Organisation de l'aviation civile internationale

**NOTE DE TRAVAIL**

A41-WP/64[1]
EX/33
22/7/22

# ASSEMBLÉE — 41e SESSION

## COMITÉ EXÉCUTIF

**Point 14 : Sûreté de l'aviation – Politique**

## INTÉGRATION ET COORDINATION DES STRATÉGIES ET PLANS DE TRAVAIL DE L'OACI EN MATIÈRE DE CYBERSÉCURITÉ

[Note présentée par l'Association du transport aérien international (IATA)]

**RÉSUMÉ ANALYTIQUE**

La cybersécurité de l'aviation demeure un champ d'intérêt évolutif pour l'OACI, les États et l'industrie. Le point focal n'est pas seulement de repérer et réduire les cybermenaces et les risques d'interférence avec les systèmes numériques, mais aussi d'établir un cadre international pour la mise en place d'innovations technologiques sûres respectant des principes clés comme la sécurité dès la conception dans la chaîne d'approvisionnement aérospatiale.

La présente note de travail fait état de la nécessité d'une approche intégrée et coordonnée de la cybersécurité par le nouveau Comité spécial de coordination de la cybersécurité (AHCCC). On constate que les propositions émanant des groupes d'experts techniques et des sous-groupes, qui pourraient avoir des incidences sur les normes et pratiques recommandées (SARP) et d'autres exigences, reflètent la transversalité de cette discipline, parmi une multitude d'annexes, documents et manuels de l'OACI.

**Suite à donner :** l'Assemblée est invitée à :

a) demander au Conseil de s'assurer que tous les organes de travail de l'OACI développent conjointement une approche concertée transdisciplinaire et à multiples étapes, fondée sur le principe de sécurité dès la conception ; et à

b) demander que le Conseil reconnaisse l'impact potentiel de la mise en œuvre de technologies interconnectées et innovatrices de prochaine génération et de chaînes d'approvisionnement connexes non soumises à la réglementation et aux SARP de l'aviation civile.

| | |
|---|---|
| *Objectifs stratégiques :* | La présente note de travail se rapporte aux objectifs stratégiques transversaux : Sécurité, Sûreté et facilitation, Capacité et efficacité de la navigation aérienne. |
| *Incidences financières :* | Les coûts de développement, de coordination et de traitement des nouvelles dispositions et du matériel d'orientation qui serait livré à l'OACI par l'industrie. |

[1] Versions française, anglaise, arabe, chinoise, espagnole et russe fournies par l'IATA

| | |
|---|---|
| *Références :* | Doc 10140, *Résolutions de l'Assemblée en vigueur (au 4 octobre 2019)*<br>Doc 10108, *État du contexte de risque mondial de sûreté de l'aviation*<br>Résolution A40-10 – *Cybersécurité dans l'aviation civile ; Plan d'action et stratégie de cybersécurité de l'aviation de l'OACI* |

## 1. INTRODUCTION

1.1 Lors de la 40e session de l'Assemblée générale de l'OACI (2019), on a adopté la résolution A40-10 – *Cybersécurité dans l'aviation civile*. Essentiellement, la résolution donnait au Secrétaire général le pouvoir de s'assurer que les questions de cybersécurité sont abordées et coordonnées de façon transversale au moyen des mécanismes appropriés et dans l'esprit de la Stratégie de cybersécurité de l'aviation de l'OACI (2019).

1.2 La Stratégie de cybersécurité de l'aviation de l'OACI propose une série de principes, de mesures et d'activité et identifie de façon pragmatique les actions claires de coordination dans le cadre du Plan d'action pour la cybersécurité de l'OACI (CyAP) (2019), en vue d'aborder les cybermenaces et les éléments requis pour accentuer la posture de résilience de l'aviation civile internationale en vue de la sécurité, de la sûreté et de la confiance numériques.

1.3 En 2022, le Conseil de l'OACI a décidé de créer le Comité spécial de coordination de la cybersécurité (AHCCC) et deux groupes d'experts distincts, relevant de deux comités différents. Cela souligne de façon marquée l'importance accordée par l'OACI et le Conseil au caractère hautement stratégique de la cybersécurité de l'aviation. Le nouveau Groupe d'experts de la cybersécurité (CYSECP), approuvée par le Comité de la sûreté de l'aviation lors de sa 225e session le 24 janvier 2022, a tenu sa première réunion en mai 2022. Les précédentes réalisations du SSGC ont été soulignées par le CYSECP, et un plan de travail a été proposé pour répondre à la nécessité de coordination interne et internationale. De plus, la Commission de navigation aérienne (ANC) a créé le Groupe d'experts des systèmes de confiance (TSP) pour renforcer les perspectives de coordination entre les bureaux, les comités et les groupes d'experts techniques de l'OACI.

## 2. DISCUSSION

### Coordination de l'OACI en matière de cybersécurité

2.1 Il est largement reconnu que la cybersécurité de l'aviation est une discipline transversale et intégrée par sa nature même. En ce sens, le rôle du AHCCC est critique pour qu'une direction stratégique coordonnée mette en relation les plans de travail et les activités de plusieurs organes de l'OACI pour ultimement préserver l'aviation de toute forme d'interférence numérique tout en soutenant des innovations technologiques sûres.

