



NOTE DE TRAVAIL

QUATORZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 26 août – 6 septembre 2024

Point 4 : Hyperconnectivité du système de navigation aérienne

4.2 : Cybersécurité et résilience des systèmes d'information

MISE EN ŒUVRE DES ÉLÉMENTS DE BASE
D'UN CADRE DE CYBERSÉCURITÉ DE L'AVIATION

(Note présentée par le Secrétariat)

RÉSUMÉ ANALYTIQUE

La transformation numérique de tous les domaines de l'aviation civile rend pressante la nécessité de réfléchir à la cybersécurité de l'aviation civile afin d'assurer la sécurité, la sûreté, la capacité et l'efficacité du secteur. La présente note de travail recense un certain nombre d'éléments de base de haut niveau que les États et les parties prenantes doivent prendre en compte s'ils veulent aborder la question de la cybersécurité de l'aviation de manière intégrée et harmonisée dans tous les domaines concernés. Elle souligne aussi la nécessité d'élaborer des éléments indicatifs supplémentaires de l'OACI pour soutenir les États et les parties prenantes dans le renforcement de la protection et de la résilience du secteur face aux cybermenaces et aux risques. Elle formule en outre des recommandations pour plus d'harmonisation et de cohérence au niveau régional.

Suite à donner : La Conférence est invitée à approuver la recommandation 4.2/x — Cybersécurité de l'aviation, qui figure au paragraphe 3.

<i>Objectifs stratégiques :</i>	La présente note de travail se rapporte aux objectifs Sécurité, Capacité et Efficacité de la navigation aérienne, et Sûreté et Facilitation
<i>Incidences financières :</i>	<i>Pour le secteur de l'aviation :</i> La mise en œuvre des éléments abordés par la présente note de travail occasionnera des coûts. Toutefois, cette mise en œuvre offrira l'occasion d'adopter une approche claire de la cybersécurité de l'aviation, avec des rôles et des responsabilités clairement définies pour toutes les parties prenantes. <i>Incidence pour l'OACI (par rapport aux ressources actuellement prévues au budget du Programme ordinaire) :</i> Les activités de l'OACI visées par la présente note de travail se poursuivront pendant les prochains triennats. Il faudra des ressources supplémentaires pour soutenir le développement de ces activités, organiser les campagnes de sensibilisation et assurer le soutien à la mise en œuvre.

Références :	Doc 8973, <i>Manuel de sûreté de l'aviation (Diffusion restreinte)</i> Doc 9750, <i>Plan mondial de navigation aérienne</i> Doc 10004, <i>Plan pour la sécurité de l'aviation dans le monde</i> Doc 10118, <i>Plan pour la sûreté de l'aviation dans le monde</i> Doc 10184, <i>Résolutions de l'Assemblée en vigueur (au 7 octobre 2022)</i> Stratégie de l'OACI pour la cybersécurité de l'aviation Plan d'action pour la cybersécurité Orientations en matière de politique de cybersécurité Culture de la cybersécurité dans l'aviation civile
---------------------	--

1. INTRODUCTION

1.1 À sa 40^e session, l'Assemblée de l'OACI a réaffirmé l'importance et l'urgence d'un engagement mondial de toutes les parties prenantes à réfléchir conjointement sur la cybersécurité de l'aviation civile dans le cadre de l'adoption de la résolution A40-10 : *Cybersécurité dans l'aviation civile* et de l'approbation de la Stratégie de l'OACI pour la cybersécurité de l'aviation¹. L'Assemblée a réitéré la nécessité de réfléchir sur la cybersécurité de l'aviation civile dans la résolution A41-19 actualisée.

1.2 L'Assemblée a également appelé l'OACI à élaborer un plan d'action pour soutenir la mise en œuvre de la Stratégie pour la cybersécurité de l'aviation. La deuxième édition du Plan d'action pour la cybersécurité² publiée en janvier 2022 fournit à l'OACI, aux États et aux parties prenantes des bases pour travailler ensemble, et propose une série de principes, mesures et actions pour atteindre les objectifs des sept piliers de la Stratégie pour la cybersécurité³.

