

**PROJET DE DÉCLARATION DE MASCATE SUR LA SÛRETÉ
ET LA CYBERSÉCURITÉ DE L'AVIATION
Mascate (Sultanat d'Oman), 11 décembre 2024**

Nous, Ministres et Chefs de délégation, participant au débat ministériel de la Semaine de la sûreté de l'Organisation de l'aviation civile internationale (OACI), à Mascate (Sultanat d'Oman), le 11 décembre 2024, en présence de hauts représentants du secteur de l'aviation :

Rappelant les résolutions A41-18 et A41-19 de l'Assemblée de l'OACI qui consacrent la détermination générale des États à renforcer la sûreté et la cybersécurité de l'aviation ;

Affirmant que l'aviation connecte le monde, rapproche les peuples et les pays, et favorise le développement économique et social grâce au transport, au commerce et au tourisme, ce pour quoi elle doit être effectivement protégée ;

Confirmant l'importance d'une stratégie commune au sein des Nations Unies, faisant appel à la coopération et à la coordination entre tous les organes et toutes les institutions spécialisées compétentes des Nations Unies, pour bien comprendre que le secteur aéronautique est une infrastructure essentielle dont dépendent la sûreté, la prospérité et le développement sur le plan national, ainsi que l'économie mondiale ;

Constatant que la sûreté et la cybersécurité de l'aviation sont indispensables au développement durable du transport aérien et qu'elles doivent être en bonne place dans l'ordre des priorités et s'appuyer sur un financement adéquat ;

Soulignant la nécessité de ne pas baisser la garde, car l'absence d'incidents graves qui menacent la sûreté ou la cybersécurité de l'aviation ne signifie pas que le risque est moindre.

**EN CONSÉQUENCE, PRIONS INSTAMMENT LES ÉTATS, L'OACI,
LES ORGANISATIONS INTERNATIONALES ET RÉGIONALES,
LES ACTEURS DU SECTEUR ET AUTRES PARTIES PRENANTES :**

- a) De redoubler d'efforts pour faire face aux menaces émergentes et existantes pour l'aviation civile internationale, dont la menace interne et les cyberattaques ;
- b) D'appeler les États à ratifier la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* et le *Protocole additionnel à la Convention pour la répression de la capture illicite d'aéronefs* (Beijing 2010), comme moyen de dissuasion et de répression des attaques dirigées contre l'aviation civile ;
- c) D'accorder à la sûreté et à la cybersécurité de l'aviation le même niveau d'importance, le même degré élevé de priorité et les mêmes moyens que ceux qui sont accordés à d'autres pans de l'aviation civile ;
- d) De veiller à une coordination efficace de la sécurité, de la sûreté et de la cybersécurité de l'aviation afin de tirer parti de la mise en commun des connaissances et du renforcement des efforts ;
- e) De mobiliser suffisamment de ressources pour garantir la disponibilité de professionnelles et de professionnels qualifiés et compétents pour réglementer, piloter, gérer, maintenir et superviser la mise en œuvre effective de mesures relatives à la sûreté et à la cybersécurité de l'aviation ;
- f) D'adopter des politiques, des normes, des règles et des stratégies novatrices fondées sur les risques et axées sur les résultats, notamment la mise au point de systèmes de gestion et d'une supervision efficace visant à orienter la conception coordonnée de mesures durables en matière de sûreté et de cybersécurité de l'aviation ;

- g) De veiller à la communication immédiate d'informations afin de faciliter l'évaluation des risques qui menacent l'aviation, dont les cybermenaces, en prévenant et en atténuant ces menaces, en créant et en préservant un écosystème de l'aviation résilient, et en assurant une riposte et une reprise en cas d'incidents touchant l'aviation civile. Sur le plan technique, la communication d'informations devrait inclure tous les experts compétents ;
- h) De renforcer la coopération pour élaborer des éléments indicatifs harmonisés et complets en matière de sûreté et de cybersécurité de l'aviation ;
- i) De veiller à ce que les mesures de sûreté soient efficaces et qu'elles facilitent en même temps le flux des passagers et des marchandises ;
- j) D'assurer la mise en œuvre effective des normes de l'OACI et de s'efforcer de réaliser l'objectif ambitieux du Plan mondial pour la sûreté de l'aviation (GASep) de l'OACI et de tenir compte de ses six domaines d'intervention prioritaires ;
- k) De constater les compétences de spécialistes qui sont nécessaires pour exploiter et gérer les technologies de sûreté de l'aviation actuelles et nouvelles, et recruter et former le personnel qui les utilisera, tout en poursuivant les efforts pour attirer la prochaine génération de professionnelles et de professionnels de l'aviation, et promouvoir les politiques et les initiatives destinées à renforcer la diversité, l'équité et l'inclusion, notamment en comblant l'écart entre les sexes dans le secteur de l'aviation ;
- l) D'accélérer la mise en œuvre de la stratégie OACI pour la cybersécurité de l'aviation et son plan d'action pour la cybersécurité afin d'appuyer un cadre de cybersécurité de l'aviation mondial qui soit solide ;
- m) De prendre les devants pour recenser et contrer les cybermenaces qui pèsent sur l'aviation civile et encourager l'organisation de séances de formation et de sensibilisation régulières en matière de cybersécurité destinées au personnel de l'aviation afin de le doter des compétences nécessaires ;
- n) D'appuyer en amont les groupes régionaux en matière de sûreté et de cybersécurité de l'aviation et les programmes de coopération de l'OACI, comme le Plan régional de mises en œuvre complet pour la sûreté de l'aviation et la facilitation en Afrique (Plan AFI-SECFAL), le Programme de coopération pour la sûreté de l'aviation pour le Moyen-Orient (CASP-MID) et le Programme de coopération pour la sûreté de l'aviation pour l'Asie et le Pacifique (CASP-AP), qui sont essentiels pour aider les États à mettre en œuvre les normes de l'OACI et pour améliorer les gains d'efficacité opérationnelle ;
- o) De réaffirmer la valeur et l'importance de l'initiative *Aucun pays laissé de côté* de l'OACI qui vise à aider les États à s'aider eux-mêmes en assurant des services de formation, d'assistance et de renforcement des capacités ciblés et efficaces en matière de sûreté de l'aviation et de cybersécurité aux États qui en ont besoin.