



ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 13 : Sûreté de l'aviation — Politique

GOUVERNANCE DE LA CYBERSÉCURITÉ DANS LE SECTEUR DE L'AVIATION CIVILE ET EXPÉRIENCE DU SULTANAT D'OMAN DU PROGRAMME UNIVERSEL D'AUDITS DE SÛRETÉ – MÉTHODE DE SURVEILLANCE CONTINUE (USAP-CMA)

(Note présentée par le Sultanat d'Oman)

RÉSUMÉ ANALYTIQUE

La présente note insiste sur l'importance d'une gouvernance efficace pour protéger le secteur de l'aviation civile contre les cyberattaques, car elle est la base qui permet de renforcer la coordination et la communication afin de contrer les cyberattaques dans ce secteur vital.

La riposte aux cyberattaques commence par la mise en place d'une structure claire au sein de l'Autorité de l'aviation civile (AAC), l'organe de réglementation du secteur. La structure comprend une division de la réglementation (législation et supervision) et plusieurs divisions chargées de la mise en œuvre des différentes dispositions, dans l'ensemble du secteur.

La note souligne également à quel point il importe de respecter les prescriptions de l'Annexe 19 — *Gestion de la sécurité* et des éléments indicatifs de l'OACI en matière de cybersécurité de l'aviation afin d'atteindre le plus haut degré de conformité et renforcer ainsi l'écosystème de sûreté de l'aviation mondiale.

Suite à donner : L'Assemblée est invitée à :

- a) inviter instamment les États membres à définir et adopter une structure uniforme de gouvernance de la cybersécurité dans le secteur de l'aviation, dans le but d'assurer le respect systématique des engagements internationaux et renforcer ainsi la sûreté et la sécurité du transport aérien mondial face aux cyberattaques ;
- b) inciter les États à élaborer des prescriptions en matière de cybersécurité et à coordonner leur mise en œuvre avec la section ou le service chargé de la conformité aux dispositions de l'Annexe 17 — *Sûreté de l'aviation* de la Convention de Chicago ;
- c) inciter l'OACI à formuler des orientations visant l'établissement d'une gouvernance uniforme de la cybersécurité ;
- d) prendre note de l'expérience du Sultanat d'Oman et tirer parti des enseignements tirés du *Programme universel d'audits de sûreté — Méthode de surveillance continue (USAP-CMA)*.

¹ Version arabe fournie par Oman.

<i>Objectifs stratégiques :</i>	La présente note se rapporte à l'objectif stratégique <i>Chaque vol est sûr et sécurisé.</i>
<i>Incidences financières :</i>	Les concepts proposés dans la présente note seront mis en œuvre sous réserve des ressources financières et humaines disponibles dans les États membres. Les concepts proposés ici peuvent également être compris dans le Plan mondial pour la sûreté de l'aviation (GASeP).
<i>Références :</i>	Politiques mondiales sur l'aviation civile Stratégie en matière d'aviation civile <i>Manuel de sûreté de l'aviation</i> (Doc 8973) Annexe 17 — <i>Sûreté de l'aviation</i> <i>Plan mondial pour la sûreté de l'aviation</i> (GASeP)

1. INTRODUCTION

1.1 Les deux dernières décennies ont vu une évolution rapide dans l'utilisation de technologies modernes de l'information et des communications en aviation civile, afin d'appuyer l'automatisation, la connectivité, l'interopérabilité et la transformation numérique en général. Cette tendance s'est récemment confirmée, en particulier dans le domaine opérationnel, grâce à l'apparition de technologies nouvelles comme l'intelligence artificielle, l'apprentissage automatique et l'analyse des mégadonnées. Cette transformation numérique a permis d'accélérer la mise en œuvre de nouveaux concepts opérationnels au sol et embarqués, qui soutiennent la croissance du secteur de l'aviation civile tout en renforçant la sécurité, la sûreté, l'efficacité, la capacité et la durabilité.

1.2 Dans le cadre de ses responsabilités et obligations énoncées dans la Loi relative à l'aviation civile et en accord avec les normes de pratiques recommandées de l'OACI conçues pour protéger l'aviation civile contre les cyberattaques, l'Autorité de l'aviation civile (AAC) d'Oman travaille de concert avec les autorités nationales pour élaborer la législation dans ce domaine et en superviser la mise en œuvre, conformément au Programme national de sûreté de l'aviation civile, qui reflète les SARP pertinentes de l'Annexe 17 — *Sûreté de l'aviation* ainsi que les dispositions de la réglementation en matière de cybersécurité.

