



TREIZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 9 – 19 octobre 2018

COMITÉ A

Point 5 : Questions émergentes

5.4 : Cyberrésilience

CONSIDÉRATIONS RELATIVES À LA CYBERSÉCURITÉ EN AVIATION

[Note présentée par la Civil Air Navigation Services Organisation (CANSO), le Conseil international de coordination des associations d'industries aérospaceiales (ICCAIA), la Fédération internationale des associations de contrôleurs de la circulation aérienne (IFATCA) et la Fédération internationale des associations de pilotes de ligne (IFALPA)]

RÉSUMÉ ANALYTIQUE

La présente note fait état des positions de la CANSO, de l'ICCAIA, de l'IFATCA et de l'IFALPA au sujet de la nécessité, parmi les moyens indispensables pour accroître la résilience de l'aviation civile en matière de cybersécurité, d'élaborer un cadre mondial, harmonisé entre toutes les parties prenantes de l'aviation, pour l'échange d'information numérique fiable et sûre en aviation (un Cadre de confiance pour l'aviation), afin d'appuyer la modernisation de l'aviation à l'échelle mondiale. Plus précisément, la note exprime leur appui aux principes stratégiques proposés dans la note du Secrétariat de l'OACI AN-Conf/13-WP/27 et la nécessité d'élaborer les exigences en matière de politique et de gouvernance qui permettront une mise en œuvre sûre, compétente et abordable. Il est entendu que les détails techniques relatifs à la mise en œuvre seront définis une fois qu'un forum officiel de l'OACI aura été établi.

Suite à donner : La Conférence est invitée à approuver la recommandation figurant au paragraphe 3.2.

1. INTRODUCTION

1.1 Le secteur de l'aviation civile dans son ensemble évolue rapidement grâce à l'adoption de nouveaux concepts opérationnels qui, facilités par une large connectivité et les nouvelles technologies, permettent de rendre le trafic aérien plus sûr et plus ordonné. Ces efforts de modernisation de l'exploitation des vols promettent des avantages importants en optimisant l'usage de l'espace aérien. À mesure que la demande d'échanges de données interconnectés, dynamiques et fiables s'accroît, les avantages de cette évolution s'accompagnent d'une augmentation des risques de cybersécurité et

¹ Les versions française, anglaise, arabe, chinoise, espagnol et russe sont fournies par l'ICCAIA.

de la possibilité de cyberattaques menaçant la sécurité, la capacité de la navigation aérienne, l'efficacité des vols et les moyens opérationnels.

1.2 Face à ces changements, une nouvelle approche de bout en bout harmonisée à l'échelle mondiale, répondant au besoin de renforcer la cyberrésilience du système de l'aviation civile, doit être définie et ce, en englobant toutes ses parties prenantes. Cette approche doit prendre en compte les aspects techniques et de gouvernance et tirer profit des technologies et des méthodes disponibles dans le commerce pour satisfaire au besoin de rapidité et de bas coût de l'industrie. Au fur et à mesure de l'accroissement de la complexité des futurs systèmes aéronautiques, des méthodes et des stratégies modernes devront être adoptées pour créer un environnement mondial intégrant toutes les spécificités régionales ou locales. Ce défi ne peut être analysé fonctionnellement, comme par le passé, selon les éléments aéronefs/services de navigation aérienne/aérodromes, mais doit être traité comme une solution intégrée de bout en bout, prenant en compte les moyens horizontaux et transversaux et les risques de cybersécurité.

1.3 L'aviation civile doit adopter, entre autres, un cadre mondial harmonisé et convenu entre toutes les parties prenantes de l'aviation pour l'échange fiable et sûr d'information numérique en aviation (un Cadre de confiance pour l'aviation) tenant compte des sensibilités géopolitiques et financières de la communauté aéronautique.

