



ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 13 : Sûreté de l'aviation — Politique

PRATIQUES ACTUELLES ET AMÉLIORATION DE LA CYBERSÉCURITÉ DANS L'AVIATION CIVILE INTERNATIONALE

[Note présentée par la République d'El Salvador, au nom des États membres de la Corporation des services de navigation aérienne d'Amérique centrale (COCESNA)²]

RÉSUMÉ ANALYTIQUE

La technologie joue un rôle essentiel dans le secteur de l'aviation, puisqu'elle contribue à faciliter le tourisme, le commerce et la connectivité mondiale, à stimuler la croissance économique et à améliorer la qualité de vie. Les progrès réalisés dans le domaine des systèmes avioniques ont permis d'améliorer considérablement la gestion de la navigation, la sécurité des avions et l'efficacité opérationnelle. L'innovation technologique dans le secteur est indispensable pour assurer la compétitivité et répondre à la demande croissante en matière de transport aérien.

La cybersécurité de l'aviation civile est devenue une pierre angulaire de la sécurité et de l'efficacité de la navigation aérienne. Le secteur doit actuellement composer avec un environnement dynamique où les cybermenaces sont en constante évolution, d'où la nécessité d'avoir une approche stratégique et coordonnée pour assurer la protection des infrastructures cruciales.

La présente note de travail met en avant une analyse des pratiques actuelles en matière de cybersécurité qui ont cours dans le secteur de l'aviation et recense les principaux aspects de ces pratiques qui devraient être améliorés, en vue de leur application, pour renforcer la résilience des systèmes de l'aviation face aux nouvelles cybermenaces.

Suite à donner : L'Assemblée est invitée à :

- a) prendre note de la teneur de la présente note ;
- b) demander à l'OACI d'évaluer et de renforcer les stratégies de cybersécurité, en adoptant des approches fondées sur les meilleures pratiques internationales, l'échange d'informations et les nouvelles technologies ;
- c) demander à l'OACI de continuer à aider les États à établir et à mettre en œuvre des cadres réglementaires pour la réglementation de la cybersécurité, à former le personnel et à perfectionner ses compétences dans ce domaine, et à élaborer des plans nationaux de sécurité de l'aviation qui tiennent compte de la question de la cybersécurité afin d'assurer la cyberrésilience du secteur.

¹ Version espagnole fournie par El Salvador.

² Belize, Costa Rica, El Salvador, Guatemala, Honduras et Nicaragua.

<i>Objectifs stratégiques :</i>	<i>Chaque vol est sûr et sécurisé. Aucun pays laissé de côté. Le développement économique du transport aérien assure la prospérité économique et le bien-être de la société pour toutes et tous.</i>
<i>Incidences financières :</i>	
<i>Références :</i>	Cadre réglementaire de l'Institut national des normes et de la technologie [National Institute of Standards and Technology (NIST)] Doc 9985 de l'OACI, <i>Manuel de sûreté de la gestion du trafic aérien</i> Doc 10075 de l'OACI, <i>Résolutions de l'Assemblée en vigueur (au 6 octobre 2016)</i> Doc 10161 de l'OACI, <i>Feuille de route pour la sécurité de l'aviation dans le monde</i> Annexe 17 – <i>Sûreté de l'aviation</i>

1. INTRODUCTION

1.1 La technologie joue un rôle essentiel dans le secteur de l'aviation, et les progrès technologiques ont grandement contribué à améliorer la prestation des services de navigation aérienne. Des systèmes tels que la navigation fondée sur les performances (PBN), la surveillance dépendante automatique (ADS-B) et les systèmes de gestion du trafic aérien (ATM) ont transformé la façon dont les vols sont gérés, en apportant plus de précision et en renforçant la sécurité et l'efficacité. Ces systèmes permettent une meilleure planification des routes, réduisent les retards et optimisent l'utilisation de l'espace aérien.