1.3 Des textes de loi sont périodiquement promulgués et actualisés en phase avec les meilleures pratiques qui sont conformes aux dispositions de l'Annexe 17 de la Convention de Chicago, aux SARP sur la cybersécurité, à la Convention de Beijing de 2010, au Protocole de Beijing de 2010, aux résolutions A39-19, A40-10 et A41-19 de l'Assemblée, à la Stratégie et au plan d'action de l'OACI sur la cybersécurité de l'aviation, ainsi qu'aux éléments indicatifs et manuels pertinents, dont le plus récent est le document *Global Cyber Risk Considerations* (Doc 10 213 — Diffusion restreinte — anglais seulement). La législation nationale constitue le principal pilier pour la structuration du secteur et la répartition des tâches et responsabilités aux différents organismes en vue de protéger l'aviation civile contre les cybermenaces.

1.4 Les mesures prises pour s'acquitter des engagements internationaux en matière de sûreté de l'aviation civile et de facilitation doivent s'inscrire dans une structure administrative claire et organisée assurant l'élaboration d'une législation nationale globale qui soutient le personnel opérationnel dans ses efforts pour atténuer les risques et protéger les installations d'aviation civile contre les menaces.

1.5 Selon un rapport publié par l'OACI le 31 décembre 2024, 179 pays ont subi un audit sur site ou sur pièces dans le cadre du Programme universel d'audits de sûreté — Méthode de surveillance continue. Le taux de conformité dans le monde à la norme 4.9.1 est en moyenne de 49 %, ce qui traduit soit l'absence d'une exigence de recenser les infrastructures critiques, soit l'absence de mesures de cybersécurité efficaces.

2. GOUVERNANCE DE LA CYBERSÉCURITÉ

2.1 Il importe de veiller à ce que les rôles et les responsabilités dans le domaine de la cybersécurité fassent consensus et soient bien compris, afin d'assurer la conformité internationale et nationale en matière de réglementation et de supervision. Il en résulte un flux de travail optimal conçu pour éviter le chevauchement des compétences et des responsabilités entre les services chargés de la cybersécurité, pour répondre à tous les besoins afin de protéger l'aviation civile contre les cybermenaces.

2.2 Tout aussi important pour les AAC est d'attacher beaucoup d'attention à la sûreté de l'aviation civile, surtout vu sa nature complexe, afin de garantir un cadre de l'aviation sûr, sécuritaire, régulier, efficace, économique et protégé, par la mise en place d'une structure de gouvernance globale et de catalyseurs opérationnels qui la protègent contre les cyberattaques en tirant parti des dernières technologies.

2.3 Cet aspect revêt encore plus d'importance compte tenu du degré de sophistication et de la fréquence des cybermenaces et attaques dans le monde, leur complexité croissante et les différents motifs invoqués (crime organisé, objectifs financiers, politiques, etc.). S'ajoute à cela le fait que les institutions et les entreprises sont de plus en plus imbriquées dans l'espace numérique en raison des processus de transformation numérique et de leur intégration mutuelle.

3. GOUVERNANCE DE LA CYBERSÉCURITÉ À OMAN (NIVEAU NATIONAL)

3.1 La réglementation de la cybersécurité dans le domaine de l'aviation a été confiée au Service de sûreté de l'aviation de l'Autorité de l'aviation civile (AAC). Dans ce contexte, la Division des systèmes de sûreté de l'aviation est chargée de concevoir et d'actualiser les systèmes de cybersécurité, la Division de la supervision et des licences est responsable du contrôle qualité (audits, inspections, suivi, tests et enquêtes) tandis que la Division de l'évaluation du risque évalue les risques pour la cybersécurité.

3.2 Plusieurs services à l'intérieur du secteur ont pour mandat de mettre en œuvre l'ensemble des dispositions législatives relatives à la cybersécurité en aviation.