1.3 Conformément au Plan d'action pour la cybersécurité, l'OACI a déjà publié des éléments indicatifs sur les questions liées à la cybersécurité de l'aviation. Les travaux de l'OACI comprennent aussi des initiatives liées à la recherche sur l'adéquation des instruments juridiques internationaux de lutte contre les cyberattaques contre l'aviation civile ; la recherche sur la nécessité d'intégrer des normes et des pratiques recommandées pour la cybersécurité de l'aviation dans les Annexes à la Convention relative à l'aviation civile internationale (Convention de Chicago), l'élaboration d'outils pour faciliter la confiance et l'interopérabilité dans les différents domaines de l'aviation, la sensibilisation sur la nécessité de lutter contre les cybermenaces et les risques qui pèsent sur l'aviation civile, l'élaboration de programmes de renforcement des compétences en cybersécurité de l'aviation et la réalisation d'exercices théoriques de cybersécurité de l'aviation internationale.

2. ANALYSE

2.1 Le secteur de l'aviation civile continuant à tirer parti des innovations technologiques pour renforcer sa capacité et son efficacité, tout en maintenant des niveaux convenus de sécurité et de sûreté, la cybersécurité a été intégrée séparément dans chaque domaine de l'aviation. Au fil des ans, cette stratégie a fait de l'aviation un système des systèmes où les contrôles et les processus pour la cyberprotection et la

¹<https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx>

²<https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.FR.pdf>

³ Les piliers de la Stratégie de l'OACI pour la cybersécurité de l'aviation sont : coopération internationale, gouvernance, législation et règlements efficaces, politique de cybersécurité, partage de l'information, gestion des incidents et planification d'urgence, et renforcement des capacités, formation et culture de cybersécurité.

résilience n'ont été ni conçus ni mis en œuvre, de manière intégrée, engendrant ainsi de possibles lacunes au niveau le plus général.

2.2 À cet égard, il est important d'intégrer la cybersécurité dans les domaines de l'aviation civile aux niveaux national, régional et international de manière coordonnée, harmonisée et globale. Ce qui permettrait de soutenir la lutte contre les cybermenaces et les risques qui pèsent sur l'aviation civile, sans compromettre les exigences de sécurité, de sûreté, de capacité et d'efficacité.

2.3 Des progrès notables ont été enregistrés dans la cybersécurité de l'aviation civile, mais il faut élaborer des orientations supplémentaires pour soutenir l'intégration de la cybersécurité de l'aviation dans les systèmes réglementaires et de supervision par les États, ainsi que dans leurs plans régionaux et nationaux dans les domaines pertinents de l'aviation civile, principalement la sécurité et la sûreté de l'aviation, la facilitation, ainsi que la navigation aérienne.

2.4 En outre, la résolution 2341 (2017) du Conseil de sécurité des Nations Unies sur la protection des infrastructures critiques contre les actes terroristes, et la résolution (A/RES/77/298) de l'Assemblée générale de l'ONU sur le huitième examen de la Stratégie antiterroriste mondiale des Nations Unies (A/RES/60/288) soulignent l'importance d'une coopération multipartite et transversale en matière de cybersécurité entre les organisations internationales, régionales et sous-régionales, le secteur privé et la société civile.

2.5 Par conséquent, et conformément aux résolutions de l'Assemblée de l'OACI en vigueur, à sa Stratégie pour la cybersécurité, à son Plan d'action, et aux différents éléments indicatifs élaborés par l'Organisation, la présente note de travail propose des éléments de base qui doivent être pris en compte par les États et les parties prenantes pour répondre aux cybermenaces et aux risques qui pèsent sur l'aviation civile. Ces éléments de base devraient comprendre les éléments suivants :

a) Aspects réglementaires au niveau des États :

