'une formation dédiée à la cybersécurité pour les équipages d'avions.

Deux types de formation ont été envisagés à l'origine :

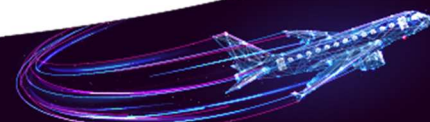
1. Formation théorique (en classe ou sur ordinateur)
2. Formation sur simulateur

En raison de contraintes pratiques, la formation s'est finalement limitée à **un module d'apprentissage sur ordinateur sur la cybersécurité, qui a fait l'objet d'une autoévaluation.**

L'expérience a porté sur huit équipages de deux pilotes chacun (seize au total). Les équipages participants ont été amenés à effectuer une séance de simulateur standard pour des motifs non divulgués, c'est-à-dire qu'ils ne savaient pas qu'ils participaient à une expérience ayant un rapport à la cybersécurité. Le simulateur utilisé était le simulateur Boeing 737-800 d'ASL au centre de formation SIMAERO près de l'aéroport Charles de Gaulle (CDG). Il convient de souligner que le choix du simulateur s'est fait en fonction de sa disponibilité et qu'il ne faut pas en déduire que les scénarios simulés sont effectivement pertinents pour le modèle d'avion en question.



Les participants ont été divisés (à leur insu) en deux groupes : un groupe test et un groupe témoin. En raison de contraintes pratiques, il n'a pas été possible de fournir une formation préalable sur simulateur au groupe test, mais seulement un dossier d'auto-apprentissage sur ordinateur. Au cours de la séance d'information, les deux groupes ont reçu des dossiers d'apprentissage sur ordinateur - le groupe témoin a reçu un dossier sur le "Programme d'amélioration du système de rudder" (RSEP) - un sujet utilisé pour "dissimuler" la véritable



## Détermination du besoin en formation à la cybersécurité pour les pilotes

nature de l'expérience ; le groupe test a reçu le même dossier RSEP, mais en plus un dossier sur les "Menaces de cybersécurité pour les avions modernes".

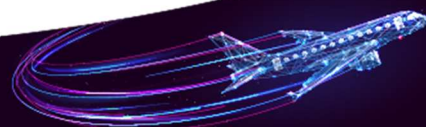
Groupe test



Groupe témoin



Toutes les autres conditions étaient similaires à une séance de simulateur régulière à laquelle les équipages sont habitués, y compris la documentation de vol et le briefing, conformément aux données et pratiques disponibles. Les séances expérimentales étaient familières aux pilotes de l'équipe ASL.



## IV. Description de l'Expérience

### A. Détails Techniques du Vol

Séance en mode LOFT de l'aéroport de Lyon-Saint-Exupéry (LYS) à l'aéroport de Bergame (BGY).

Vol cargo sur B737-800BCF : F-HIQB (RNP baroVNAV).

Commandant de Bord : Pilot Monitoring (PM), Officier Pilote de Ligne : Pilote en Fonction (PF)

Conditions météorologiques : Piste 17R au départ, vent 220° 8 kt, visibilité 4000 m, nuages fragmentés 1200 ft, température 22 °C, point de rosée 7 °C, QNH 1016 hPa, piste mouillée.

Un dossier d'information est disponible pour la préparation du vol (ASL - 19 pages - PDF)

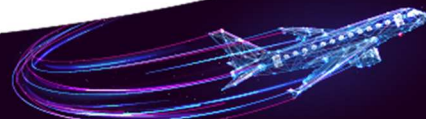
Line Training LYS BGY avec déroutement possible à Milan

22° 220/08KT 1016

Calcul des performances : Poussée moteur - 24K, Volets 5°, Température fictive 35 °C, N1 93.3%, V1 129 kt, Vr 137 kt, V2 143 kt.

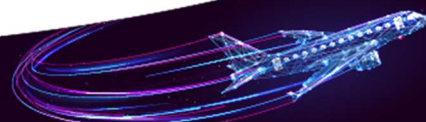
F-HIQB	Poids (kg)
Charge	18200
Masse zéro carburant	57652
Bloc carburant	5400
Roulage	200
Masse au décollage	62852

ATIS LFLL	F-HIQB
T/O RWY 17R- A4 due to work	Parking stand (Ramp)
220/08 4000 BKN012 22/07 1016 WET	Block Fuel 5400 kg



## B. Evènements du Vol

Temps	Rang	Vol cargo FPO123	Attaque Num.	Nature
-20 min	1	BRIEFING DEPART – C/L AVANT ROULAGE ET AVANT DECOLLAGE		
0h00	2	Décollage RWY 17R A4 SID RISOR 2S FL70		
6 min	3	Montée à FL290 STANDBY RUDDER ON		Dysfonctionnement "fictif" en lien avec l'apprentissage sur ordinateur du RSEP
12 min	4	CRZ ATC : « Confirmez stable au FL290 ? »	#1	Piratage ADS-B
22 min	5	ACARS MESSAGE AVEC FAUX ZFW = 52 880 KG	#2	Feuille de chargement falsifiée via ACARS
	6	Descente - STAR DIXER 3E – ITVUN – TIXUM, ILS hors service, pas de secours électrique		
32 min	7	DESCENT - STAR DIXER 3E – ITVUN – TIXUM Augmentation des jaugeurs carburant de 200 kg/min	#3	Donnée de la consommation de carburant piratée
46 min	8	RNP Y 28 GPS POSITION DRIFT FAST 5 NM AVANT TIXUM APPROACHING ME541 « CONFIRM ESTABLISHED ON FINAL RNP 28 ? »	#4	GPS Piraté
52 min	9	APPROCHE INTERROMPUE 4 000 FT DYSFONCTIONNEMENT GPS ANNULE 10 km B2000		
70 min	10	GUIDAGE RADAR POUR APPROCHE A VUE 28 ALERTE EGPWS ERRONEE A 1 700 FT	#5	Alerte GPS erronée
	11	ATTERRISSAGE		



