



NOTE DE TRAVAIL

ASSEMBLÉE — 41^e SESSION

COMITÉ EXÉCUTIF

Point 14 : Sûreté de l'aviation — Politique

GOUVERNANCE DE LA CYBERSÉCURITÉ DANS L'AVIATION CIVILE

(Note présentée par Oman)

RÉSUMÉ ANALYTIQUE

La présente note traite de l'importance d'une gouvernance efficace pour assurer la protection de l'aviation civile contre les cyberattaques, facteur fondamental pour renforcer les processus de coordination et de communication visant à protéger l'aviation contre les cyberattaques.

Les cyberattaques sont mieux contrôlées en mettant en œuvre de manière efficace les exigences de la cybersécurité. La première étape de ce processus consisterait à demander à l'Autorité de l'aviation civile (AAC) qui est chargée de réglementer ce secteur de mettre en place une structure claire. Cette structure devrait comprendre la fonction de base de la réglementation (législation et supervision) ainsi que d'autres fonctions qui seront confiées à diverses parties prenantes.

Suite à donner : L'Assemblée est invitée à entériner les recommandations suivantes :

- a) demander instamment aux États, par le biais des autorités de l'aviation civile, de mettre en place et d'adopter une structure normalisée de gouvernance de la cybersécurité de l'aviation civile afin d'assurer une intégration harmonisée et appropriée des obligations internationales dans leurs cadres de réglementation nationaux, qui doivent protéger la sécurité et la sûreté de l'aviation civile contre les cyberattaques ;
- b) demander instamment aux États d'élaborer, de tenir à jour et de coordonner la mise en œuvre des spécifications relatives à la cybersécurité par l'entité compétente de l'Autorité de l'aviation civile chargée de la mise en œuvre des prescriptions de l'Annexe 17 à la Convention de Chicago ;
- c) fournir soutien, assistance et orientations aux États pour élaborer une structure normalisée de gouvernance de la cybersécurité de l'aviation.

<i>Objectifs stratégiques</i> :	La présente note se rapporte à l'objectif stratégique <i>Sûreté et facilitation</i> .
<i>Incidences financières</i> :	Les mesures à prendre indiquées dans la présente note doivent être entreprises sur la base de la disponibilité de ressources financières et humaines dans les États contractants. Ces mesures peuvent également être intégrées dans le Plan pour la sécurité de l'aviation dans le monde (GASeP).

¹ Version arabe fournie par Oman.

<i>Références :</i>	Stratégie de cybersécurité de l'aviation Annexe 17 – <i>Sûreté de l'aviation</i> Programme universel d'audits de sûreté – Méthode de surveillance continue (USAP-CMA) Doc 8973, <i>Manuel de sûreté de l'aviation de l'OACI</i>
---------------------	--

1. INTRODUCTION

1.1 La présente note vise à réaliser l'initiative *Aucun pays laissé de côté* de l'OACI en mettant en oeuvre la norme 2.1.2 de l'Annexe 17 – *Sûreté de l'aviation* : « Chaque État contractant établira une organisation, élaborera et mettra en application des règlements, pratiques et procédures pour protéger l'aviation civile contre les actes d'intervention illicite, en tenant compte de la sécurité, de la régularité et de l'efficacité des vols. »

1.2 La législation nationale élaborée sur la base des meilleures pratiques et en conformité avec la Convention de Chicago de 1944 et les normes et pratiques recommandées (SARP) de l'Annexe 17 relatives à la cybersécurité, ainsi que la Convention et le Protocole de Beijing de 2010, prévoient les dispositions les plus essentielles pour la réglementation de l'industrie et déterminent la manière dont les tâches et les responsabilités sont assignées au personnel pour protéger l'aviation civile contre les actes d'intervention illicite.

1.3 L'obligation internationale de renforcer la sûreté et la facilitation de l'aviation civile en introduisant des exigences au niveau national devrait suivre un plan clair et structuré, assurant ainsi l'établissement d'une législation nationale complète qui aiderait le personnel opérationnel à atténuer les risques et les menaces et protégerait les installations de l'aviation civile contre des actes d'intervention illicite.

1.4 L'élaboration de règlements et de procédures relatifs à la cybersécurité conformes aux prescriptions de l'Annexe 17 et aux dispositions relatives à la sûreté qui figurent dans d'autres Annexes à la Convention de Chicago est d'une importance capitale, car bon nombre d'aspects réglementaires et fonctionnels doivent être pris en compte conformément à l'environnement de travail créé par les AAC par le biais de la législation nationale. L'objectif visé est de s'assurer que lesdits règlements et procédures sont mis en oeuvre conformément à l'obligation internationale de renforcer la sûreté de l'aviation et de protéger le secteur contre les cyberattaques.