1.2 La cybersécurité de l'aviation civile revêt à présent une importance fondamentale. Les opérations dépendent de plus en plus de systèmes numériques interconnectés, et les ressources technologiques qui les exploitent sont essentielles au fonctionnement sûr et efficace de l'aviation civile. L'évolution technologique a conduit à des problèmes importants, notamment des cyberattaques visant les systèmes de contrôle de la circulation aérienne, les aéroports et les exploitants de transport aérien. Il est donc stratégique et essentiel de les protéger contre les cybermenaces. L'intégrité et la disponibilité de ces systèmes doivent être préservées afin d'éviter les interruptions susceptibles d'affecter la sécurité des opérations et la continuité du transport aérien. Dans ce contexte, la cybersécurité protège non seulement les données et les systèmes, mais renforce aussi la confiance dans l'infrastructure mondiale de la navigation aérienne.

1.3 En réponse à ces menaces, les États ont mis en œuvre diverses mesures de cybersécurité fondées sur des normes internationales, telles que celles élaborées par l'OACI, l'Association du transport aérien international (IATA) et l'Agence de l'Union européenne pour la sécurité aérienne (EASA). Cependant, il reste encore des lacunes à combler pour assurer une protection complète de l'écosystème de l'aviation.

1.4 La présente note a été rédigée dans l'esprit de certaines résolutions de l'Assemblée de l'OACI, soit la résolution **A39-19**, qui constitue une reconnaissance par la communauté internationale du fait que la cybersécurité est une priorité urgente pour l'aviation civile ; la résolution **A40-10** sur la stratégie de l'OACI pour la cybersécurité de l'aviation, qui préconise une approche collaborative et multidisciplinaire ; et la résolution **A41-19**, qui réaffirme l'urgence de prendre en compte la cybersécurité et la cyberrésilience.

2. PRATIQUES ACTUELLES EN MATIÈRE DE CYBERSÉCURITÉ APPLIQUÉES PAR LA COCESNA

2.1 L'importance de la mise en œuvre d'un cadre de cybersécurité de l'OACI a été prise en compte pour la surveillance, la prévention, la détection, la réponse aux cyberincidents, et la reprise après les cyberincidents. À l'heure actuelle, on procède à une mise en commun des meilleures pratiques au sein de la région et au-delà de celle-ci, avec la participation d'organisations internationales comme l'IATA, l'Organisation européenne pour la sécurité de la navigation aérienne (EUROCONTROL) et l'EASA.

2.2 En ce qui concerne la gestion des cyberrisques, la COCESNA est en train de préparer le terrain pour l'application de méthodes d'analyse des risques (ISO 27001, NIST, et MITRE ATT&CK). L'application de telles méthodes permettra d'évaluer en permanence les vulnérabilités des systèmes d'aviation et d'intégrer la cybersécurité dans les systèmes utilisés pour les services de navigation aérienne de la région Amérique centrale. La COCESNA œuvre dans le même sens puisqu'elle a l'intention d'établir un centre des opérations de sécurité, qui permettra à l'organisation de renforcer sa situation en matière de sécurité grâce à une surveillance continue, à une analyse avancée des menaces et à une réponse rapide en cas d'incident. Ce service l'aidera à mettre en œuvre une approche stratégique et efficace pour la protection des systèmes, des données et des utilisateurs, en réduisant au minimum les risques et en garantissant la continuité des activités et la conformité aux réglementations.

2.3 Dans le domaine de la formation et de la sensibilisation, la COCESNA travaille en ce moment à la mise au point d'une formation de base en cybersécurité destinée à tout son personnel, et créera des cours spécialisés destinés à certains membres du personnel qui porteront sur les meilleures pratiques et les tendances en matière de cybersécurité.

3. ASPECTS À PRENDRE EN COMPTE POUR L'AMÉLIORATION DE LA CYBERSÉCURITÉ DANS L'AVIATION

3.1 Pour faciliter la coopération et l'échange d'informations avec des fournisseurs de services de navigation aérienne, il faut créer des plateformes sécurisées permettant de communiquer en temps réel des informations sur les menaces et les vulnérabilités. Pour ce faire, il faut renforcer la collaboration régionale en matière de cybersécurité au moyen d'accords multilatéraux.

3.2 Un cadre réglementaire pour réglementer la cybersécurité devrait être défini et mis en œuvre. Un tel cadre devrait fournir des lignes directrices et des normes claires que les organisations pourraient appliquer pour protéger leurs actifs numériques et préserver la confidentialité des données. La mise en œuvre d'un cadre réglementaire solide contribuera à atténuer les risques, à prévenir les incidents de sécurité et à assurer la continuité des opérations.