## C. Cyberattaques Simulées

Les cinq cyberattaques simulées dans le cadre de l'expérience ont été choisies pour un ensemble de raisons liées à l'objectif de l'expérience, qui était de tester le facteur humain et l'efficacité de la formation à la cybersécurité pour les équipages d'avions. L'objectif n'était pas technique et il n'y avait donc aucune intention de "prouver" la validité technique de ces attaques dans le cadre de cette étude, ni leur pertinence par rapport au modèle d'avion utilisé dans le simulateur.

Les critères utilisés pour le choix des scénarios sont les suivants :

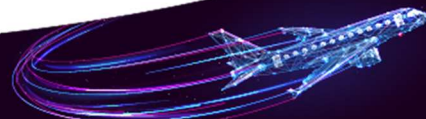
1. **Attaques détectables** – les attaques pouvant être potentiellement détectables par les équipages. Une attaque totalement dissimulée et qui ne se manifeste d'aucune manière dans l'avion n'est pas pertinente pour la réponse du pilote soumis à l'essai.
2. **Attaques exploitables** – les attaques pour lesquelles les actions des pilotes sont pertinentes. Une attaque pour laquelle les actions des pilotes n'ont aucun effet n'est pas pertinente pour cette expérience.
3. **Différence avec les dysfonctionnements** – les attaques qui ne se manifestent pas comme des dysfonctionnements standards pour lesquels l'équipage se contenterait d'exécuter une check-list existante.
4. **Attaques "raisonnables"** – nous n'avons pas choisi de scénarios extrêmement spectaculaires ou irréalistes (par exemple, l'arrêt d'un moteur ou la prise en charge des commandes de vol). Comme nous l'avons déjà mentionné, l'objectif de l'étude n'était pas de prouver à quel point ces attaques sont difficiles ou faciles à réaliser, c'est pourquoi nous avons choisi de rester dans des limites "crédibles".

### 1. Attaque n° 1 – Usurpation du signal ADS-B

**Description** : pendant la phase de croisière, un attaquant diffuse un faux signal ADS-B au contrôleur au sol de sorte que ce dernier voit l'avion comme s'il était à une altitude incorrecte (le contrôleur voit l'avion comme s'il volait à 28 500 pieds, alors qu'il vole en réalité à 29 000 pieds, comme demandé). Une fois que l'équipage change de fréquence pour passer au contrôleur au sol suivant, le problème est résolu car l'usurpation d'identité vise localement le premier contrôleur.

---

<sup>4</sup>Thabet Kacem, Duminda Wijesekera, Paulo Costa, and Alexandre Barreto. "An ADS-B Intrusion Detection System. In: *2016 IEEE Trustcom/BigDataSE/ISPA*. 2016, pp.544-551. DOI:10.1109/TrustCom.2016.0108.



**Raison d'être** : ce scénario tient compte du fait que le protocole ADS-B n'est pas sécurisé (non crypté, non authentifié) et peut donc être relativement facilement usurpé<sup>45678</sup>. L'objectif de l'attaquant est de perturber les opérations en créant une confusion entre les avions et l'ATC, et éventuellement d'essayer de faire voler l'avion à une altitude erronée.

**Méthode de simulation** : le contrôleur signale "Steady FL290, ATC reads 285, check altimeter setting" (FL290 stable, ATC indique 285, vérifier le calage altimétrique).

**Actions potentielles du pilote :**

1. Se fier aux indications de l'avion
2. Vérification croisée des trois altimètres
3. Dialoguer avec le contrôleur
4. Assurer la sécurité - déclarer "Unable RVSM" et demander la descente au FL280 [RVSM - Reduced Vertical Separation Minimum - permet de réduire la séparation verticale au-dessus du niveau de vol 290 de 2000 pieds minimum à 1000 pieds minimum].
5. Problème ADS-B suspecté / spoofing (peu probable)

## 2. Attaque n° 2 – Faux message ACARS avec fausse mise à jour de la feuille de chargement

**Description** : pendant la phase de croisière, un message ACARS est reçu indiquant que la masse sans carburant fournie lors de l'expédition (57652 kg) était erronée, et qu'une nouvelle valeur ZFW (52880 kg) doit être introduite dans les systèmes de l'avion. Il convient de noter que la valeur initiale est plus sûre car elle impose des marges de sécurité sur les vitesses plus importantes.

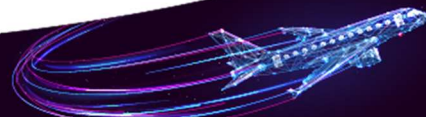
---

<sup>5</sup>Xuhang Ying, Joanna Mazer, Giuseppe Bernieri, Mauro Conti, Linda Bushnell, and Radha Poovendran. *Detecting ADS-B Spoofing Attacks using Deep Neural Networks*. 2019. arXiv: 1904.09969 [cs.CR].