2. ANALYSE

2.1 À une époque de grande connectivité entre les acteurs du système de l'aviation civile, l'objectif de résilience identifié dans le Plan pour la sûreté de l'aviation dans le monde (GASEP) et dans la note de travail du Secrétariat portant sur cette question ne pourra être atteint sans l'élaboration d'un cadre de confiance où seront énoncés les grands principes permettant d'assurer la confiance dans l'infrastructure aéronautique et dans l'information qui y est échangée (identité, intégrité, confidentialité et disponibilité). Un cadre de confiance est un facteur clé de la mise en œuvre d'une solution intégrée de bout en bout, efficace et efficiente, englobant toutes les parties prenantes connectées. Aujourd'hui, les parties prenantes consacrent beaucoup de temps et d'argent à gérer des interfaces externes et ont souvent une connaissance limitée du risque que représente chaque connexion externe. Les considérations ci-après décrivent les dimensions critiques de confiance et d'interopérabilité qui doivent faire l'objet de discussions et de décisions si l'on veut tirer les avantages de l'évolution du système tout en gérant les risques :

Gouvernance :

a) Établir des exigences minimales en matière de respect de la cybersécurité

Identifier le niveau minimal d'exigences acceptables en matière de cybersécurité et de normes communes permettant d'assurer une intégrité accrue. Un système de gestion des risques de cybersécurité doit être au cœur de cette démarche et doit être complété par des normes de l'industrie ouvertes et par une approche de conformité pour réaliser un cadre fiable.

b) Établir une inspection ou des méthodes de validation

La cybersécurité exige une démarche complémentaire aux évaluations de conformité physiques réalisées aujourd'hui. Le risque de cybersécurité évolue continuellement et la validation continue de la conformité aux normes d'exploitation en cette matière sera nécessaire. Une coopération mutuelle entre les partenaires connectés pour

valider et gérer le risque individuel aussi bien que le risque conjoint de bout en bout du système sera nécessaire au fur et à mesure de l'intégration entre les parties prenantes.

c) Politiques en matière de droit

À l'heure actuelle, l'industrie s'appuie sur des normes de sécurité physiques. L'évaluation des risques et la validation de la conformité en matière de cybersécurité doivent s'ajouter aux processus actuels et les organisations doivent maintenir un niveau acceptable de conformité dans ce domaine.

Considérations techniques :

Toutes les parties prenantes doivent être en mesure de mettre en place et d'exploiter leur système par les moyens les plus efficaces et les plus efficaces. Au fur et à mesure de l'intégration de la communauté, les solutions techniques peuvent devenir plus complexes et plus coûteuses. La modernisation de la structure technique et des normes mises en œuvre par toutes les parties prenantes doit être adaptée à chaque environnement, la normalisation devant assurer l'interopérabilité et la connectivité entre ces parties prenantes.

Le cadre doit :

- a) répondre à la demande croissante d'interconnectivité en utilisant les technologies les plus récentes, en favorisant l'utilisation de méthodes techniques communes, comme les certificats numériques, et d'attributs convenus entre les parties pour instaurer la confiance mutuelle.
- b) favoriser la confiance entre les parties prenantes qui adoptent un cadre commun associé à des normes, des protocoles et des technologies modernes disponibles dans le commerce.
- c) soutenir la création d'un environnement d'exploitation commun pour favoriser l'interconnectivité et l'échange d'information numérique. Les concepts visant à encourager cette évolution, comme le réseau de la Society for Worldwide Interbank Financial Telecommunication (SWIFT) utilisé par les banques dans le monde entier, et les enseignements tirés de l'expérience de l'industrie financière peuvent être utiles.
- d) réduire les coûts d'exploitation dans l'ensemble de la communauté mondiale pour un grand nombre de parties prenantes et favoriser l'accès à d'autres marchés.
- e) considérer l'adaptabilité et la modularité des moyens comme une façon d'actualiser et d'adapter rapidement le cadre en fonction de l'évolution de la technologie et de suivre l'évolution des auteurs de cyberattaques.

