



ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 13 : Sûreté de l'aviation — Politique

**STRATÉGIE DE CYBERSÉCURITÉ DE L'AVIATION DANS LE CADRE D'UN
PLAN DE TRAVAIL CONCERTÉ POUR LA PROTECTION DE L'AVIATION
CIVILE**

(Note présentée par la Colombie avec l'appui de 16 États membres de la CLAC²)

RÉSUMÉ ANALYTIQUE

L'aviation connaît une transformation numérique sans précédent. Des technologies telles que les communications numériques, l'intégration de systèmes intelligents, l'analytique des données, la surveillance avancée, les systèmes ATM prédictifs et l'informatique en nuage sont en train de remodeler le secteur. Toutefois, cette interconnexion croissante augmente la surface de cyberattaque et la vulnérabilité aux cybermenaces. Des attaques de plus en plus sophistiquées compromettent la sécurité, la confidentialité des données et la confiance dans le système.

Pour relever ce défi, il est essentiel de renforcer la cybersécurité du secteur. Les États membres devraient mettre en œuvre les recommandations de l'OACI, telles que la Stratégie pour la cybersécurité de l'aviation et le Plan d'action pour la cybersécurité, et les adapter à leur contexte national, en renforçant leur culture organisationnelle, leur infrastructure technologique et leur réglementation relative à la cybersécurité afin de relever les défis spécifiques liés à la cybersécurité dans l'aviation civile.

En outre, la nature transactionnelle du cyberspace exige un dialogue et des mécanismes de coopération technique et opérationnelle entre les États membres.

Suite à donner : L'Assemblée est invitée à :

- a) demander au Conseil de l'OACI d'élaborer, dans le cadre de son Plan stratégique 2026-2050, un outil d'auto-évaluation permettant aux États de mesurer leur niveau de maturité en matière de cybersécurité de l'aviation.

<i>Objectifs stratégiques :</i>	La présente note de travail se rapporte aux objectifs stratégiques suivants : - <i>Chaque vol est sûr et sécurisé</i> - <i>L'aviation assure une mobilité fluide, accessible et fiable pour tous</i> - <i>Aucun pays laissé de côté</i>
<i>Incidences financières :</i>	

¹ Version espagnole fournie par la Colombie.

² Belize, Bolivie (État plurinational de), Costa Rica, Cuba, Équateur, El Salvador, Guatemala, Honduras, Jamaïque, Mexique, Nicaragua, Panama, Paraguay, Pérou, Uruguay, Venezuela (République bolivarienne du).

<i>Références :</i>	- Annexe 17 — <i>Sûreté de l'aviation</i> - Document de l'OACI : <i>Stratégie pour la cybersécurité de l'aviation</i> - Document de l'OACI : <i>Orientations en matière de politique de cybersécurité</i> - <i>Résolution A41-19, Cybersécurité dans l'aviation civile</i> - Document de l'OACI : <i>Plan d'action pour la cybersécurité</i>
---------------------	--

1. INTRODUCTION

1.1. L'aviation mondiale a connu une transformation numérique sans précédent, sous l'impulsion des technologies de pointe. Cette numérisation accroît toutefois la vulnérabilité aux cyberattaques, qui peuvent compromettre la sûreté et la confiance dans le système. Le renforcement de la cybersécurité est donc essentiel à la protection des informations et à la poursuite des opérations aériennes.

1.2. Les États ont élaboré une stratégie globale de cybersécurité qui comprend la formation des ressources humaines, le renforcement des technologies de sûreté, la mise en place d'un cadre réglementaire, la coopération du secteur public et du secteur privé et la collaboration internationale. Cette stratégie vise à améliorer de manière globale la formation du personnel, l'infrastructure technologique et la gestion des risques au niveau de l'État.

