



ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 13 : Sûreté de l'aviation — Politique

**APPROCHE GLOBALE DE LA CYBERSÉCURITÉ DE L'AVIATION :
DU CONCEPT À LA RÉALITÉ**

(Note présentée par le Danemark au nom de l'Union européenne, de ses États membres¹ et des autres États membres de la Conférence européenne de l'aviation civile², et par EUROCONTROL, avec le coparrainage du Brésil, du Kazakhstan et du Pérou)

RÉSUMÉ ANALYTIQUE

À mesure que l'aviation civile devient de plus en plus interconnectée, les cybermenaces occasionnent une intensification des risques pesants sur la sécurité, la sûreté et l'efficacité de l'aviation. La présente note de travail souligne la nécessité d'adopter une approche globale de la cybersécurité pour unifier les efforts actuellement fragmentés visant à atténuer les risques liés à la cybersécurité.

Une telle approche devrait être appliquée aux principes clés de cybersécurité, tels que l'établissement de cadres de gouvernance, la prise en compte de la sûreté intégrée dans les systèmes, la gestion proactive des cyberrisques alignée sur les protocoles de sûreté et de sécurité, et la formation fondée sur la compétence en cybersécurité dans tous les domaines de l'aviation. L'approche insiste sur l'importance de la résilience tout au long du cycle de vie, d'une coordination à l'échelle mondiale et de l'harmonisation avec les stratégies existantes. À cet égard, l'OACI est invitée à mettre à jour ses politiques, à favoriser la collaboration et à promouvoir des initiatives de renforcement des capacités, en vue d'une harmonisation des pratiques en matière de cybersécurité à l'échelle mondiale.

¹ Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Suède et Tchéquie

² Albanie, Arménie, Azerbaïdjan, Bosnie-Herzégovine, Géorgie, Islande, Macédoine du Nord, Monaco, Monténégro, Norvège, République de Moldova, Royaume-Uni, Saint-Marin, Serbie, Suisse, Türkiye et Ukraine

Suite à donner : L'Assemblée est invitée à :

- a) encourager l'OACI à continuer de renforcer ses politiques ainsi que ses normes et pratiques recommandées, afin de soutenir une approche globale de la cybersécurité et de veiller à ce que l'ensemble de ses organes de travail collaborent pour intégrer la cybersécurité à d'autres cadres réglementaires, favorisant ainsi une mise en œuvre globale et coordonnée des mesures de cybersécurité dans l'aviation civile ;
- b) exhorter les États membres et l'ensemble des parties prenantes concernées de l'aviation à adopter une approche globale de la cybersécurité à l'échelle de tout l'écosystème de l'aviation civile, afin de garantir une gestion harmonisée, proactive et fondée sur le cycle de vie des cyberrisques, ainsi que leur atténuation ;
- c) encourager l'OACI à promouvoir des initiatives de renforcement des capacités afin d'aider les États membres à adopter une approche globale de la cybersécurité, en tirant le meilleur parti des activités de renforcement des capacités existantes et de ses propres ressources ;
- d) considérer, dans la résolution A42-XX de l'Assemblée, qui est proposée pour mettre à jour la résolution A41-19 sur la cybersécurité dans l'aviation civile, la nécessité d'aborder les cybermenaces et les cyberrisques pour l'aviation civile de manière globale.

<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>	Les mesures visées dans la présente note seront entreprises sous réserve des ressources prévues au budget-programme ordinaire et/ou provenant de contributions extrabudgétaires.
<i>Références :</i>	Résolution A41-19 de l'Assemblée

1. INTRODUCTION

1.1 À mesure que l'aviation civile devient de plus en plus interconnectée et numérisée, les cybermenaces font peser des risques de plus en plus importants sur la sécurité, la sûreté et l'efficacité de l'aviation. Cette vulnérabilité est aggravée par l'évolution rapide des fonctions et services de traitement des mégadonnées et des données avancées. De plus, l'intégration croissante de systèmes et d'applications, qu'ils soient récents ou anciens, rendus interopérables par des capacités de mise en réseau renforcées et l'usage de composants « intelligents », transforme l'aviation civile en un écosystème à la fois complexe et hautement évolutif.