2.2 La normalisation crée un niveau commun de confiance dans l'exploitation des aéronefs et les services de la circulation aérienne dans le monde entier. La communauté de l'aviation civile ne dispose pas actuellement des normes nécessaires pour assurer à l'avenir la confiance mutuelle et la protection des échanges d'information numérique, des méthodes d'interconnectivité ni du processus de protection contre les risques mutuels. La mise en place d'un cadre commun d'échange d'information fondé sur des normes validées par toutes les parties permettra de gérer les risques et d'assurer le niveau nécessaire de confiance.

2.3 Avec un cadre de confiance commun, les grandes initiatives habilitantes de l'aviation civile identifiées dans le Plan mondial de navigation aérienne (GANP, Doc 9750) de l'OACI devraient être réalisées plus rapidement, grâce à la réduction de la complexité et des coûts, tout en ouvrant la porte aux moyens futurs nécessaires :

- a) intégration mondiale (par exemple SWIM, FF-ICE, etc.) de communications numériques sûres et fiables entre les acteurs de l'aviation civile ;
- b) modernisation des cadres de confiance existants pour permettre l'interopérabilité avec les anciens cadres ;
- c) regroupement du contrôle des nouveaux arrivants provenant de l'infrastructure ancienne plus lourde ;
- d) utilisation de l'effet de levier de l'identité, de l'intégrité et de la confidentialité pour améliorer d'autres moyens (par exemple, les données opérationnelles et de mission pour accroître l'efficacité).

2.4 Le cadre de confiance doit prendre en compte toutes les parties prenantes, dont le degré de maturité de la structure de gouvernance ou des moyens techniques pourra varier. Lors de la mise en œuvre du cadre, il faudra que les parties prenantes puissent évoluer peu à peu de façon fluide à partir des éléments traditionnels, alors que les nouveaux arrivants sur le marché devront s'intégrer rapidement et à un coût acceptable selon leurs propres objectifs opérationnels et commerciaux. La méthode de transition doit fournir une base commune à laquelle toutes les parties prenantes pourront accéder graduellement et être mise en place par étapes pour en réduire l'impact sur chaque partie prenante selon son niveau de maturité. Toutes devront assurer une intégration sûre et sans heurts au sein de l'espace aérien.

3. CONCLUSION

3.1 La Civil Air Navigation Services Organisation (CANSO), le Conseil international de coordination des associations d'industries aérospatiales (ICCAIA), la Fédération internationale des associations de contrôleurs de la circulation aérienne (IFATCA) et la Fédération internationale des associations de pilotes de ligne (IFALPA) préconisent, pour l'échange d'information numérique, l'élaboration d'un cadre de confiance pour l'aviation coordonné à l'échelle mondiale, qui sera un facteur clé pour faciliter la création d'un écosystème futur de l'aviation civile cyberrésilient. Compte tenu des moyens horizontaux et transversaux existants et des risques de cybersécurité, ce défi ne peut être analysé fonctionnellement, comme par le passé, selon les éléments traditionnels aéronefs/services de navigation aérienne/aérodromes, mais doit être conçu comme une solution intégrée de bout en bout.

3.2 La Conférence est invitée à approuver la recommandation suivante :

Recommandation 5.4/x – Cyberrésilience

Il est recommandé que la Conférence :

- a) demande à l'OACI de mettre sur pied un projet officiel, avec la participation des États et des organisations internationales, pour élaborer un cadre de confiance harmonisé et accepté à l'échelle mondiale selon les objectifs exposés dans la présente note ;

- b) demande à l'OACI d'élaborer une feuille de route, faisant appel à l'industrie et intégrée dans le GANP, pour mettre au point des moyens à la fine pointe de la technologie en vue de répondre aux besoins futurs de l'aviation civile en matière de cybersécurité (par exemple chaînes de blocs, infonuagique et autres technologies en évolution).

— FIN —