2. INTERDÉPENDANCE DES RÉSEAUX DE L'AVIATION

2.1 Le réseau d'informations de l'aviation civile est relié à plusieurs parties prenantes, notamment les fournisseurs de services de sûreté, les installations de navigation aérienne, les fournisseurs de services d'assistance d'escale, le fret aérien, les services de restauration, et d'autres entités opérationnelles et gouvernementales pertinentes. Les réseaux sont également reliés entre eux au niveau opérationnel en envoyant et en recevant des informations pertinentes.

2.2 Le secteur de l'aviation civile est de plus en plus tributaire de la technologie dans tous les aspects de son exploitation. Animées par le besoin de protéger l'industrie contre les cyberattaques, ce qui pourrait entraîner un risque grave pour cette industrie vitale, les AAC s'acquittent des fonctions réglementaires de législation et de supervision dans ce domaine pour veiller à ce que les activités soient

alignées sur les politiques et les méthodologies de l'OACI. À cette fin, elles doivent pouvoir attirer des ressources ayant l'expertise et les compétences nécessaires pour élaborer une législation relative à la cybersécurité et assurer convenablement le rôle de supervision

2.3 Le secteur de l'aviation dépend de plus en plus de la disponibilité de systèmes d'information, de communication et de surveillance. En conséquence, les AAC doivent accélérer l'élaboration de la législation et mettre en place un système de supervision qui exige que les parties prenantes protègent leurs systèmes en élaborant et en mettant en œuvre des mesures d'atténuation. Cela ne peut se faire que par une bonne coordination et une division appropriée des tâches et des responsabilités en matière de cybersécurité. Notamment, l'Annexe 17 prévoit une obligation internationale qui demande à l'entité de l'AAC chargée de la sûreté de l'aviation de promouvoir la cybersécurité.

3. GOUVERNANCE DE LA CYBERSÉCURITÉ

3.1 Il est absolument important d'avoir une bonne compréhension des rôles et des responsabilités liées à la cybersécurité du point de vue de la réglementation et de la supervision. L'objectif est d'établir un cadre opérationnel efficace et durable pour éviter tout chevauchement dans les fonctions et les responsabilités entre les entités concernées par la cybersécurité et pour se conformer à toutes les exigences afin de protéger le secteur contre les actes d'intervention illicite. La question a pris une importance majeure, surtout en ce moment où les cyberattaques constituent une menace émergente et une préoccupation majeure pour la communauté de la sûreté de l'aviation internationale.

3.2 Les AAC doivent accorder l'attention nécessaire à la sûreté de l'aviation civile en traitant des différentes préoccupations pour assurer un secteur aéronautique sécurisé, sûr, réglementé, économique et convivial. Cela se fera en élaborant un mécanisme de gouvernance réglementaire complet et en établissant des catalyseurs opérationnels qui protègent contre les cyberattaques avec les dernières technologies et les systèmes de communication les plus récents.

3.3 L'importance d'un tel cadre est maintenant d'autant plus évidente compte tenu de la nécessité de traiter du nombre de plus en plus grand de cybermenaces et de cyberattaques dans le monde et pour faire face à leur grande complexité et à leurs motivations diverses, tels que la criminalité organisée, les visées financières ou politiques, etc., maintenant que les entreprises et les institutions passent au domaine numérique par le biais de l'expansion de la numérisation, des services électroniques et de l'intégration entre institutions de par le monde, y compris entre les entités de l'aviation civile.

4. GOUVERNANCE DE LA CYBERSÉCURITÉ AU SEIN D'UNE AUTORITÉ DE L'AVIATION CIVILE (NIVEAU NATIONAL)

4.1 La régulation de la cybersécurité est une responsabilité qui incombe à l'entité compétente de la sûreté de l'aviation civile chargée de l'établissement et de la tenue à jour des systèmes de cybersécurité. La section des licences et de la supervision met en œuvre diverses activités d'assurance de la qualité. Par ailleurs, la section de l'évaluation des risques est chargée de l'évaluation des risques pour la cybersécurité².

² Exemple de structure d'une entité de sûreté de l'aviation

4.2 Les différents organes du secteur exécutent des opérations au jour le jour conformément aux exigences réglementaires en matière de cybersécurité.



5. NIVEAU OPÉRATIONNEL

5.1 Les entités opérationnelles doivent se conformer aux spécifications nationales, fixer des procédures d'exploitation normalisées et mettre en œuvre les mesures nécessaires pour protéger les informations critiques sur l'aviation civile et les systèmes et données de la technologie des communications.



— FIN —