<sup>6</sup>Andrei Gurtov, Tatiana Polishchuk, and Max Wernberg. "Controller-Pilot Data Link Communication Security". In: *Sensors* 18.5 (2018). ISSN: 1424-8220. DOI: 10.3390/s18051636. URL <https://www.mdpi.com/1424-8220/18/5/1636>

<sup>7</sup>Sofie Eskilsson, Hanna Gustafsson, Suleman Khan, and Andrei Gurtov. "Demonstrating ADS-B AND CPDLC Attacks with Software-Defined Radio". In: *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*. 2020, 1B2-1-1B2-9. DOI: /10.1109/ICNS50378.2020.9222945

<sup>8</sup>Gustav Lindahl and Anton Blaberg. *Simulating ADS-B attacks in air traffic management :By the help of an ATM simulator*. 2020



**Raison d'être :** Le protocole ACARS n'est ni crypté ni authentifié. Des recherches antérieures ont déjà montré que de faux messages ACARS pouvaient cibler des avions commerciaux<sup>91011</sup>. L'attaquant tente de créer un risque pour la sécurité (à savoir un touché de queue -tailstrike- à l'atterrissage ou un décrochage au cours de l'approche) en amenant les équipages à accepter une feuille de chargement falsifiée avec un poids erroné.

**Méthode de simulation :** le "message ACARS" suivant est remis aux pilotes :

```
RA 0540Z
DSP MSG CDGFP50
FROM DISPATCH.
DUE TO ERROR: NEW ZFW 52880
```

**Actions potentielles du pilote :**

1. Ne pas suspecter le message ACARS reçu et changer la ZFW
2. Essayer de contacter le Dispatch par ACARS ou par radio pour obtenir une confirmation
3. Sans confirmation, l'équipage décide de conserver la ZFW initiale, qui est une valeur sûre
4. Contrôler attentivement les données de vol
5. Signaler l'événement après l'atterrissage

### 3. Attaque n° 3 – Valeur du carburant erronée

**Description :** pendant la phase de descente, la quantité de carburant de l'avion est augmentée. Le carburant est augmenté de 200 kg par minute jusqu'à +400 kg dans chaque réservoir d'aile .

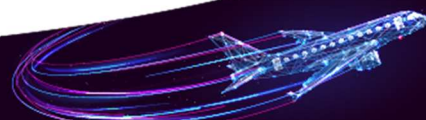
**Raison d'être :** il s'agit sans doute de l'attaque la plus improbable, car elle est à la fois difficile à exécuter (il faut pénétrer dans le système de l'avion) et n'a qu'un effet limité pour l'attaquant. Cependant, nous avons voulu tester un événement qui sort des procédures normales et ne fait pas l'objet d'une check-list préétablie (contrairement à la diminution de

---

<sup>9</sup>Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. "Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS". In: *Financial Cryptography and Data Security (FC 2017)*, 21<sup>st</sup> International Conference. April 2017. URL: [file:///b3-vsrv-ctxfs01/Downloads/Tamirg/Downloads/Economy\\_Class\\_Crypto\\_FC17.pdf](file:///b3-vsrv-ctxfs01/Downloads/Tamirg/Downloads/Economy_Class_Crypto_FC17.pdf)

<sup>10</sup>M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic. "On the Security and Privacy of ACARS". In: *Integrated Communications Navigation and Surveillance Conference (ICNS)*. IEEE, Herndon, 2016.

<sup>11</sup>P. E. Storck. "Benefits of Commercial Data Link Security". In: *Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE, Herndon, 2013.



carburant qui peut résulter d'une fuite de carburant). Du point de vue de l'attaquant, cette attaque vise à créer une surprise pour l'équipage à un moment délicat du vol. Une augmentation de la charge de travail est attendue. Si elle est combinée à une autre attaque entraînant un déroutement vers un aéroport de dégivrage, elle peut conduire les pilotes à se reposer sur un excès de carburant qu'ils n'ont pas vraiment.

**Méthode de simulation** : le simulateur permet de modifier les quantités de carburant de l'avion en cours de vol.

**Actions potentielles du pilote :**

1. Remarquer une quantité excessive de carburant peu après le début de l'attaque
2. Remarquer la quantité excessive de carburant dans le cadre de la procédure de remise des gaz suivant l'attaque n° 4
3. Ne jamais remarquer un excès de carburant
4. Après avoir constaté un excès de carburant, accepter cette quantité comme carburant disponible
5. Après avoir constaté un excès de carburant, soupçonner une erreur de l'indication de la quantité de carburant
6. Signaler l'événement après l'atterrissage

#### 4. Attaque n° 4 – Piratage du GPS

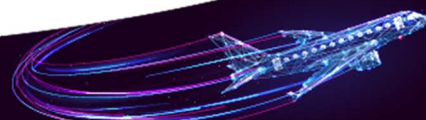
**Description** : pendant l'approche RNAV, le GPS est altéré à une vitesse d'environ 0,05 NM/minute (environ 100 mètres par minute). Il faut environ 5 minutes pour dépasser la performance de navigation réelle (ANP) de 0,3, qui est requise pour l'approche RNP. Cette vitesse est suffisamment lente pour que l'équipage ne la détecte pas jusqu'à ce qu'une alerte se produise.

**Raison d'être** : le piratage du GPS est un risque connu<sup>12131415</sup>. Un pirate peut utiliser le piratage du GPS pour tenter de créer un risque pour la sécurité en faisant atterrir l'avion dans un obstacle ou avant la piste, en particulier dans des conditions météorologiques de vol aux instruments (IMC).

**Méthode de simulation** : le simulateur permet l'usurpation d'identité GPS. Après avoir passé le FAF, la tour demande : "Confirm established on final APP RNP 28 ?" La valeur ANP augmente pendant l'approche et finalement les messages d'alerte "Terrain Position" et "Unable Required Navigation Performance" apparaissent .

