



ASSEMBLÉE — 42^e SESSION

COMMISSION TECHNIQUE

Point 25 : Autres questions à examiner par la Commission technique

**MODERNISER LA FORMATION EN SÉCURITÉ AÉRIENNE :
INCLURE L'INTELLIGENCE ARTIFICIELLE ET LA CYBERSÉCURITÉ
DANS LES NORMES DE COMPÉTENCES DE L'OACI POUR L'ATSEP**

[Note présentée par la Fédération internationale de
L'Association de la Sécurité électronique aérienne (IFATSEA)]

RÉSUMÉ ANALYTIQUE

L'industrie de l'aviation devient de plus en plus complexe chaque jour avec les avancées technologiques telles que l'intelligence artificielle, l'automatisation et la numérisation. Ces technologies refaçonnent et redéfinissent l'exécution des opérations techniques très vite. Étant donné que l'industrie de l'aviation dépend fortement de l'atteinte d'un niveau de sécurité élevé, il sera préférable pour l'industrie que les professionnels au cœur de ces opérations techniques maîtrisent l'utilisation et la gestion de ces technologies qui s'appliquent aux opérations de l'aviation civile. Ce document recommande une mise à jour du *Manuel sur la formation et l'évaluation basées sur les compétences du personnel dans l'aspect électronique de la sécurité de la circulation aérienne* (Doc 10057), afin d'intégrer l'intelligence artificielle (IA) et la cybersécurité en tant que domaines de formation distincts et essentiels. Ces technologies en évolution rapide présentent à la fois des défis et des opportunités de transformation pour le secteur de l'aviation. Les intégrer dans les directives de formation de l'OACI, aux côtés des dispositions des *Procédures pour les services de navigation aérienne – Formation* (Doc 9868), est essentiel pour assurer la préparation, la sécurité et la résilience dans tous les États membres.

Suite à donner : L'Assemblée est invitée à :

- a) approuver l'inclusion d'un domaine d'IA et de cybersécurité dans le document 10057 de l'OACI ;
- b) charger le Secrétariat de l'OACI d'initier la rédaction et la consultation avec les experts concernés ;
- c) encourager les États membres à piloter de nouveaux modules de formation et à partager les résultats.

<i>Objectifs stratégiques :</i>	Ce document de travail concerne les objectifs stratégiques tels que : <i>Chaque vol est sûr et sécurisé, L'aviation est écologiquement durable, L'aviation offre une mobilité transparente, accessible et fiable pour tous et Aucun pays laissé de côté.</i>
<i>Incidences financières :</i>	À déterminer

¹ Versions française, anglaise, arabe, chinoise, espagnole et russe fournies par l'IFATSEA.

Références :	Doc 10057, <i>Manuel sur la formation et l'évaluation basées sur les compétences du personnel dans le domaine électronique et de la sécurité de la circulation aérienne</i> Doc 9868, <i>Procédures pour les services de navigation aérienne – Formation</i>
--------------	---

1. INTRODUCTION

1.1 L'industrie de l'aviation civile est en pleine révolution technologique. L'automatisation, l'analyse prédictive et la sécurité numérique redéfinissent la façon dont les opérations de l'aviation civile sont gérées, exploitées et sécurisées. L'IA est utilisée dans les opérations et les systèmes de contrôle de l'aviation civile, la planification de l'équipage, l'analyse de la sécurité et les services aux passagers. L'augmentation des menaces cybernétiques nécessite une main-d'œuvre solide et qualifiée en matière de cybersécurité dans tous les systèmes aéronautiques. Pour suivre le rythme de cette évolution, le *Manuel sur la formation et l'évaluation basées sur les compétences du personnel dans le domaine électronique et de la sécurité de la circulation aérienne* (Doc 10057) doit être mis à jour pour inclure des conseils structurés sur l'élaboration de programmes de formation en IA et en cybersécurité.