2.2 Naturellement, les SARP et directives issues des documents font souvent référence à la conformité des États par rapport à leurs obligations internationales énoncées dans l'Annexe 19. Par conséquent, il est de première importance que le AHCCC assure la coordination au moyen d'une gouvernance structurée et efficace.

2.3 Les paragraphes qui suivent décrivent plusieurs efforts en lien avec le AHCCC :

a) les activités du Groupe d'experts des systèmes de confiance sont basées sur les fondations de la prochaine génération de mobilité aérienne et touchent le développement d'un concept d'opérations et de gouvernance d'un tel cadre ;

b) le Groupe d'experts de la cybersécurité établit les activités reliées à des propositions de modification des annexes, documents et manuels existants en matière de cybersécurité ;

c) le Groupe d'experts de la gestion de l'information, dans ses Procédures des services de navigation aérienne – Gestion de l'information (PANS-IM) exprime certaines exigences relatives à la sécurité de l'information, et ses efforts portent sur d'autres points, comme la rédaction en cours de la révision 3 du Doc 9896, portant sur la mise en œuvre de services IP sur le réseau de télécommunication aéronautique, ce qui implique aussi des exigences de sécurité dans les manuels ;

d) des modifications sont aussi proposées au Manuel de gestion de la sécurité (Doc 9859) ;

e) mentionnons les résultats du Programme universel de vérification de la sûreté (USAP) pour les SARP relatives à la cybersécurité dans l'Annexe 17, mentionnées dans la note de travail A41-WP/22 présentée par le Conseil de l'OACI ; et

f) mentionnons aussi le travail du sous-groupe de recherche sur les aspects juridiques (RSGLA) et la coordination du Secrétariat avec le Comité juridique, comme il est mentionné dans la note de travail A41-WP/22 présentée par le Conseil de l'OACI.

2.4 Avec le temps, l'intégration des exigences de cybersécurité aux modalités contenues dans différents documents et annexes deviendra complexe. Par conséquent, il faudra peut-être envisager la création d'une nouvelle annexe pour réduire la complexité de l'intégration et faire en sorte que des SARP soient élaborées transversalement pour adopter des mesures d'atténuation des événements intentionnels et non intentionnels et plus encore, les menaces pouvant entraîner des conséquences secondaires ou cumulatives pour la sécurité ou la sûreté qui ne seraient pas nécessairement immédiatement identifiées comme une forme d'interférence numérique.

**Intégration de la transformation numérique**

2.5 Il se produit une évolution constante de la transformation numérique dans plusieurs domaines, qui donne lieu à de plus en plus de technologies connectées, comme la maintenance prédictive des aéronefs, l'intelligence artificielle ou la prise de décision basée sur l'apprentissage machine, l'informatique de pointe, l'architecture ouverte et la mise à jour en direct (OTA) des systèmes critiques de télécommunication.

2.6 Les plus récents concepts de mobilité aérienne émanent de technologies nouvelles et efficaces. Toutefois, les chaînes d'approvisionnement de l'aérospatiale ne sont pas nécessairement régies par les réglementations et normes nationales traditionnelles sur l'aviation civile. Les nouvelles chaînes d'approvisionnement introduisent des possibilités occultes de vulnérabilités dans un environnement opérationnel déjà complexe, dans lequel les cibles de cyberattaques, autrefois limitées aux systèmes existants, comprennent maintenant des technologies interconnectées inconnues. Dans l'ensemble, l'interconnectivité émergente et les dépendances accrues exigent une structure réglementaire claire du domaine aéronautique pour soutenir la navigabilité et la certification des aéronefs.

2.7 Le principe de sécurité dès la conception fait partie d'une approche de politique de cybersécurité soulignée dans la stratégie de cybersécurité de l'aviation de l'OACI. Dans ce contexte, des plans de travail visant à protéger numériquement l'industrie et à soutenir les technologies de prochaine génération ainsi que les produits et services innovateurs doivent être agnostiques et viser l'ensemble du système d'aviation civile. Ils ne doivent pas se limiter à un concept de cadre de confiance ou proposer des modifications des annexes et documents, mais aussi comporter un plan de travail holistique transdisciplinaire selon une approche à plusieurs étapes.

## 3. CONCLUSION

3.1 Les politiques et obligations relatives à la cybersécurité de l'aviation internationale, qui permettent aux exploitants réglementés et à leurs chaînes d'approvisionnement d'obtenir un rendement efficace des investissements, sont critiques pour la durabilité du secteur aérien. De plus, il en va de même de la nécessité du soutien de l'OACI et des États aux efforts internationaux qui permettent à l'industrie d'innover et d'accroître la résilience de l'aviation civile face aux nouvelles chaînes d'approvisionnement. Il est essentiel de promouvoir l'approche de sécurité dès la conception, transdisciplinaire et à plusieurs étapes par sa nature, et d'intégrer les modalités et exigences dans un plan de travail universel, sous la compétence du AHCCC, dans tous les groupes d'experts, de travail et d'étude de l'OACI.

3.2 Un plan de travail basé sur la sécurité dès la conception établirait la base essentielle d'un écosystème intégré, cyberrésilient, agile et innovateur, afin de réduire la fréquence et les impacts des cyberattaques dirigées contre les États et l'industrie susceptibles de compromettre la sécurité et l'ensemble de l'industrie de l'aviation civile internationale.

— FIN —