---

<sup>12</sup>Berz, G. 2018. GNSS spoofing and aviation: an evolving relationship. Inside: *GNSS*, 25 September [online]. Available at: <https://insidegnss.com/gnssspoofing-and-aviation-an-evolving-relationship>.



Remarque : "Terrain position" est une alerte liée au système EGPWS qui utilise un récepteur GPS différent de celui du système de navigation. Cette alerte ne fait pas partie de la procédure de remise de gaz. "UNABLE REQD NAV PERF-RNP" est un avertissement du système de navigation qui justifie une procédure d'approche interrompue.

**Actions potentielles du pilote :**

1. Interrompre l'approche
2. Demander un guidage radar
3. Demander une approche ILS (réponse : aucun ILS n'est disponible)
4. Demander une nouvelle tentative d'approche RNP de la même piste sous guidage radar ou LNAV
5. Demande de RNP 10 ou de VOR 10 sous guidage radar ou LNAV
6. Demande de déroutement vers un autre terrain
7. Vérifier les systèmes de l'avion
8. Suspicion de brouillage ou piratage du GPS
9. Demander à l'ATC s'il y a eu d'autres rapports sur des problèmes de GPS (réponse : oui, un rapport il y a 10 minutes).

## 5. Attaque n° 5 - fausse alerte EGPWS

**Description** : après l'attaque n°4, les conditions météorologiques s'améliorent et permettent une approche à vue. Au cours de l'étape finale de l'approche, à 1700 ft QNH, une fausse alerte EGPWS "Terrain Pull up" est déclenchée, résultant de l'altération du GPS. À ce moment-là, l'équipage a un contact visuel avec la piste .

**Raison d'être**: l'une des conséquences du piratage ou du brouillage du GPS peut être de fausses alertes EGPWS. De telles alertes ont été constatées lors d'incidents réels dans des zones de brouillage du GPS.

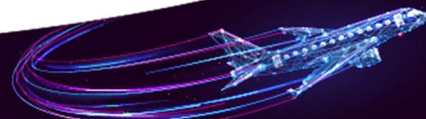
**Méthode de simulation** : le simulateur permet de déclencher ces alertes à des moments précis.

---

<sup>13</sup>Morales-Ferre, R., Richter, P., Falletti, E., de la Fuente, A. & Lohan, E.S. "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft". In: *IEEE Communications Surveys&Tutorials*,22(1), pp.249-291. Available at: <https://doi.org/10.1109/COMST.2019.2949178>.

<sup>14</sup>Nicola, M., Falco, G., Morales-Ferre, R., Lohan, E-S., Fuente, A. de la& Falletti. "Collaborative solutions for interference management in GNSS based aircraft navigation". In: *Sensors*, 20(15), pp.4085-4108 Available at: <https://doi.org/10.3390/s20154085>.

<sup>15</sup>Steindl, E., Dunkel, W., Hornbostel, A., Haettich, C. & Remi, P. "The impact of interference caused by GPS repeaters on GNSS receivers and services". In: European Navigation Conference (ENC) GNSS 2013, April 22-25 [online]. Available at: <https://elib.dlr.de/84739>



**Actions potentielles du pilote :**

1. Interrompre l'approche
2. Vol à vue, l'équipage ne tient pas compte de l'alarme
3. Communication entre PF et PM
4. Après le piratage du GPS, l'équipage peut faire le lien entre l'alerte EGPWS et les interférences GPS

## **D. Collecte de Données**

Les données de l'expérience ont été collectées de la manière suivante :

### **1. Enregistrement vidéo**

Utilisé pour enregistrer des données brutes sur :

- communication à bord et vers le sol
- actions de l'équipage
- les durées entre les entrées et les réponses de l'équipage
- synchronisation générale des comportements (verbal, geste, action, temps)

Ces données brutes permettent une analyse immédiate et différée du comportement de l'équipage.

### **2. Grilles d'Observation**

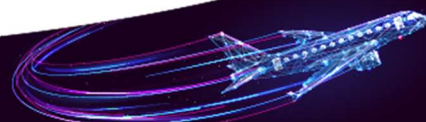
Deux grilles d'observation ont été utilisées :

- Une grille "Technique" pour recueillir des observations sur les comportements techniques
- Une grille "Attitude" pour collecter des données relatives aux compétences non techniques

### **3. Debriefing Individuel "à chaud"**

Un questionnaire personnel d'une durée de 10 minutes, fourni immédiatement après le vol en simulateur, était à remplir individuellement par chaque pilote. Le questionnaire comprenait:

- Une courte série de questions sur leur expérience en tant que pilote
- Questions concernant le vol (sans mention de la possibilité d'une cyber-attaque)



#### 4. Debriefing "à froid"

Un entretien basé sur la "méthode des 3R" - une méthode destinée à analyser le comportement de l'équipage face à des événements imprévus :

R1 – Readiness/Préparation

R2 – Recognition/Reconnaissance

R3 - Reaction/Réaction

Les comportements des équipages ont été codés pour chaque attaque selon R1, R2 et R3.

#### 5. Enquête Post-Expérience

Après la fin de l'expérience, une enquête a été envoyée à tous les équipages pour connaître leur nouvelle perception des cyber-risques. Sur les 16 pilotes ayant participé à l'expérience, 12 réponses ont été obtenues.

### E. Méthodologie d'Analyse des Données

Les données ont été analysées sur la base de la méthode de formation et d'évaluation basées sur les compétences (CBTA).

