



NOTE DE TRAVAIL

ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 18 : Développement des capacités et soutien à la mise en œuvre — Politique et activités

ÉLABORATION D'UN PROGRAMME DE FORMATION À LA
CYBERSÉCURITÉ ALIGNÉ SUR LES NOUVELLES LIGNES DIRECTRICES :
UNE PROPOSITION

(Note présentée par la République de Corée)

RÉSUMÉ ANALYTIQUE

L'analyse des statistiques récentes sur les cyberincidents dans l'aviation révèle que les cybermenaces sont devenues un **danger réaliste**. Pour faire face à ce constat, le Groupe d'experts de la cybersécurité est en train d'élaborer et de publier des orientations utiles fondées sur la **section 4.9 de l'Annexe 17 – Sûreté de l'aviation**. Cela étant, à l'heure actuelle, il n'existe qu'un seul cours de formation officiel de l'OACI à la cybersécurité. Pour renforcer les capacités de lutte contre ces menaces, réalistes, il faut s'appuyer sur l'éducation et la formation. Il est donc nécessaire d'inciter les États membres à mettre au point des programmes de formation fondés sur les lignes directrices en matière de cybersécurité, et l'OACI doit **normaliser** ces efforts.

Suite à donner : L'Assemblée est invitée à :

- prendre acte de la nature évolutive des cybermenaces qui pèsent sur l'aviation civile ;
- examiner les lignes directrices en matière de cybersécurité élaborées à partir des dispositions de la section 4.9 de l'Annexe 17 – *Sûreté de l'aviation* ;
- lancer l'élaboration de nouveaux programmes de formation, sous la direction de l'OACI, sur la base des lignes directrices en matière de cybersécurité.

<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 activités de l'OACI visées dans le projet de note de travail de l'Assemblée ci-joint devraient être entreprises dans le cadre des ressources disponibles dans le budget ordinaire 2026-2028 et/ou au moyen de contributions extrabudgétaires, selon les indications contenues dans le plan d'activités 2026-2028.
<i>Références :</i>	Doc 10184, <i>Résolutions de l'Assemblée en vigueur (au 7 octobre 2022)</i> A42-WP/12 <i>Cybersécurité dans l'aviation civile</i> A42-WP/13 – <i>Résultats du débat ministériel de haut niveau, Semaine de la sûreté 2024 de l'OACI, Mascate (Oman)</i>

1. INTRODUCTION

1.1 L'objectif des cyberattaques a récemment changé. Dans le passé, les malfaiteurs se concentraient sur le vol de renseignements personnels, par exemple nom des passagers, numéros de téléphone et numéros de cartes de crédit. Aujourd'hui, ils cherchent à perturber directement et concrètement l'aviation civile, notamment en paralysant les services de transport aérien ou en détraquant les systèmes de navigation aérienne.

1.2 Selon les données publiées par le Centre de réponse aux urgences informatiques du Système européen de gestion de la circulation aérienne (EATM-CERT), pour la période de douze mois allant jusqu'à la fin du premier semestre 2025, le type de cyberattaque le plus courant est le rançongiciel, qui représente 15 incidents sur 33 au total (environ 45 %), suivi par les cas de piratage informatique (sept) et les attaques par déni de service distribué (cinq). Les principales cibles étaient les transporteurs aériens avec 16 incidents (environ 48 %), suivies par les aéroports avec sept incidents, la chaîne d'approvisionnement avec sept incidents aussi et les autorités de l'aviation civile (AAC) avec trois incidents.

1.3 Le nombre de ces cas devrait continuer d'augmenter et, compte tenu du nombre important d'incidents non signalés, les cybermenaces doivent désormais être reconnues comme un danger réaliste et présent pour le secteur aérien.

2. ANALYSE

2.1 La section 4.9 de l'Annexe 17 – *Sûreté de l'aviation* indique qu'il faut déterminer les systèmes et données informatiques et de communication critiques utilisés aux fins de l'aviation civile et, conformément à une évaluation des risques, élaborer et mettre en œuvre, selon qu'il convient, des mesures pour les protéger des interventions illicites.

2.2 Avec sa réglementation nationale sur la cybersécurité, la République de Corée a satisfait aux normes pertinentes et aux conditions du Programme universel d'audits de sûreté – Méthode de surveillance continue (USAP-CMA), et de nombreux autres États membres devraient aussi être en mesure de respecter suffisamment ces normes.

2.3 En outre, le Groupe d'experts de la cybersécurité a élaboré et en partie publié plusieurs documents d'orientation au cours des quatre dernières années afin de renforcer les capacités en cybersécurité de l'aviation, facilitant ainsi leur application par les États membres.

2.4 Dans cette optique, le moment est jugé opportun pour mettre au point en parallèle une formation OACI appliquée aux lignes directrices en matière de cybersécurité. Il est en effet nécessaire d'étoffer les programmes d'éducation et de formation pour tenir compte de ces lignes directrices qui sont en cours d'élaboration ou qui ont déjà été publiées. (Il n'y a actuellement qu'un seul programme OACI de formation à la cybersécurité.)

3. CONCLUSION

3.1 L'analyse des statistiques des cinq dernières années et des données récentes montre qu'il faut reconnaître qu'il est temps de renforcer proactivement la résilience de la cybersécurité de l'aviation, car les cybermenaces qui pèsent sur l'aviation civile sont devenues une réalité.

3.2 Des lignes directrices sur la cybersécurité donnant suite aux recommandations figurant à la section 4.9 de l'Annexe 17 – *Sûreté de l'aviation* sont en cours d'élaboration et de publication, sous la houlette du Groupe d'experts de la cybersécurité. Il est nécessaire que tous les États membres déterminent ces lignes directrices et préparent des mesures d'ajustement institutionnel.

3.3 Pour cela, le besoin le plus important est de développer des programmes d'éducation et de formation à la cybersécurité. Le Groupe d'experts de la cybersécurité est en train d'élaborer des lignes directrices en matière de formation, mais il n'existe pour l'instant qu'un seul cours de formation officiel de l'OACI, et celle-ci devrait inviter en nombre les États membres à mettre au point des formations à la cybersécurité, puis à les normaliser.

— FIN —