1.2 L'inclusion d'un domaine de formation à l'IA et à la cybersécurité dans le Doc 10057 de l'OACI va doter les professionnels de l'électronique de la sécurité du trafic aérien (ATSEP) dans toutes les régions d'un ensemble de compétences unifié, améliorant les compétences en matière de gestion du trafic aérien, de partage de données et de réponse à la cybersécurité

1.3 La maîtrise de l'IA et de la cybersécurité par l'ATSEP renforce la résilience du système et favorise un esprit de proactivité pour prévenir, atténuer et relever les défis des menaces numériques.

1.4 Pour rendre les cadres de compétences de l'OACI conforme aux réalités technologiques, le Doc 10057 devrait être mis à jour pour offrir des conseils structurés sur l'IA et la cybersécurité, complétant les principes de formation fondamentaux des *Procédures pour les services de navigation aérienne – Formation* (PANS-TRG, Doc 9868).

2. DISCUSSION

2.1 Les menaces liées à l'IA et à la cybersécurité transforment l'industrie de l'aviation civile et les systèmes de gestion du trafic aérien (ATM) mondiaux en mettant fortement l'accent sur la numérisation, l'automatisation, la centralité des données et l'interopérabilité. Ces développements auront des implications importantes pour les professionnels de l'ATSEP, dont le rôle est essentiel pour assurer la sécurité et la performance des systèmes ATM.

2.2 Les professionnels de l'ATSEP va travailler de plus en plus avec des technologies émergentes telles que :

- a) automatisation pilotée par l'IA ;
- b) plateformes numériques de partage d'informations ;
- c) infrastructure modulaire et ritualisée ;
- d) outils de performance du système en temps réel.

2.3 La portée des travaux de l'ATSEP s'étend progressivement au-delà de la maintenance et de l'exploitation des systèmes existants pour s'étendre à la gestion des infrastructures intégrées, numériques et dynamiques.

2.4 Compte tenu du fait que les systèmes de l’aviation civile évoluent vers l’intégration des systèmes et la cybersécurité, l’ATSEP sera crucial pour :

- a) concevoir, mettre en œuvre et sécuriser les systèmes interconnectés ;
- b) assurer la cyber-résilience dans un environnement ATM tellement interconnecté ;
- c) prise en charge des systèmes centrés sur humain et par humain ;
- d) développer et maintenir des outils qui permettent aux contrôleurs et aux systèmes de cogérer les opérations de l’espace aérien ;
- e) s’assurer que les systèmes sont intuitivement conçus, traçables et réactifs aux besoins opérationnels en temps réel.

3. CONCLUSION

3.1 Incluant un domaine de formation sur l’IA et la cybersécurité dans le document 10057, l’OACI ouvre la voie à une communauté mondiale de l’aviation plus résiliente, unifiée et avant-gardiste grâce aux éléments suivants :

Développement collaboratif de programme de formation

- a) Encourager les initiatives conjointes de programmes d’études entre les États membres de l’OACI, les académies d’aviation et les partenaires de l’industrie.
- b) Permettre aux pays à faibles ressources de tirer parti de l’expertise mondiale et de localiser des programmes de formation de pointe.

Innovation collective

- a) La formation partagée stimule la pollinisation croisée des idées entre les États et les opérateurs, contribuant ainsi au développement de technologies plus intelligentes et plus sûres.
- b) Favoriser une culture de collaboration, où les solutions d’IA et les cadres de cybersécurité bénéficient de perspectives diverses et d’une recherche commune.

3.2 L’inclusion d’un domaine de formation sur l’IA et la cybersécurité dans le document 10057 encourage le développement de parcours de formation permettant aux économies émergentes de participer à l’innovation aéronautique. Cela va réduire également la fracture numérique en démocratisant l’accès à l’éducation essentielle en matière d’IA et de cybersécurité.

3.3 La coordination dirigée par l’OACI va veiller à ce que les programmes d’études intègrent des modules d’IA et de cybersécurité conformes aux cadres du Doc 9868.

3.4 Les professionnels conscients de la cybercriminalité seraient mieux équipés pour défendre l’infrastructure de l’aviation contre les menaces croissantes telles que les ransomwares et les violations de système.

3.5 L’Assemblée est invitée à examiner les actions contenues dans le résumé analytique.