Guidance Material CBTA IATA - 21/01:

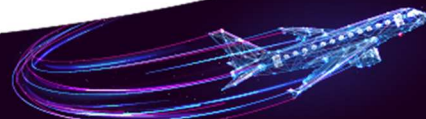
<https://www.iata.org/contentassets/c0f61fc821dc4f62bb6441d7abedb076/competency-assessment-and-evaluation-for-pilots-instructors-and-evaluators-gm.pdf>

#### 1. Définition de la Compétence

**Compétence** : une dimension de la performance humaine utilisée pour prédire de manière fiable la réussite au travail. Une compétence se manifeste et s'observe par des comportements qui mobilisent les connaissances, les aptitudes et les attitudes pertinentes pour mener à bien des activités ou des tâches dans des conditions spécifiques.

L'OACI décrit les connaissances, les compétences et l'attitude comme suit :

- Les connaissances sont des informations spécifiques nécessaires pour permettre à celui qui apprend de développer et d'appliquer les compétences et les attitudes nécessaires pour se rappeler des faits, identifier des concepts, appliquer des règles ou des principes, résoudre des problèmes et penser de manière créative dans le contexte du travail.



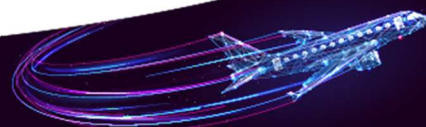
- Une compétence est une capacité à réaliser une activité ou une action. Elle est souvent divisée en trois types : les compétences motrices, cognitives et métacognitives.
- L'attitude est un état mental interne persistant ou une disposition qui influence le choix d'une action personnelle d'un individu à l'égard d'un objet, d'une personne ou d'un événement, et qui peut être apprise. Les attitudes ont des composantes affectives, des aspects cognitifs et des conséquences comportementales. Pour adopter la "bonne" attitude, celui qui apprend doit "savoir être" dans un contexte donné.

## 2. Liste de Compétences

Liste des compétences des pilotes CBTA dans les documents d'orientation de l'IATA :

- 0 – Application des connaissances
- 1 – Application des procédures et respect de la réglementation
- 2 – Communication
- 3 – Gestion des trajectoires de vol des avions – pilotage aux automatismes
- 4 – Gestion des trajectoires de vol des avions – pilotage manuel
- 5 – Leadership et travail d'équipe
- 6 – Résolution de problèmes et prise de décision
- 7 – Conscience de la situation et gestion de l'information
- 8 – Gestion de la charge de travail

Chacune de ces compétences est identifiée à l'aide de comportements observables (CO). Elles sont énumérées dans les documents d'orientation de l'IATA.



## V. Résultats

Comme indiqué dans la section II, cette expérience a été mise en place pour répondre à la question suivante :

**Existe-t-il un écart de performance dans la manière dont les pilotes font face aux incidents de cybersécurité à bord de leur avion et, si oui, comment la formation préalable peut-elle contribuer à combler cet écart ?**

Les résultats ont été analysés sous deux angles complémentaires à l'aide de deux méthodes :

A. Analyse des résultats par observation directe

B. Analyse des résultats à l'aide de la "méthode des 3R" - une méthode systématique d'analyse des rapports sur la sécurité aérienne

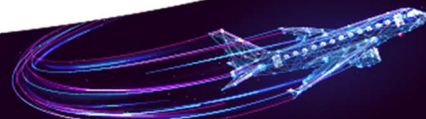
### A. Analyse des Résultats par Observation Directe

L'étude a mis en évidence trois points remarquables :

#### 1. Premier résultat : une faible sensibilisation à la cybersécurité de la part de tous les équipages

À l'exception d'une seule mention de la cybersécurité par l'un des "équipages formés", aucun des huit équipages n'a compris qu'il était confronté à une série de cyberattaques. Cela est vrai à la fois pendant le vol et après le vol, car aucun des équipages n'a jamais mentionné une cyberattaque comme cause possible lors des débriefings. En d'autres termes, aucun des équipages n'avait imaginé qu'un vol commercial puisse faire l'objet de ce type d'attaque, et les stratégies appliquées pour poursuivre le vol en toute sécurité ont été choisies sans identifier la menace.

Ceci est particulièrement remarquable pour le groupe test (les "équipages formés"), car ces pilotes ont reçu un dossier d'apprentissage numérique sur les cybermenaces potentielles pesant sur les avions juste avant de monter à bord du simulateur. Il convient toutefois de noter que les équipages ont parcouru le dossier d'apprentissage numérique de leur propre chef, sans recevoir d'accompagnement d'aucune sorte. Par conséquent, le manque de sensibilisation aux cybermenaces peut être largement attribué au type de formation qui



semble ne pas avoir eu d'impact significatif sur les équipages (contrairement, par exemple, à la formation sur simulateur elle-même, comme le montre le point 3 ci-dessous).

## 2. Deuxième résultat : la sécurité des vols n'a jamais été compromise

La deuxième observation remarquable est qu'aucun des huit équipages n'a été mis en difficulté et que la sécurité du vol n'a jamais été compromise. Bien que, comme indiqué à la section IV.C, les cyberattaques aient été choisies en partie parce qu'elles étaient "raisonnables" et non extrêmes, de faibles niveaux de performance ou de vigilance auraient quand même pu entraîner un risque accru pour la sécurité.

