Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/197
TE/79
1/8/19

ASSEMBLÉE — 40e SESSION

COMMISSION TECHNIQUE

Point 30 : Autres questions à examiner par la Commission technique

CADRE DE CONFIANCE POUR UN ENVIRONNEMENT NUMÉRIQUE

(Note présentée par le Brésil)

RÉSUMÉ ANALYTIQUE

La croissance des infrastructures et des services numériques en aviation a apporté d'énormes avantages à l'élargissement de la capacité et à l'optimisation de l'espace aérien ; elle a cependant son lot de difficultés en termes d'interopérabilité et de cyber résistance. L'établissement d'un cadre de confiance est requis pour que l'aviation puisse être exploitée de façon homogène à travers les frontières internationales.

Suite à donner : L'Assemblée est invitée :

a) à demander à l'OACI de promouvoir le concept de cadre et de réseau mondial de confiance afin d'éviter les écarts d'exécution dans les activités des États et des régions;
b) à recommander à l'OACI de poursuivre les activités demandées par la 13e Conférence de navigation aérienne pour la création d'un cadre et d'un réseau de confiance afin d'échanger des informations de sécurité critiques;
c) à demander à l'OACI d'inclure dans le cadre de confiance des moyens logiques d'isoler la communauté aéronautique de l'internet public;
d) à demander à l'OACI de définir, avec l'appui de l'industrie aéronautique et d'autres secteurs, l'architecture et les besoins d'un réseau de confiance aux fins d'échange d'information dans un environnement numériquement connecté; et
e) à recommander aux États d'appuyer les activités d'établissement du réseau de confiance en fournissant les ressources nécessaires.

Objectifs stratégiques :	La présente note de travail se rapporte aux Objectifs stratégiques A – Sécurité, B – Capacité et efficacité de la navigation aérienne et C – Sûreté et Facilitation....
Incidences financières :	Formation du personnel, installation du matériel et des systèmes terrestres et aéroportés
Références :	Annexe 17 — Sûreté — Protection de l'aviation civile internationale contre les actes d'intervention illicite Doc 10075, Résolutions en vigueur de l'Assemblée (au 6 octobre 2016) Doc 9896, Manuel sur le réseau de télécommunications aéronautiques utilisant les normes et protocoles de la suite de protocoles Internet (IPS) Doc 9750, Plan mondial de navigation aérienne

1. INTRODUCTION

1.1 Nous vivons à l'ère de l'information. De plus en plus, les divers appareils et machines sont interconnectés dans un réseau complexe de données où les distances diminuent alors que la vitesse d'échange de messages augmente. Le monde rétrécit. Mais avec le développement de ces facilités, nous assistons à une multiplication de nouvelles menaces invisibles provenant de sources diverses à travers le monde.

1.2 Répondre à ces menaces constitue un des plus grands défis de nos jours, car elles sont diverses, omniprésentes et capables d'infliger de lourdes pertes tant en vies humaines qu'en coûts financiers.

1.3 Il est évident que, dans un monde de plus en plus interconnecté, l'aviation ne saurait échapper à un tel scénario. Malgré les nombreux systèmes analogues et isolés déjà en place, les nouvelles technologies mises en œuvre utilisent des informations numériques communiquées par des réseaux de données. Des concepts tels que le système mondial de navigation par satellite (GNSS), la surveillance dépendante automatique en mode diffusion (ADS-B), les communications contrôleur-pilote par liaison de données (CPDLC), les communications de données entre installations des services de la circulation aérienne (ATS) (AIDC), le réseau de télécommunications aéronautiques (ATN), la gestion des informations à l'échelle du système (SWIM), les systèmes d'aéronefs télépilotés (RPAS), etc. apportent d'énormes avantages à l'aviation, mais ils sont accompagnés de nouveaux problèmes à résoudre pour assurer la disponibilité, l'intégrité, la confidentialité et l'authenticité des informations transmises par ces services.

1.4 Pour mieux comprendre les risques inhérents aux nouveaux concepts, pour les réduire et les réglementer, la seule façon de procéder est de pratiquer une gouvernance solide. Et à cette fin, il faudra commencer par mettre sur pied un cadre de confiance capable de normaliser les procédures et les protocoles aux fins de la gestion et de l'intégration des infrastructures de réseaux et de services, aussi bien que de la protection contre les cyberattaques.

2. ANALYSE

2.1 Le cycle d'évolution technologique en aviation est relativement lent, mais le monde numérique a envahi de plus en plus les divers systèmes de communication, la navigation, la surveillance, la météorologie, la gestion du trafic aérien (ATM), la gestion des informations aéronautiques (AIM), etc. La numérisation de l'information, l'interconnections des réseaux et l'automatisation des services nécessitent une très bonne gouvernance afin d'assurer l'interopérabilité et la sûreté des opérations..