- 1) **Gouvernance de la cybersécurité au niveau des États** : Cet élément couvre, sans s'y limiter, les aspects liés à l'identification d'une autorité compétente pour la cybersécurité de l'aviation, l'intégration de la cybersécurité de l'aviation dans les programmes nationaux de sécurité et les programmes nationaux de sûreté de l'aviation civile, la définition des rôles et des responsabilités des autorités aéronautiques et non aéronautiques (par ex., les autorités nationales de cybersécurité) et la coordination de leurs activités de réglementation et de supervision de la cybersécurité de l'aviation civile, l'exploitation des ressources nationales en matière de sécurité pour soutenir les organisations dans la surveillance, la détection, la réponse aux cyberincidents, et la reprise après les cyberincidents.
- 2) **Cadre juridique national** : Cet élément concerne les aspects liés aux cadres juridiques des États permettant de poursuivre les auteurs de cyberattaques contre l'aviation civile. Il couvre aussi les aspects liés à la ratification de la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* (Convention de Beijing de 2010) et du *Protocole complémentaire pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing de 2010) en tant que moyens de faire face aux cyberattaques contre l'aviation civile dans le monde.

- 3) **Politique de cybersécurité de l'aviation** : Cet élément couvre les aspects liés à la politique de cybersécurité de l'aviation au niveau des États.
- 4) **Fonctions de supervision** : Cet élément concerne les aspects liés aux capacités des États en matière de supervision de la cybersécurité de l'aviation qui peut être mise en œuvre à travers les mécanismes existants de supervision de la sécurité et de la sûreté de l'aviation, de manière coordonnée.

b) Éléments liés aux États et aux parties prenantes :

- 1) **Gestion des cyberrisques** : Cet élément couvre les aspects liés à l'identification des infrastructures critiques de l'aviation et l'intégration de l'évaluation des cyberrisques dans les évaluations des risques de sécurité et de sûreté existantes de ces infrastructures.
- 2) **Notification des cyberincidents** : Elle concerne les aspects liés à la mise en œuvre du mécanisme de notification des cyberincidents aux autorités par les entités, à travers un canevas distinct ou à travers les mécanismes de notification existants pour la sécurité ou la sûreté de l'aviation.
- 3) **Partage des cyberinformations** : Cet élément couvre les aspects liés à la mise en œuvre des mécanismes de partage des informations entre les États et les parties prenantes aux niveaux national, régional et mondial.
- 4) **Réponse aux cyberincidents et reprise** : Cet élément concerne les aspects liés à la mise en œuvre de la réponse aux cyberincidents, ainsi que les plans et les capacités de reprise. Il couvre également les aspects liés à l'intégration de ces plans dans les plans de réponse aux urgences/gestion des crises de l'aviation.
- 5) **Gestion de la cyberchaîne d'approvisionnement** : Cet élément couvre les aspects liés à la gestion des cyberrisques auxquels les chaînes d'approvisionnement aéronautiques et non aéronautiques sont exposées. Elles comprennent plusieurs types de chaînes d'approvisionnement, par exemple, les équipements/systèmes certifiés par l'aviation, les services au système de l'aviation (par ex., les systèmes de planification des vols, les réseaux d'aéroport), et les fournisseurs de services non aéronautiques (par ex., les fournisseurs de services d'infonuagique, les fournisseurs de communications satellitaires).
- 6) **Culture de la cybersécurité** : Cet élément comprend les aspects liés à la mise en œuvre d'une culture de la cybersécurité robuste dans l'aviation civile qui tire parti de l'expérience acquise par le secteur dans la mise en œuvre des cultures de la sécurité et de la sûreté.
- 7) **Programmes de formation en cybersécurité de l'aviation** : Cet élément concerne les aspects liés à la conception et au déploiement de programmes de formation en cybersécurité de l'aviation ciblant différents publics (par exemple, sensibilisation générale par opposition à la formation en fonction des rôles).