1.2 Ces interconnexions posent de nouveaux défis pour garantir la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. Ces derniers doivent être relevés de manière globale, en veillant à ce que chaque aspect de l'écosystème de l'aviation soit sécurisé, de la conception et de l'exploitation des systèmes à la gestion stratégique, dans une logique d'application cohérente à l'échelle mondiale.

1.3 Pour éviter la multiplication d'initiatives isolées, une approche globale de la cybersécurité doit s'étendre à chacun des aspects des pratiques organisationnelles, des mesures proactives et réactives, et des capacités des autorités et de l'industrie. Une telle approche permet d'aligner les efforts de cybersécurité sur l'ensemble des activités de l'aviation civile, assurant une gestion cohérente des risques et renforçant la résilience. Elle facilite également l'intégration des considérations traditionnelles de sûreté et de sécurité de l'aviation à la cybersécurité dans les systèmes et les stratégies de gestion organisationnels, améliorant ainsi leur efficacité et leur performance globales.

1.4 La mise en place par le Conseil de l'OACI du Comité ad hoc de coordination de la cybersécurité (AHCCC) au cours du triennat 2022-2025 constitue une avancée significative vers une réponse plus coordonnée aux questions de cybersécurité. Cette initiative offre une opportunité solide de faire progresser une approche véritablement globale et intégrée de la cybersécurité. L'intégration systématique de la cybersécurité dans l'ensemble des activités, cadres réglementaires et priorités stratégiques de l'OACI renforcera la résilience mondiale et garantira une meilleure préparation du secteur de l'aviation face à la nature complexe et évolutive des cybermenaces.

2. ANALYSE

2.1 Une approche globale permet d'évaluer les cybermenaces et d'atténuer les risques dans l'ensemble de l'écosystème, plutôt qu'au sein de composantes isolées. L'intégration de la cybersécurité à toutes les étapes du développement et de l'exploitation des systèmes peut permettre aux États membres et aux parties prenantes de l'aviation de renforcer leur résilience et de contribuer à un secteur de l'aviation sûr et sécurisé, prêt pour l'avenir.

Cette approche globale devrait guider l'application des principes fondamentaux de la cybersécurité, notamment :

2.1.1 **La gouvernance de la cybersécurité :** Une approche globale de la gouvernance renforce la prise de décisions, l'allocation des ressources et la coopération entre les différents segments du secteur de l'aviation. Une gouvernance efficace permet d'aligner les objectifs en matière de cybersécurité sur les priorités stratégiques et opérationnelles, en fournissant un cadre structuré pour la gestion des ressources. Elle recense les parties prenantes clés, les processus de prise de décisions, les cadres juridiques et les politiques permettant d'orienter les efforts en cybersécurité, tout en facilitant la détermination des menaces et des risques. En outre, la gouvernance de la cybersécurité doit s'intégrer de manière transparente aux domaines de la sûreté et de la sécurité et à la résilience organisationnelle.

2.1.2 **La cybersécurité intégrée :** Une approche de sûreté intégrée globale consiste à prendre en compte la cybersécurité comme un élément central de l'écosystème de l'aviation, plutôt que comme une considération additionnelle. Cette approche est bénéfique, car elle permet aux organisations de traiter proactivement leurs vulnérabilités et d'améliorer leur résilience en intégrant la cybersécurité à chaque phase de développement. Associée à une logique de « sécurité par défaut », elle renforce les infrastructures et les processus de l'aviation, de la conception à l'exploitation. Sa mise en œuvre efficace repose notamment sur la modélisation des menaces dès les premières étapes, l'application de principes de génie sécurisés et l'évaluation des risques tout au long du cycle de vie, afin de traiter les vulnérabilités de manière préventive. La surveillance continue, les mises à jour régulières et les mécanismes de réponse automatisés renforcent l'agilité des systèmes face aux nouvelles cybermenaces, positionnant ainsi l'écosystème de l'aviation à un niveau de cybersécurité élevé.

