Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A41-WP/416[1]
EX/187
2/8/22

ASSEMBLÉE — 41e SESSION

COMITÉ EXÉCUTIF

Point 14 : Sûreté de l'aviation — Politique

MISE AU POINT D'UN iPACK POUR AIDER LES ÉTATS À METTRE EN ŒUVRE LA STRATÉGIE DE CYBERSÉCURITÉ DE L'OACI

[Note présentée par le Venezuela (République bolivarienne du) et appuyée par la Bolivie (État plurinational de), la Colombie, le Costa Rica, l'Équateur, le Panama et l'Uruguay][2]

RÉSUMÉ ANALYTIQUE

L'aviation mondiale est un système intégré très complexe qui repose sur des technologies de l'information et des communications essentielles à la sûreté et nécessaires à la protection de l'activité aéronautique civile. C'est pourquoi, y voyant une question d'importance vitale, l'OACI s'est dotée d'une stratégie de cybersécurité qui, par l'entremise de ses sept piliers, expose la nécessité d'une sensibilisation à la cybersécurité, qu'il convient d'approcher de manière transversale et interdisciplinaire pour l'intégrer à toutes les facettes de l'aviation civile. Les iPack de l'OACI comprennent des orientations, des instructions, des outils et un appui spécialisé qui permettent aux États de renforcer leur capacité de mettre en œuvre les normes et pratiques recommandées. À cet égard, il est important d'avoir des trousses iPack pour fournir aux États des conseils d'experts sur l'élaboration et la mise en œuvre de mesures de protection pour les systèmes informatiques et les données critiques utilisées dans l'aviation civile, ainsi que des lignes d'action utiles pour renforcer les capacités de contrer les cybermenaces.

Suite à donner : L'Assemblée est invitée à :
a) prendre note des renseignements figurant dans le présent document ;
b) demander au Conseil d'élaborer une trousse iPack qui vise à aider les États à accélérer la mise en œuvre de la stratégie de cybersécurité de l'OACI selon une logique multidisciplinaire, sachant son interdépendance, sa nature transversale et son importance pour la sûreté, la disponibilité, la continuité et la sécurité en général.

Objectifs stratégiques :	La présente note de travail se rapporte à l'objectif stratégique *Sûreté et facilitation*.
Incidences financières :	Il est proposé que les activités visées dans la présente note soient entreprises dans les limites des ressources disponibles dans le budget ordinaire pour la période triennale en cours et/ou au moyen de contributions extrabudgétaires.

[1] Version espagnole fournie par le Venezuela (République bolivarienne du).
[2] États membres de la région Amérique du Sud et de la Commission latino-américaine de l'aviation civile (CLAC).

Références :	Annexe 17 — *Sûreté* *Stratégie de cybersécurité de l'aviation*

1. INTRODUCTION

1.1 L'aviation mondiale est un système intégré très complexe qui repose sur des technologies de l'information et des communications essentielles à la sûreté et nécessaires à la protection de l'activité aéronautique civile. Le caractère critique et vulnérable de ces technologies fait qu'il est toujours plus important de les protéger contre les attaques délibérées ou les incidents qui mettent en péril l'offre d'activités et de services et leur continuité.

1.2 Compte tenu de l'interdépendance des processus de l'aviation civile et donc de tous les moyens informatiques qui les sous-tendent, la mise en œuvre de la stratégie de cybersécurité de l'OACI est d'une importance vitale, car ses sept piliers permettent une sensibilisation à la cybersécurité et une reconnaissance de cette importance en utilisant une approche transversale et interdisciplinaire qui intègre la question à toutes les facettes de l'aviation civile.

1.3 Il est donc essentiel d'accélérer la mise en œuvre de la stratégie dans tous les États membres et de chercher à l'insérer dans un cadre unique permettant la gestion des cyberrisques et le renforcement de la cybersécurité dans le secteur aéronautique.

2. ANALYSE

2.1 La série de trousses d'assistance (les « iPack ») que l'OACI met à la disposition des États pour les appuyer dans la mise en œuvre effective de normes et pratiques recommandées, de politiques, de stratégies, de plans et de programmes à l'aide d'éléments indicatifs et de cours de formation spécialisés donnés par des experts témoigne de l'effort de coordination de l'OACI. C'est là une initiative qui a obtenu des résultats considérables et tangibles à l'échelle mondiale.

2.2 Les iPack qui existent déjà abordent des questions prioritaires pour les États et le secteur aéronautique, comme la sécurité et la sûreté de l'aviation, la santé publique, la facilitation au service des passagers, les aéroports, les services de navigation aérienne ou les aspects économiques du transport aérien. Cependant, il n'existe toujours pas de textes d'orientation, de formation, d'outils ou d'expertise liés à la mise en œuvre de la stratégie de cybersécurité de l'OACI selon une approche multidisciplinaire, qui permettrait d'aborder de manière logique, ordonnée et cohérente chacun des piliers et des domaines qui composent le système de l'aviation civile et de reconnaître leur interdépendance et les facteurs de risque associés susceptibles d'affecter et de perturber la continuité et la sécurité dans son ensemble.

2.3 Il est donc proposé d'élaborer une nouvelle trousse d'assistance (iPack) qui aidera les États à accélérer la mise en œuvre de la stratégie de cybersécurité de l'OACI à l'aide d'outils et de conseils d'expert favorisant l'adoption de pratiques exemplaires propres à assurer la protection des systèmes informatiques et des données critiques utilisées dans l'aviation civile, ainsi que de lignes d'action utiles pour renforcer les capacités des États de contrer les cybermenaces.

3. CONCLUSION

3.1 L’aviation civile est un système très complexe qui repose sur des technologies essentielles pour un fonctionnement sûr, et donc à protéger. La stratégie de cybersécurité de l’OACI touche à un aspect vital de l’aviation civile et est axée sur une approche transversale et interdisciplinaire qui intègre la question à toutes les facettes de l’aviation civile.

3.2 À cet égard, il importe que les États disposent de conseils d’experts pour l’élaboration et la mise en œuvre de mesures permettant de protéger les systèmes informatiques et les données critiques utilisés dans l’aviation civile, ainsi que de lignes d’action utiles pour renforcer les capacités des États de contrer les cybermenaces.

— FIN —