1.3. La coopération internationale est essentielle pour renforcer l'aviation contre les cybermenaces. Le partage d'informations, la coordination des réponses et les mécanismes de collaboration — dont l'importance a été illustrée par l'incident du 19 juillet 2024 qui a eu des répercussions sur les systèmes de gestion des entreprises de transport aérien dans le monde entier — contribuent à atténuer les risques et à garantir la sécurité.

1.4. La numérisation a accru la vulnérabilité de l'aviation civile aux cyberattaques qui mettent en péril sa sécurité et son infrastructure. Le renforcement de la cybersécurité est une priorité stratégique pour assurer la continuité et la résilience.

1.5. La stratégie et le plan d'action de l'OACI pour la cybersécurité de l'aviation constituent un cadre solide pour relever ces défis. Toutefois, la mise en œuvre effective de ces recommandations nécessite une action coordonnée et soutenue au niveau régional, ainsi qu'un engagement fort de la part de toutes les parties prenantes, y compris les États membres, l'industrie et le monde universitaire, à l'appui des objectifs stratégiques de l'OACI pour la période 2026-2050.

2. ANALYSE

2.1. La numérisation a optimisé l'aviation civile, améliorant les processus et la compétitivité. Cependant, l'interconnexion des systèmes a accru les risques de cybersécurité, notamment l'accès non autorisé aux données et les tentatives d'altération de systèmes critiques. Les États doivent donc renforcer leurs capacités individuelles et coopérer pour améliorer la sécurité et la confiance dans le secteur.

2.2. L'aviation civile est confrontée au défi de tirer parti de la numérisation tout en garantissant la cybersécurité. Cela nécessite la mise en œuvre de technologies de sécurité numérique, la formation du personnel, le partage d'expériences et l'élaboration de politiques et de stratégies de sécurité de l'information et de sécurité numérique pour les entreprises du secteur.

2.3. L'OACI considère la cybersécurité comme une responsabilité partagée qui nécessite une coopération internationale. Étant donné l'évolution rapide et le caractère transnational des cybermenaces,

les États devraient réagir de manière souple et coordonnée en partageant des informations, des bonnes pratiques et des ressources techniques.

2.4. Les cyberattaques contre l'aviation civile ne sont pas une menace hypothétique mais une préoccupation réelle. Des acteurs malveillants peuvent compromettre des systèmes critiques tels que les systèmes de contrôle de la circulation aérienne, de navigation et de gestion des vols, mettant ainsi en péril la sécurité de millions de passagers et membres d'équipage. Les cyberattaques peuvent en outre perturber considérablement les opérations aériennes, entraînant des pertes financières qui se chiffrent en millions et portant atteinte à la réputation du secteur.

2.5. L'aviation civile est confrontée à des cyberrisques, notamment le vol de données, l'altération des systèmes, l'interruption de services cruciaux, entraînant la perte de confiance du public. Le renforcement de la cybersécurité est essentiel pour garantir la sûreté et la sécurité des opérations et préserver la stabilité du secteur.

2.6. Face à la menace croissante des cyberattaques, il est essentiel d'adopter une approche globale et concertée pour renforcer la cybersécurité dans l'aviation civile en créant un cadre solide pour guider les États et les parties prenantes dans la mise en œuvre de mesures de sûreté efficaces. Ce cadre devrait s'appuyer sur l'engagement de la haute direction, une gouvernance efficace et des politiques claires en matière de cybersécurité pour la protection des systèmes d'information et d'exploitation critiques.

2.7. Un processus devrait être mis en place pour renforcer les capacités de cybersécurité de l'aviation civile. Sa stratégie devrait reposer sur quatre piliers : i) la formation du personnel, ii) le renforcement de l'infrastructure technologique interne, iii) l'élaboration d'un cadre réglementaire pour promouvoir la cybersécurité dans l'ensemble de l'aviation civile et iv) la coopération entre les entités.