2.1.3 **La gestion des cyberrisques :** Dans un environnement technologique en évolution rapide, caractérisé par des processus de traitement des données de plus en plus sophistiqués au sein de l'aviation civile, il est essentiel de recenser les actifs et infrastructures critiques (par exemple, la gestion de la circulation aérienne), de les protéger et de renforcer leur résilience face aux cyberattaques, y compris celles liées à des menaces inédites telles que l'intelligence artificielle. La nature interconnectée des systèmes modernes élargit le champ d'exposition aux cybermenaces, rendant indispensable une approche globale de la gestion des cyberrisques. En associant cette dernière aux autres disciplines de gestion des risques, l'aviation peut bâtir un cadre complet et résilient, conciliant sécurité, sûreté et efficacité. Cette stratégie renforce la capacité à atténuer les risques et améliore la résilience face à l'évolution des cybermenaces.

2.1.4 Les connaissances et compétences en cybersécurité : L'élaboration d'une approche globale en matière de formation à la cybersécurité dans l'aviation est essentielle pour développer des compétences solides. Une telle stratégie permet aux personnels concernés d'acquérir l'expertise nécessaire pour gérer efficacement les risques et les mesures liés à la cybersécurité. La formation doit être à la fois pratique et adaptée aux rôles, combinant connaissances théoriques et expérience pratique. L'instauration d'une culture de la formation continue permet au personnel de l'aviation de se tenir au fait des dernières pratiques et tendances, d'adopter les bonnes pratiques, de cerner ses propres vulnérabilités et de mettre en œuvre des stratégies d'atténuation efficaces. Des programmes de formation, des ateliers et des simulations doivent être proposés régulièrement à tous les niveaux, en incluant tous les employés, et pas uniquement le personnel de la technologie de l'information. Cette approche de la formation contribue non seulement à renforcer la cyberrésilience globale de l'écosystème de l'aviation, mais elle permet également à tous les acteurs du secteur d'anticiper et de réagir plus efficacement aux cybermenaces, consolidant ainsi la posture de cybersécurité de l'aviation.

2.2 L'OACI, en tant que chef de file mondial dans la promotion des meilleures pratiques du domaine de l'aviation, joue un rôle déterminant dans l'amélioration de la cybersécurité de l'aviation. Compte tenu de la diversité des niveaux de maturité et des ressources disponibles selon les États, l'OACI devrait promouvoir des initiatives de renforcement des capacités afin de soutenir les États membres dans l'adoption d'une approche globale de la cybersécurité. Ce faisant, l'OACI devrait tirer le meilleur parti des activités de renforcement des capacités existantes (par exemple, les séminaires interrégionaux sur l'innovation et la cybersécurité organisés dans le cadre des projets CASE, financés par la Commission européenne et mis en œuvre par la Conférence européenne de l'aviation civile [CEAC], ou encore les formations en cybersécurité proposées par la CEAC) et de ses propres ressources. Ces initiatives devraient promouvoir une approche cohérente et coordonnée du renforcement des capacités en cybersécurité, tout en favorisant une collaboration sur le plan international par l'échange des meilleures pratiques.

2.3 En outre, l'OACI doit veiller à ce que ses normes et pratiques recommandées, ses politiques et ses outils restent à jour, afin de fournir aux États membres les cadres nécessaires pour gérer efficacement les cyberrisques et adopter une approche globale de la cybersécurité. En outre, les organes de travail de l'OACI devraient renforcer leur collaboration afin de garantir une intégration effective des dispositions relatives à la cybersécurité aux autres exigences réglementaires. Dans ce contexte, le Comité ad hoc de coordination de la cybersécurité (AHCCC) joue un rôle clé en facilitant et en guidant cette coordination, soutenant ainsi une stratégie globale et cohérente dans l'ensemble du secteur de l'aviation.

2.4 Pour faire progresser cette approche globale, il est proposé qu'à la 42^e session de son Assemblée, l'OACI appuie, par la résolution A42-XX de l'Assemblée, qui met à jour la résolution A41-19, la nécessité d'aborder les cybermenaces et les cyberrisques pour l'aviation civile de manière globale. Cette prise en considération au niveau de l'Assemblée renforcera l'engagement des États membres à intégrer systématiquement la cybersécurité dans toutes les activités de l'aviation, assurant ainsi une harmonisation à l'échelle mondiale et une meilleure résilience collective du secteur.

3. SUITE À DONNER

L'Assemblée est invitée à adopter les mesures présentées ci-dessus.