



ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 13 : Sûreté de l'aviation – Politique

NÉCESSITÉ DE RENFORCER LES MESURES DE GESTION DES FACTEURS HUMAINS ET DE LA CYBERSÉCURITÉ DANS LE DOMAINE DE LA SÛRETÉ DE L'AVIATION

(Note présentée par la République de Cuba et appuyée par 17 États membres de la CLAC²)

RÉSUMÉ ANALYTIQUE

La présente note porte sur les facteurs humains et leurs incidences sur le développement et les performances du personnel chargé de la sûreté de l'aviation, un domaine essentiel dans lequel il est possible de définir des stratégies et de prendre des mesures supplémentaires en vue d'attirer des professionnels de la sûreté de l'aviation et, plus généralement, d'apporter une stabilité aux personnes formées à ces fonctions. Il conviendra d'agir en concertation pour continuer de renforcer la sûreté de l'aviation, laquelle joue un rôle essentiel dans le développement durable du transport aérien, en recrutant et en retenant un personnel qualifié et compétent, capable d'assurer et de maintenir l'efficacité et l'efficience du système.

Suite à donner : L'Assemblée est invitée à :

- a) prendre note des informations présentées ;
- b) prier instamment les États de renforcer les mesures de gestion des facteurs humains et de la cybersécurité dans le domaine de la sûreté de l'aviation, notamment par :
 - l'élaboration de plans de gestion globaux des facteurs humains et de la cybersécurité qui soient conformes aux prescriptions de l'Annexe 17 à la Convention de Chicago et à la stratégie pour la cybersécurité de l'aviation de l'OACI ;
 - des évaluations périodiques des risques et l'actualisation des mesures de sûreté ;
 - la promotion de la coopération nationale et internationale aux fins de la mise en commun des informations et des meilleures pratiques ;
 - une formation continue du personnel à la cybersécurité et aux facteurs humains ;
 - la promotion d'une culture institutionnelle axée sur la sécurité numérique et la résilience.

<i>Objectifs stratégiques :</i>	La présente note de travail se rapporte à l'objectif stratégique <i>Chaque vol est sûr et sécurisé.</i>
<i>Incidences financières :</i>	Des ressources consacrées au recrutement et à la formation du personnel ainsi que des investissements dans la technologie.

¹ Version espagnole fournie par Cuba.

² Belize, Bolivie (État plurinational de), Brésil, Chili, Colombie, El Salvador, Équateur, Guatemala, Honduras, Jamaïque, Mexique, Nicaragua, Panama, Paraguay, Pérou, Uruguay, Venezuela (République bolivarienne du)

<i>Références :</i>	Doc 10118, Plan mondial pour la sûreté de l'aviation (GASep), deuxième édition Résolution A41-18, <i>Exposé récapitulatif de la politique permanente de l'OACI relative à la sûreté de l'aviation</i> Résolution A41-19, <i>Cybersécurité dans l'aviation civile</i> Annexe 17 – <i>Sûreté de l'aviation</i> Doc 8973, <i>Manuel de sûreté de l'aviation</i> Stratégie pour la cybersécurité de l'aviation Déclaration de Mascate sur la sûreté et la cybersécurité de l'aviation
---------------------	---

1. INTRODUCTION

1.1 La sûreté de l'aviation est essentielle pour le développement durable et efficace du transport aérien dans le monde. Pour une exploitation sûre et fiable, ce secteur vital pour la connectivité mondiale et la croissance économique doit pouvoir s'appuyer sur des normes de sûreté strictes. Les facteurs humains jouent à cet égard un rôle décisif car la prévention des incidents et des accidents dépend largement de la formation, des performances et de la prise de décision du personnel à toutes les phases des opérations aériennes. En outre, la mise en œuvre appropriée des normes et procédures internationales nécessite obligatoirement une gestion efficace des facteurs humains. Si elle était davantage étudiée et mise en application, cette gestion pourrait permettre de renforcer encore la sûreté du système aéronautique et de garantir sa résilience.

1.2 La complexité croissante de l'aviation, qui est due au développement technologique et à l'apparition de nouvelles menaces, a conduit la communauté internationale à mettre en place des cadres réglementaires solides. À cet égard, l'Annexe 17 de l'OACI constitue la principale réglementation sur la protection de l'aviation civile internationale contre les actes d'intervention illicite, y compris contre les menaces physiques et les cybermenaces. Il est noté dans cette Annexe que pour garantir la sûreté de l'aviation, il convient de mettre en place non seulement des barrières et des procédures physiques, mais aussi une gestion globale des facteurs humains et de la cybersécurité. Ces deux éléments sont devenus essentiels pour garantir la résilience de l'aviation face aux défis actuels et futurs.