Par exemple, dans le cas de l'attaque n°1 consistant à transmettre un niveau de vol erroné à l'ATC (les 3 relevés altimétriques étaient tous cohérents entre eux), les équipages ont douté de leur altitude réelle lorsque l'ATC a indiqué qu'il les voyait à une altitude différente. Certains ont contacté le secteur ATM suivant, d'autres ont essayé de vérifier ou de poser des questions. En d'autres termes, à aucun moment ils ne se sont isolés du reste des opérations, ce qui a contribué à une analyse pertinente de la situation.

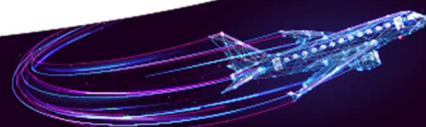
Pour toutes les attaques, la stratégie des huit équipages a toujours été d'impliquer tous les acteurs liés au vol, en particulier l'ATC, pour comprendre la situation, recouper les informations et lever leurs doutes. Enfin, ils ont tous évalué correctement la situation avec les informations disponibles et ont mentionné les alternatives possibles à la suite de cette analyse.

## 3. Troisième résultat : la formation sur simulateur a permis d'accroître la sensibilisation aux cybermenaces

Après la fin de l'expérience, une enquête a été envoyée à tous les équipages pour connaître leur nouvelle perception des cyber-risques. Sur les 16 pilotes qui ont participé à l'expérience, 12 réponses ont été obtenues. Ces réponses démontrent que l'expérience a permis de sensibiliser les équipages aux cybermenaces.

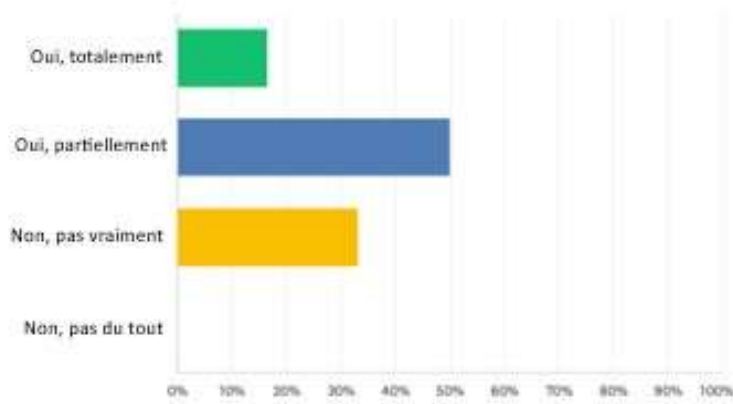
a) Deux tiers des équipages reconnaissent qu'ils sont désormais plus conscients des effets des cyberattaques sur la sécurité des vols. C'est également ce qui ressort des comptes rendus de vol (à chaud et à froid).

b) Plus de 90 % des pilotes interrogés déclarent être désormais plus conscients de la nécessité de signaler d'éventuels cyber-événements.



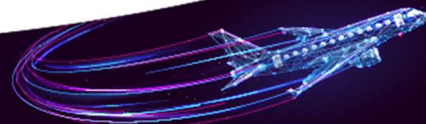
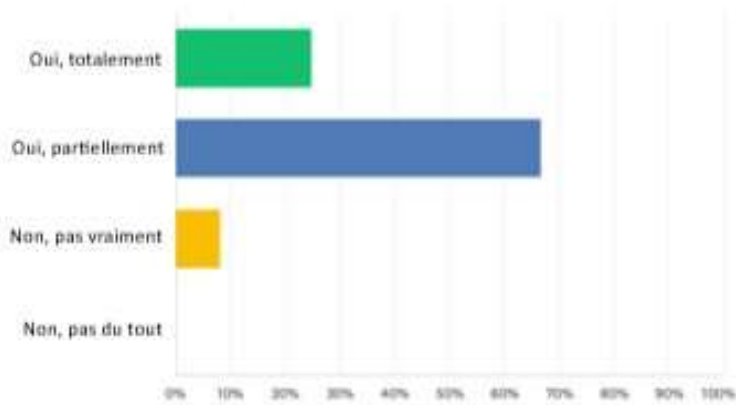
**Q6** En conclusion de cette expérience, vous sentez mieux armé que vos collègues pour comprendre et/ou pour faire face aux cyberattaques en vol ?

Réponses obtenues : 12 Question(s) ignorée(s) : 0



**Q7** Cette expérience vous encourage-t-elle à reporter plus souvent les événements dont vous êtes témoin ?

Réponses obtenues : 12 Question(s) ignorée(s) : 0



## B. Analyse des Résultats selon la Méthode des 3R

La grille d'analyse 3R a le mérite d'avoir été testée à grande échelle dans un autre contexte. Elle consiste à effectuer une analyse systématique d'un grand nombre de rapports de sécurité en posant successivement trois questions simples sur un événement survenu en vol :

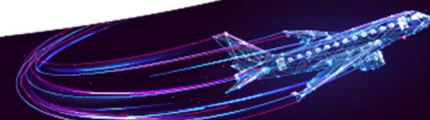
- A. "L'équipage était-il prêt ?" = Readiness/Préparation
- B. "A-t-il identifié le problème ?" = Recognition/Reconnaissance
- C. "A-t-il mis en œuvre la bonne réaction ?" = Reaction/Réaction

Les réponses respectives à ces trois questions sont établies à l'aide de 4 critères.

Nous avons d'abord essayé de faire la moyenne des résultats des 5 types de cyberattaques. Cependant, malgré des scores significativement différents, la petite taille de l'échantillon ne nous a pas permis d'identifier des différences liées au fait que les équipages aient reçu un briefing avant le vol sur les cybermenaces. De plus, cette analyse des résultats par la moyenne masque la diversité des types d'attaques, c'est pourquoi cette approche ne nous a pas semblé pertinente.