2.6 Le secteur de l’aviation étant identifié dans plusieurs États comme une infrastructure critique nationale, il faut une approche progressive à plusieurs niveaux pour la protection de la cybersécurité et de la résilience du secteur. L’objectif est de mettre en œuvre une stratégie de défense en profondeur⁴ faisant intervenir directement ou indirectement tous les intervenants impliqués dans la lutte contre les cybermenaces et les risques qui pèsent sur l’aviation civile. Les éléments énumérés ci-dessus ne constituent pas une liste exhaustive des domaines qui doivent être pris en compte dans la portée de la cybersécurité de l’aviation ; toutefois, ils fournissent une base qui permet une gestion solide et efficace de la cybersécurité de l’aviation, y compris la protection et la résilience des actifs de l’aviation gérés par les États et les parties prenantes.

2.7 Des groupes dédiés à la cybersécurité sont établis dans les régions de l’OACI pour soutenir les discussions régionales sur la cyberprotection et la résilience des divers domaines de l’aviation. Ces activités sont très importantes pour les cybermenaces et les risques qui pèsent sur les domaines spécifiques de chaque région, toutefois, il existe un risque de double emploi voire de conflit au cas où ces activités ne sont pas coordonnées entre les différents groupes et plans régionaux. Cette coordination permettra une approche intégrée, harmonisée et coordonnée de la réponse aux cybermenaces et aux risques dans les différentes régions, ainsi que la cohérence et la complémentarité des plans régionaux pour la navigation aérienne, la sécurité et la sûreté, ainsi que la facilitation en ce qui concerne la cybersécurité, ce qui aura une incidence positive sur les activités de planification et de mise en œuvre au niveau des États membres. Les États peuvent utiliser ces instances pour rendre compte à l’OACI des difficultés rencontrées en matière de cybersécurité de l’aviation civile, ce qui va orienter les activités de l’Organisation en matière d’élaboration des dispositions et des éléments indicatifs.

3. CONCLUSION

3.1 La transformation numérique de tous les domaines de l’aviation souligne la nécessité de prendre en compte la cybersécurité dans l’aviation civile afin de garantir la sécurité, la sûreté, la capacité et l’efficacité du secteur. Tout en prenant en considération les difficultés posées par la cybersécurité de l’aviation, les États et les parties prenantes devraient réfléchir aux éléments de base à mettre en place sur les plans réglementaire et opérationnel.

3.2 À la lumière de ce qui précède, la Conférence est invitée à approuver la recommandation suivante :

Recommandation 4.2/x — Cybersécurité de l’aviation

Il est recommandé que les États :

- a) élaborent et mettent en œuvre un plan national pour répondre de manière intégrée aux cybermenaces et aux risques qui pèsent sur tous les domaines de l’aviation civile, conjointement avec les parties prenantes qui ne font pas partie du secteur de l’aviation, en utilisant les éléments de base comme référence ;

⁴ La défense en profondeur est l’application de contre-mesures à plusieurs niveaux ou par étapes pour atteindre les objectifs de sécurité. La méthodologie consiste à mettre en place plusieurs couches hétérogènes de technologies de sécurité dans les vecteurs d’attaque courants pour s’assurer que les attaques qui échappent à une technologie sont stoppées par une autre (voir la norme ISO/IEC 62443 1-1).

- b) harmonisent les activités en matière de cybersécurité de l'aviation dans les plans régionaux de navigation aérienne, de sécurité, de sûreté et de facilitation, au moyen des processus de coordination des groupes régionaux de planification et de mise en œuvre (PIRG), des groupes régionaux de sécurité de l'aviation (RASG) et des groupes régionaux sur la sûreté de l'aviation et la facilitation (AVSEC/FAL) ;
- c) rendent compte à l'OACI de leur expérience dans la mise en œuvre des dispositions et des éléments indicatifs liés à la cybersécurité de l'aviation, par l'intermédiaire des groupes d'experts compétents ou des processus des PIRG, des RASG et des groupes AVSEC/FAL régionaux ;

Il est recommandé que l'OACI :

- d) donne des orientations sur les éléments de base afin de soutenir les États et les parties prenantes dans la réflexion sur la cybersécurité de l'aviation, et intègre toutes les activités en matière de cybersécurité de l'aviation de façon cohérente et coordonnée.

— FIN —