3.3 Les programmes de formation en cybersécurité doivent porter sur des aspects techniques et pratiques, tels que la gestion des incidents, l'analyse des risques et la mise en œuvre de mesures de protection. De plus, il est important de favoriser les compétences en communication et en collaboration afin que le personnel puisse travailler en équipe et faire part de ses connaissances en matière de cybersécurité. Investir dans la formation est une stratégie rentable qui renforce la résilience d'une organisation à l'égard des cybermenaces.

3.4 La sensibilisation du personnel à la cybersécurité permet de réduire l'erreur humaine, qui est l'une des principales causes des incidents de sécurité. Selon des études telles que le *Global Risks Report 2022* (rapport d'analyse de 2022 sur les risques mondiaux) du Forum économique mondial, 95 % des

problèmes de cybersécurité sont causés par l'erreur humaine. La sensibilisation aux menaces et les meilleures pratiques en matière de cybersécurité contribuent à créer une culture organisationnelle axée sur la sécurité numérique.

3.5 Il faudrait élaborer un plan de cyberrésilience qui permette d'intégrer la cybersécurité dans les plans nationaux de sécurité de l'aviation (NASP). Un tel plan devrait prévoir des stratégies de reprise en cas de cyberattaque qui permettraient de réduire au minimum leur incidence sur les opérations.

3.6 Il faudrait recenser les vulnérabilités et les aborder de manière proactive afin de protéger l'infrastructure technologique et d'assurer la sécurité des données.

3.7 La coopération avec des spécialistes en cybersécurité de divers secteurs (secteurs technologique, bancaire et autres) peut donner lieu à la transmission de connaissances utiles et permet d'avoir accès à des ressources spécialisées qui améliorent la protection des systèmes de l'aviation.

3.8 L'adoption de technologies nouvelles telles que l'intelligence artificielle et l'informatique en nuage offre des possibilités d'améliorer l'efficacité et la sécurité de l'aviation civile. Cependant, il faut absolument que la mise en œuvre de ces technologies repose sur des mesures de cybersécurité robustes pour conférer une protection contre les vulnérabilités et les menaces potentielles. L'intégration sécurisée de ces technologies pourrait transformer le secteur, mais elle nécessitera une planification rigoureuse et une gestion des risques adéquate.

4. CONCLUSION

4.1 La cybersécurité est un élément clé de la sécurité et de l'efficacité des opérations de l'aviation civile. La protection des systèmes de l'aviation contre les cybermenaces est essentielle pour assurer la sécurité des opérations et la continuité du transport aérien. Bien que des progrès considérables aient été accomplis dans la mise en œuvre des mesures de protection, des problèmes pressants subsistent.

4.2 Le renforcement de la coopération internationale et de l'échange d'information entre les organisations du secteur de l'aviation au moyen de plateformes sécurisées et d'accords multilatéraux sont essentiels non seulement pour l'amélioration de la cybersécurité, mais pour l'intégration de technologies avancées et l'adoption d'approches proactives en matière de gestion des cyberrisques dans l'aviation civile internationale.

4.3 Des normes internationales telles que ISO/IEC 27001 et NIST CSF fournissent des lignes directrices claires pour protéger les actifs numériques et garantir la confidentialité des données, et leur mise en œuvre contribuera ainsi à atténuer les risques et à prévenir les incidents.

4.4 La formation du personnel et la sensibilisation à la cybersécurité réduisent l'erreur humaine, améliorent la capacité de réponse aux menaces et renforcent la résilience des organisations.

4.5 Afin de protéger l'infrastructure technologique, il est crucial d'agir en amont de sorte à recenser et à aborder les vulnérabilités en procédant à une évaluation des risques, à des mises à niveau, à des tests d'intrusion et à une surveillance continue.

4.6 La collaboration avec des spécialistes en cybersécurité de divers secteurs et la sous-traitance de services spécialisés à un centre des opérations de sécurité ou à un fournisseur de services de sécurité gérés permettent une surveillance continue et une réponse rapide en cas d'incident, assurant ainsi une meilleure protection des systèmes de l'aviation.

4.7 L'intégration de mesures de cybersécurité robustes à des technologies telles que l'intelligence artificielle et l'informatique en nuage offre des possibilités d'amélioration de la sécurité et de l'efficacité de l'aviation civile, pour une adoption sûre et efficace de ces technologies.

— FIN —