4. NIVEAU OPÉRATIONNEL

4.1 Les organes opérationnels ont la responsabilité de se conformer aux prescriptions nationales, d'élaborer des procédures opérationnelles normalisées et de mettre en œuvre les procédures nécessaires pour protéger les systèmes critiques des TIC et les données utilisées en aviation civile.

5. COMITÉ NATIONAL DE SÛRETÉ DE L'AVIATION CIVILE ET DE FACILITATION

5.1 Le Comité national de sûreté de l'aviation civile et de la facilitation d'Oman assure la pérennité de l'aviation civile, conformément à la législation, aux programmes et aux plans nationaux, en phase avec les SARP de l'OACI.

5.2 Le Comité prend également des décisions stratégiques en vue de renforcer la sûreté, la facilitation les prescriptions relatives à la cybersécurité.

5.3 Il réalise en outre des examens et des évaluations en continu de l'efficacité des mesures de sûreté, face à l'évolution constante des menaces, et formule des recommandations visant à modifier des mesures en fonction des renseignements sur la menace, du développement des technologies, des techniques de sûreté et autres facteurs, afin d'arriver à un équilibre entre sûreté et facilitation.

5.4 Le Comité national sur la sûreté de l'aviation et la facilitation est convenu de mettre sur pied un comité technique/consultatif sur la cybersécurité en aviation.

6. LÉGISLATION NATIONALE SUR LA CYBERSÉCURITÉ DANS LE SECTEUR DE L'AVIATION CIVILE

6.1 Outre le Programme national de sûreté de l'aviation civile et du Manuel sur la sûreté de l'aviation civile et la facilitation, l'AAC d'Oman a publié des documents qui traitent de la cybersécurité, tels que :

6.1.1 la Politique sur la cybersécurité en aviation civile ;

6.1.2 les éléments indicatifs relatifs à la cybersécurité de l'aviation civile.

7. SENSIBILISATION À LA CYBERSÉCURITÉ

7.1 L'Autorité de l'aviation civile d'Oman s'attache à sensibiliser aux risques pour la cybersécurité dans l'aviation civile au moyen de la diffusion de bulletins de sensibilisation par plusieurs canaux internes de communication du secteur, de même que par la tenue d'ateliers visant à expliquer les cybermenaces et les risques, et comment s'en protéger, en vue d'atténuer ces menaces.

7.2 L'AAC supervise la préparation de matériel pédagogique et de sensibilisation à la cybersécurité en aviation dans l'ensemble du secteur pour veiller à ce que la documentation soit conforme à la législation nationale et à l'approche avalisée par l'OACI.

8. L'EXPÉRIENCE D'OMAN DU PROGRAMME UNIVERSEL D'AUDITS DE SÛRETÉ — MÉTHODE DE SURVEILLANCE CONTINUE (USAP – CMA)

8.1 L'Autorité de l'aviation civile s'est préparée de façon optimale pour l'audit USAP-CMA, en suivant nombre d'étapes, dont :

a) étudier les documents de l'OACI relatifs à la cybersécurité et la résilience ;

b) élaborer, mettre à jour et adopter des lois en matière de cybersécurité, des éléments indicatifs pour appuyer les organismes dans la mise en œuvre harmonisée de cadres de

gestion de la cybersécurité ; établir une approche systématique à la gestion du risque et évaluer la maturité et l'efficacité de ces cadres ;

- c) diffuser des lignes directrices nationales et internationales de l'OACI et du matériel pédagogique en vue de promouvoir une culture de la cybersécurité ;
- d) exiger des exploitants qu'ils recensent leurs systèmes de TIC critiques pour l'aviation civile ;
- e) exiger des exploitants de concevoir et de mettre en œuvre des mesures pour protéger les systèmes des interventions illicite ;
- f) se tenir au courant des faits nouveaux et participer aux réunions organisées par les groupes de travail et les équipes de l'OACI dans le but d'améliorer la gouvernance de la cybersécurité et renforcer la résilience ;
- g) analyser les résultats des réunions et les recommandations formulées par les équipes qui facilitent l'échange d'informations et préconiser la mobilisation de ressources et l'adoption de mesures pour parvenir à une approche globale en matière de cybersécurité de l'aviation civile ;
- h) établir des centres pour offrir des séances et des ateliers de formation dans l'ensemble du secteur ;
- i) lancer le programme national « *Ertaqa 2* » (Évolution 2) destiné à concevoir et appliquer des méthodes de travail efficaces pour assurer la conformité d'Oman au *Plan mondial pour la sûreté de l'aviation* (GASeP) et proposer des solutions pour répondre aux besoins définis dans le plan de conformité, tels qu'établir des programmes de coopération avec l'OACI, fournir l'expertise pertinente et acquérir les technologies nécessaires.