2. ANALYSE

2.1 Les facteurs humains englobent tous les aspects du comportement, des performances, des compétences et des limites du personnel de sûreté, ce qui couvre la sélection et la formation, la gestion du stress et de la fatigue, la communication et la prise de décision dans les situations critiques. Le personnel de sûreté doit avoir une solide formation technique et professionnelle, des certifications spécifiques et une expérience de la gestion de telles situations. La formation continue est essentielle pour faire en sorte que le personnel reste au fait des menaces et des technologies de sûreté, toutes deux évoluant constamment.

2.2 Les difficultés qui se posent actuellement sont notamment les suivantes :

- a) **Pénurie de personnel qualifié** : le secteur a du mal à attirer et retenir les personnes qui possèdent les compétences spécialisées requises, et cela peut compromettre l'efficacité des mesures de sûreté et limiter les capacités de gestion des incidents.
- b) **Fatigue et surcharge de travail** : en raison de la pénurie de ressources humaines, il arrive que le personnel doive enchaîner de longues heures de travail, qu'il soit sujet à la fatigue et que ses performances se trouvent diminuées, ce qui accroît les risques d'erreurs et de situations dangereuses.
- c) **Adaptation technologique** : du fait de l'adoption rapide de nouvelles technologies, le personnel doit s'adapter et développer ses compétences numériques pour être en mesure d'exploiter des systèmes complexes et de protéger les informations sensibles.
- d) **Gestion des informations sensibles** : le personnel doit être en mesure de traiter des données confidentielles et de réagir correctement en cas d'incidents de sûreté, y compris face à des cybermenaces.
- e) **Diversité et travail d'équipe** : dans les équipes dont les membres appartiennent à des cultures et à des générations différentes, il est essentiel de pouvoir compter sur de solides compétences de communication et d'encadrement afin d'éviter les malentendus et de favoriser la collaboration.

2.3 La pénurie de personnel de sûreté peut être la cause d'erreurs, de retards dans les processus et d'un amoindrissement des capacités de gestion des incidents. Elle peut également avoir des incidences sur la mise en œuvre des mesures de sûreté et donner lieu à un accroissement de la charge de travail, ce qui peut conduire à des situations dangereuses. Le risque opérationnel peut s'en trouver accru et des menaces risquent de ne pas être détectées.

2.4 Les stratégies pouvant permettre de prévenir et de limiter les pénuries de ressources humaines sont notamment les suivantes :

- a) gestion prévisionnelle des ressources humaines ;
- b) recrutement et rétention du personnel ;
- c) formation continue ;
- d) appui technologique ;
- e) amélioration des conditions de travail ;
- f) supervision et amélioration continue.

2.5 Avec l'environnement numérique sont apparus de nouveaux risques et défis en matière de sûreté. L'Annexe 17 de l'OACI souligne l'importance de la cybersécurité pour la protection contre les actes d'intervention illicite. Pour être prêt à détecter, prévenir et combattre les cybermenaces, le personnel de sûreté doit pouvoir s'appuyer sur les éléments suivants :

- a) **Formation sur la cybersécurité** : une formation spécifique à l'identification des cybermenaces et à la mise en œuvre de protocoles de gestion de ce type de menaces.
- b) **Gestion des cyberincidents** : développement de compétences en matière d'intervention face aux incidents qui peuvent compromettre la sécurité.
- c) **Culture de la cybersécurité et sensibilisation à la question** : promotion des meilleures pratiques et sensibilisation du personnel à tous les niveaux.

2.6 L'Annexe 17 énonce l'obligation de recenser les systèmes critiques de technologies de l'information et de la communication et de mettre en œuvre des mesures fondées sur l'évaluation des risques pour la protection de ces systèmes. Cette mise en œuvre nécessite une intégration de la cybersécurité aux programmes de sûreté nationaux, une collaboration intersectorielle et un contrôle continu des mesures mises en place.

3. CONCLUSIONS

3.1 La sûreté de l'aviation est un système complexe et dynamique, dans lequel les facteurs humains sont la clé de l'efficacité de l'ensemble des mesures et procédures en place. La capacité des États et des organisations à anticiper les risques et menaces conventionnels et nouveaux, y compris les cybermenaces, ainsi qu'à les prévenir et à y parer efficacement repose en grande partie sur une gestion appropriée de ces facteurs.

3.2 La cybersécurité est un nouveau défi pour la gestion des facteurs humains. L'environnement numérique a élargi l'étendue des menaces pour la sûreté. Le personnel doit être préparé à faire face non seulement à des risques physiques, mais aussi à des cyberrisques. Il faut pour cela qu'il puisse s'appuyer sur une solide culture de la cybersécurité, sur des formations spécialisées et sur des protocoles clairs de gestion des incidents numériques. L'intégration de la cybersécurité dans la gestion des facteurs humains est devenue une condition préalable à la protection globale de l'aviation civile.