Nous avons donc analysé chaque attaque afin d'identifier les points remarquables en considérant la dispersion des résultats des réactions aux types d'attaques. C'est sur ce point que portera l'analyse des résultats, comme le montre l'analyse suivante selon la méthode des 3R.

	Attaque n°1	Attaque n°2	Attaque n°3	Attaque n°4	Atta5
	Falsification du signal ADS-B	Faux message ACARS	Valeur erronée du carburant	Espionnage du GPS	Faux avertissement EGPWS
<b>R1 – READINESS/PRÉPARATION</b>	O	O	O	O	O
<b>R1.1 - En forme pour le vol</b> (Pas fatigué, en bonne santé ?)	O	O	O	O	O
<b>R1.2 - Formé</b> (Compétence et actualité ?)	O	O	O	O	O
<b>R1.3 - Gestion de la charge de travail</b> (Capable de gérer toutes les situations habituelles ?)	O	O	O	O	O
<b>R1.4 – Engagé</b> (Impliqué et actif ?)	O	O	O	O	O
<b>R2 – RECOGNITION/RECONNAISSANCE</b>	O	O	N	O	O
<b>R2.1 – Détection</b> (Problème constaté ?)	O	O	N	O	O
<b>R2.2 - Identification</b> (Diagnostic correct ?)	O	O	N	O	O



## Détermination du besoin en formation à la cybersécurité pour les pilotes

<b>R2.3 - Compréhension</b> (Comprendre l'origine du problème ?)	O	O	N	O	O
<b>R2.4 - Rappel</b> (Connaissance d'une procédure applicable ?)	?	O	N	?	Y
<b>R3 – REACTION/RÉACTION</b>	O	O	N	O	O
<b>R3.1 - Immédiate</b> (Le problème a-t-il été géré à temps ?)	O	O	N	O	O
<b>R3.2 – Temps d'adaptation</b> (Bon enchaînement des actions ?)	O	O	N	O	O
<b>R3.3 – Approprié</b> (Procédure correcte appliquée ?)	O	O	N	O	O
<b>R3.4 – Efficacité</b> (Le problème est-il résolu ?)	?	O	N	O	Y

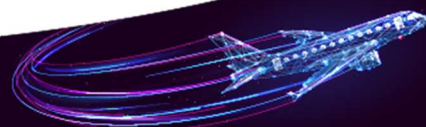
O = oui

N = non

? = impossible à évaluer

Avec la grille d'analyse 3R, trois points remarquables apparaissent :

- Les équipages sont tous "aptes au vol", c'est-à-dire préparés pour le vol.
- Dans le cas de l'attaque n°1 (ADSB), les données collectées n'ont pas permis de tirer de conclusion.
- L'attaque n° 3 (carburant) est l'attaque pour laquelle il n'y a pas d'identification claire du problème et donc pas de réaction adéquate.



## VI. Discussion

### A. L'efficacité de la formation à la cybersécurité pour les équipages d'avions

Même en combinant l'approche par observation directe et l'approche des 3R, les résultats obtenus n'ont pas permis de différencier clairement la capacité à faire face aux cyberattaques du groupe test (ceux à qui l'on a présenté le dossier d'apprentissage numérique sur la cybersécurité) de celle du groupe témoin (ceux à qui l'on n'a pas présenté le dossier d'apprentissage numérique sur la cybersécurité). Les deux groupes se sont montrés **peu sensibilisés** à la menace potentielle de cyberattaques sur un avion commercial en vol.

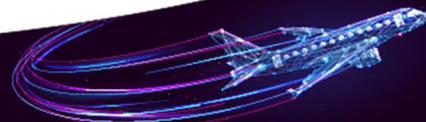
D'autre part, la confrontation directe avec des cyberattaques **au simulateur** a sensibilisé les équipages à la variété et à la quantité de cyberattaques possibles, comme le montre l'enquête menée après l'expérience. Nous concluons donc qu'un dossier d'apprentissage numérique auto-examiné n'est pas suffisant pour sensibiliser les équipages à la menace, et que si cette sensibilisation est souhaitée, une formation plus soutenue est nécessaire. Cette formation renforcée peut par exemple inclure un module approfondi en classe par un instructeur professionnel, une formation sur simulateur informatique ou une formation complète sur simulateur de vol.

La question de savoir si le niveau de menace justifie actuellement un investissement dans ce type de formation sort du cadre de cette expérience et reste une question ouverte qui doit être examinée par les parties prenantes de l'aviation civile et les autorités de réglementation.

### B. Faire face aux différents types de cyber-attaques

Comme mentionné ci-dessus, cinq types d'attaques ont été traités par les équipages et une analyse des résultats en fonction des types d'attaques permet d'éclairer davantage nos résultats en considérant les réactions des équipages dans le contexte pour lequel ils ont été sélectionnés et formés, notamment pour appliquer les procédures opérationnelles standard (SOP).

En effet, les attaques peuvent être interprétées non pas tant en fonction de leur nature (d'origine cyber ou non) mais plutôt selon que leurs conséquences peuvent être identifiées par une alarme ou une vérification prévue par les SOP. Malgré les nombreuses alarmes présentes à bord d'un avion, il existe certaines situations ou combinaisons d'événements pour lesquelles il n'y a pas d'alarmes et/ou pour lesquelles il n'y a pas de SOP.