8.2 Une simulation d'audit international a également été réalisée dans le but d'analyser et de résoudre les lacunes décelées. Cette analyse du cadre de cybersécurité de l'aviation a été exécutée et comparée à celle élaborée par l'OACI. Le cadre couvre les aspects juridique, institutionnel, opérationnel et de formation de la cybersécurité en aviation. L'analyse a permis de formuler d'importantes recommandations, notamment :

- a) attirer les compétences et l'expertise de personnes spécialisées en cybersécurité, en sûreté l'aviation et en audits de l'OACI ;
- b) nommer un expert et des inspecteurs en cybersécurité pour servir de liaison avec l'AAC et assurer la coordination avec tous les organismes du secteur ;
- c) établir des équipes de travail spécifiques pour mettre en œuvre les recommandations et proposer des solutions pratiques, ce qui comprend l'équipe *Ertaqa 2*, composée de plusieurs équipes spécialisées dans les neuf domaines d'audit ;
- d) désigner un point de contact dans chaque organisme chargé de la coordination avec l'AAC ;

- e) soutenir les équipes en répondant à leurs besoins logistiques et techniques ;
- f) concevoir et fournir des outils pour mettre en œuvre la supervision en cybersécurité et les activités d'essais dans le secteur ;
- g) établir et mettre en œuvre des plans de contrôle de la qualité et de suivi dans le cadre des activités de l'équipe opérationnelle chargée de l'audit OACI ;
- h) analyser le résultat des activités de contrôle de la qualité et soumettre les rapports et les recommandations pertinents ;
- i) organiser des activités de soutien et de renforcement des capacités, des ateliers et des programmes de sensibilisation à la cybersécurité pour toutes les parties prenantes, dans chaque organisme ;
- j) concevoir des modèles et des exercices de simulation pour évaluer les risques, recenser les systèmes critiques et définir des procédures de gestion du risque et des plans d'intervention ;
- k) mener des simulations d'audit de l'OACI pour évaluer le degré de conformité aux normes de l'Organisation relatives à la cybersécurité.

8.3 Oman a subi un audit OACI au cours du premier trimestre 2025 qui n'a donné lieu à aucune constatation, et a atteint un taux de conformité de 100 % aux dispositions de l'Annexe 17 et aux SARP relatives à la cybersécurité.

9. ENSEIGNEMENTS TIRÉS DE LA PHASE D'ANALYSE DES LACUNES ET DU PROGRAMME UNIVERSEL D'AUDITS DE SÛRETÉ — MÉTHODE DE SURVEILLANCE CONTINUE (USAP-CMA)

9.1 Il y a lieu de souligner l'importance cruciale de la coopération internationale et d'une gouvernance efficace, et de la mise en œuvre des dispositions de l'OACI pour assurer une approche uniforme et coordonnée en matière de cybersécurité partout dans le monde ; c'est un aspect fondamental, car les menaces contre la cybersécurité ne connaissent pas de frontières et peuvent avoir de profondes conséquences sur la sécurité et la sûreté de l'aviation civile.

9.2 De plus, l'analyse a abordé les défis d'ordre pratique auxquels les États et le secteur de l'aviation sont confrontés pour s'acquitter de leurs engagements dans le domaine de la cybersécurité, en mettant en lumière ces défis de même que la nécessité d'un soutien continu, de ressources et de formation pour aider toutes les parties à renforcer leurs capacités dans ce domaine.

9.3 Dans l'ensemble, l'analyse a révélé que le cadre de l'OACI constitue un pas en avant fondamental pour faire face aux risques de cybersécurité en constante évolution dans l'aviation civile, car il fournit un cadre global, des orientations et un soutien, dans le rôle vital que joue l'OACI dans la protection de la sécurité et de la sûreté de l'aviation civile.