2.8. Cette stratégie vise à promouvoir la sûreté de l'aviation civile en gérant l'intégrité, la disponibilité et la confidentialité de l'information dans les systèmes critiques, garantissant ainsi une prestation de services efficace et la protection des données sensibles grâce à des talents hautement qualifiés. Un cadre réglementaire solide devrait également être mis en œuvre pour renforcer la cybersécurité dans les entreprises de transport aérien, les aéroports, les fournisseurs et les fabricants, en encourageant des pratiques de sûreté robustes et une réponse coordonnée aux cyberincidents, afin d'accroître la résilience et de maintenir la confiance des usagers face aux menaces numériques croissantes.

2.9. Il est en outre essentiel de développer des talents spécialisés grâce à une formation continue à la cybersécurité. La formation de professionnels qualifiés est cruciale pour garantir la sécurité et réduire les risques liés à la rotation du personnel. Il est également nécessaire de constituer un centre spécialisé de réponse aux incidents de cybersécurité dans l'aviation civile afin de permettre une réaction rapide et coordonnée aux cyberincidents. Ce centre devrait faire office de plateforme pour la gestion des incidents, la coordination des efforts avec les parties prenantes de l'industrie et la formation de ses propres équipes.

2.10. La coopération internationale constitue un autre élément clé du partage d'informations et de l'élaboration d'exercices de simulation conjoints pour répondre efficacement aux cybermenaces transfrontalières. Une plateforme technologique unique favoriserait l'échange de connaissances et de bonnes pratiques.

2.11. Il convient de maintenir un dialogue permanent avec les autorités et les entreprises du secteur afin de coordonner une réponse unifiée aux cybermenaces. Toutefois, le cyberespace ne connaît pas de frontières et ce dialogue devrait donc inclure les États, qui devraient mettre en place des mécanismes efficaces et solides pour partager leurs expériences et échanger des recommandations sur les stratégies nationales de cybersécurité.

2.12. Il est essentiel que ces stratégies se fondent sur la législation et la réglementation de chaque État, mais elles devraient également être interopérables pour garantir la sécurité opérationnelle à l'échelle mondiale. La collaboration et le partage d'informations entre experts devraient être encouragés afin d'identifier et de traiter les vulnérabilités et de renforcer la résilience de l'industrie face aux cyberattaques. Il importe également de créer une instance permanente où les experts puissent fournir un retour d'information sur les stratégies locales et travailler conjointement pour combler les lacunes susceptibles d'être exploitées par les cybercriminels ou les cyberterroristes.

2.13. À cet égard, il est jugé nécessaire que l'OACI encourage les initiatives visant à renforcer la gestion de la cybersécurité dans l'aviation civile. La création d'un outil d'auto-évaluation intégré au Plan stratégique 2026-2050 se justifie dans la mesure où il permettrait aux États de détecter rapidement les lacunes politiques, opérationnelles et techniques, ce qui faciliterait la planification précoce des mesures d'atténuation et le développement des capacités nationales. Cela permettrait de garantir un niveau de protection plus homogène entre les États, en réduisant les asymétries qui génèrent actuellement des vulnérabilités dans le réseau mondial de l'aviation.

2.14. De même, il est essentiel que l'OACI promeuve des lignes directrices techniques et politiques plus spécifiques sur la cybersécurité qui guident les États dans l'adoption des meilleures pratiques et des normes internationales. Cela favoriserait la construction d'un cadre commun permettant de faire face plus efficacement aux menaces numériques, de renforcer la résilience du système aéronautique et de préserver la sécurité et la continuité des opérations aériennes au niveau mondial.

3. CONCLUSION

3.1. La cybersécurité dans l'aviation civile est un défi qui nécessite une réponse globale et coordonnée. L'OACI, en collaboration avec ses États membres, devrait prendre l'initiative de rendre le secteur plus sûr et plus résistant aux cybermenaces. La sécurité de millions de passagers et la stabilité du système aéronautique mondial en dépendent.

— FIN —