Les cinq scénarios peuvent donc être divisés en fonction des différents moyens dont disposent les équipages pour identifier et traiter le problème.

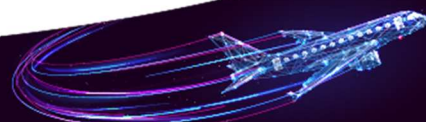
1. Lorsque les équipages ont des indications auxquelles ils peuvent réagir (alarmes et SOP), tous les équipages identifient et traitent le problème correctement, conformément à leur formation. C'est le cas pour les attaques 4 (Piratage du GPS) et 5 (EGPWS). Le fait que le problème soit d'ordre d'une cybermenace n'a pas d'importance, car les équipages savent ce qu'il faut faire sans ambiguïté.
2. En revanche, lorsque les alarmes et/ou les procédures sont incomplètes comme dans les attaques 1 (ADS-B) et 2 (ACARS) avec une intervention extérieure mentionnant un élément inattendu, les réponses de l'équipage peuvent être diverses et donc inappropriées.
3. Enfin, dans le cas où il n'y a ni alarme ni SOP (Attaque 3 - valeur erronée du carburant), la capacité à identifier le problème et à le traiter est très clairement dégradée.

Il existe trois situations très clairement différenciées, en fonction de l'exhaustivité des éléments dont disposent les équipages pour identifier une menace et y faire face. Lors de l'élaboration de la formation des pilotes à la cybersécurité, il convient d'examiner attentivement la manière dont les pilotes doivent être formés à ces trois types de scénarios. Par exemple, compte tenu de la faible probabilité d'occurrence des cyberattaques, il faut prendre en compte le risque d'inciter les équipages à attribuer à tort des problèmes ambigus ou des problèmes pour lesquels il n'existe pas de SOP à une cause cybermenace.

### **C. Étendre la formation à la cybersécurité dans l'aviation**

Cette étude a mis l'accent sur la nécessité d'une formation à la cybersécurité pour les équipages. Les observations et les résultats suggèrent également que la sensibilisation aux risques et aux effets des cyberattaques devrait éventuellement être étendue à l'ATC, aux compagnies aériennes et éventuellement à d'autres acteurs de l'aviation, car ils peuvent être confrontés à des comportements inhabituels et à des questions singulières de la part d'équipages qui tentent d'interpréter des incohérences dans les données disponibles. Dans ces situations, il est important que ces entités soutiennent les pilotes sans mettre en doute leurs compétences, même lorsqu'ils sont confrontés à des interactions et à des questions uniques ou inhabituelles.

En outre, les systèmes exploités par ces entités peuvent également faire l'objet de cyberattaques, un domaine que la présente étude n'a pas abordé.

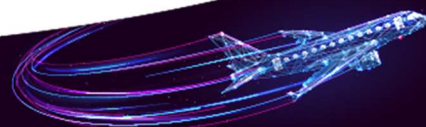


## VII. Conclusion

Dans cette expérience, nous avons examiné la nécessité et l'efficacité d'une formation à la cybersécurité pour les équipages d'avions. Nous avons conclu que tous les équipages participants sont actuellement peu sensibilisés à cette menace. Nous avons également constaté qu'un apprentissage assisté par ordinateur en autonomie n'a pas permis d'accroître cette sensibilisation de manière significative. En revanche, la session au simulateur elle-même a considérablement sensibilisé les équipages à la menace des cyberattaques.

Nous avons analysé trois "catégories" de cyber-attaques sur la base de la disponibilité d'indications et de SOP appropriées pour gérer l'attaque. Chacune de ces catégories nécessiterait un type de formation différent. Le troisième type d'attaques, celles qui ne sont pas accompagnées d'indication claire et qui ne disposent pas de SOP appropriées, représente le plus grand défi pour les pilotes.

Il est recommandé aux autorités réglementaires compétentes, ainsi qu'aux autres parties prenantes de l'aviation civile, de continuer à surveiller la menace croissante des cyberattaques contre les avions et la nécessité qui en découle de former les pilotes à cette nouvelle menace. Comme la probabilité de telles attaques augmente, il est recommandé d'envisager diverses options de formation, y compris une formation complète en classe, et potentiellement une formation sur simulateur.



## VIII. Auteurs

### ASL Airlines France

- Eymoz Franck – Commandant de bord B737 TRI/TRE/SE, ASL Airlines France
- Geslain Marine - Responsable adjoint de la sécurité des vols, ASL Airlines France
- Jacquemin Pierre – Commandant de bord, Responsable de la sécurité des vols, ASL Airlines France
- Pastorelli Ivan - Consultant en gestion de la sécurité, Safety Sciences Ltd.

### Autorité de l'aviation civile d'Israël (CAAI)

- Alook Eli – Chef du service de la réglementation, Autorité de l'aviation civile d'Israël
- Capitaine Molcho Moshe– Chef du département des transporteurs aériens, Autorité de l'aviation civile d'Israël

### Direction Générale de l'Aviation Civile (DGAC)

- Corcos Stephane – Chef de la mission Evaluation et Amélioration de la sécurité chargé de la mise en œuvre du Programme National de Sécurité, Direction Générale de l'Aviation Civile (DGAC), France
- Valot Claude– Consultant en facteurs humains dans la gestion des risques
- Vernay André – Commandant de bord, Gestionnaire du programme des risques humains, Direction Générale de l'Aviation Civile (DGAC), France

### Direction nationale israélienne du cyberspace (INCD)

- Goren Tamir– Directeur des programmes stratégiques, Direction nationale israélienne du cyberspace