2.2 L'introduction même du concept SWIM en aviation inclura des normes, des infrastructures et des principes de gouvernance qui permettront de gérer des informations liées à l'ATM et leur échange entre participants qualifiés grâce à l'interopérabilité des services..

2.3 À cette fin, les divers réseaux de télécommunications aéronautiques des États devront être interconnectés pour assurer la circulation des informations. Chaque État sera responsable du déploiement et de l'exploitation de son infrastructure de réseaux et d'en assurer la sûreté, tout en se conformant aux normes afin d'offrir un fonctionnement homogène à travers les frontières.

2.4 Ces normes devront être élaborées suivant les principes de la Convention de Chicago, dans l'établissement d'un cadre de confiance capable de garantir à toutes les parties prenantes la sécurité des échanges d'informations dans un environnement numériquement connecté.

2.5 Il convient en outre d'envisager la nécessité pour tous les acteurs utilisant les services et les réseaux d'avoir un certificat numérique garantissant leur identification à l'échelle du globe.

2.6 La communauté aéronautique a toujours voulu s'isoler physiquement des réseaux externes, mais un tel souhait devient de plus en plus difficile à réaliser, car les données suivent de multiples voies différentes dans le monde ; l'OACI dispose cependant d'un moyen de garantir l'infrastructure si elle considère que le problème n'est pas local, ni même régional. C'est l'ensemble du système mondial qui doit être sécuritaire et résistant.

2.7 En outre, puisque le système mondial utilise l'infrastructure internet existante à des fins différentes, il est nécessaire que l'industrie participe aux activités de l'OACI, afin d'assurer l'isolement logique requis pour renforcer le degré de protection des réseaux de systèmes aéronautiques.

2.8 L'isolement logique peut être acquis de plusieurs façons, à condition d'assurer que, si un mauvais élément décidait de nuire au système de l'aviation dans l'espace cybernétique, il serait reconnu comme ne faisant pas partie de l'écosystème aéronautique et l'accès lui serait refusé. Ceci ajoutera une autre couche de protection au système, qui serait compatible avec les niveaux de sécurité convenus appliqués par la communauté de l'aviation.

2.9 Il faut bien admettre qu'aucun système ne peut être protégé à 100 %, mais avec l'isolement logique, un acteur malveillant aura plus de mal à pénétrer dans le système aéronautique. Un cadre de confiance, combiné à l'isolement logique d'un réseau, ne signifie pas nécessairement que tous les membres du réseau sont complètement fiables. Cela veut dire simplement que l'ensemble de la communauté a une idée de l'identité des participants et du rôle que chacun occupe dans le réseau. Outre l'isolement logique, une autre couche de protection consiste à établir un système d'identification dans un organisme de réglementation, plutôt que d'utiliser des milliers de systèmes d'identification répandus dans l'ensemble du secteur.

2.10 Durant la 13e Conférence de navigation aérienne, les participants ont examiné et convenu de la nécessité d'établir un cadre de confiance mondial et d'élaborer des dispositions de gouvernance et de politique en vue de créer un réseau de confiance. C'est maintenant au tour de l'OACI de collaborer avec les États et l'industrie aéronautique afin de faire progresser les tâches requises et de renforcer la sensibilisation concernant les cybermenaces contre la sécurité et la durabilité du transport aérien.

3. CONCLUSION

3.1 Les échanges d'informations numériques se développent rapidement et toutes les parties prenantes sont en train de mettre en place des mesures pour protéger leurs systèmes reliés numériquement contre les cybermenaces et assurer la résistance des systèmes de navigation aérienne.

3.2 Les participants nouvellement arrivés dans le système aéronautique appliquent rapidement des innovations technologiques et ils ont besoin d'un cadre mondial de confiance ainsi que d'un réseau de confiance pour appuyer la sécurité et l'efficacité de leurs exploitations et éviter toute incidence néfaste sur

la sécurité. Les fournisseurs de services de navigation aérienne doivent être prêts à répondre à ces exigences.

3.3 L'OACI sera également interpellée pour aider les États dans leurs efforts d'intégration, et cela pourrait faire intervenir des acteurs extérieurs à l'aviation qui gèrent des réseaux privés. Ils auront en outre besoin des directives de l'OACI pour résoudre ces questions en vue de l'harmonisation mondiale des procédures et de l'interopérabilité des systèmes.

— FIN —…