



NOTE DE TRAVAIL

QUATORZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 26 août – 6 septembre 2024

Point 4 : Hyperconnectivité du système de navigation aérienne

4.2 : Cybersécurité et résilience des systèmes d'information

**ÉQUIPE D'INTERVENTION EN CAS D'ATTEINTE À LA SÉCURITÉ INFORMATIQUE
(CSIRT) POUR L'AVIATION CIVILE**

(Note présentée par la Colombie)

RÉSUMÉ ANALYTIQUE

Les équipes d'intervention en cas d'atteinte à la sécurité informatique (CSIRT) offrent des solutions d'intervention en matière de sécurité informatique à des entités qui prennent des décisions en temps réel en prévision ou en réponse à un cyberincident, leur permettant d'agir immédiatement et de reprendre leurs activités le plus rapidement possible. Pour les infrastructures critiques, la plupart des pays disposent d'équipes CSIRT qui relèvent de l'autorité nationale en matière de cybersécurité. Cependant, les secteurs nationaux du transport aérien ne disposent pas toujours de cette possibilité. Il convient de créer urgemment une équipe CSIRT propre à l'aviation civile.

Le secteur de l'aviation civile a la responsabilité d'assurer la sécurité des opérations et des passagers. Il dépend d'une couche d'infrastructure technologique considérée comme critique pour l'information et les opérations et nécessite une surveillance 24h/24 et 7j/7 pour anticiper les cybermenaces.

C'est pourquoi l'OACI devrait établir un cadre de référence afin de fournir des orientations et d'établir des procédures permettant aux pays de mettre en place une équipe CSIRT pour l'aviation civile.

Une équipe CSIRT pour l'aviation civile doit être dotée d'une structure de gouvernance appropriée et être conforme aux normes internationales en matière de cybersécurité. Elle devrait aider les États à élaborer la stratégie de cybersécurité de l'aviation civile proposée par l'OACI au moyen des outils, du personnel et des processus essentiels à l'atteinte de cet objectif.

Compte tenu de ce qui précède, nous proposons que l'OACI publie des orientations sur la création d'une équipe CSIRT propre à l'aviation civile, ainsi que des procédures connexes, qui serviraient de fil conducteur entre les ressources humaines et technologiques en matière de cybersécurité des parties prenantes du secteur de l'aviation civile dans chaque pays.

Suite à donner : La Conférence est invitée à recommander que l'OACI élabore des orientations et des procédures à l'intention de tous les États membres sur la création d'une équipe CSIRT pour l'aviation civile, et en attribue les fonctions, sous la tutelle de l'Organisation.

¹ Version espagnole fournie par la Colombie

1. INTRODUCTION

1.1 La Stratégie de cybersécurité de l'OACI tient compte de la dépendance croissante à l'égard des systèmes informatiques et de l'importance d'assurer l'intégrité, la confidentialité et la disponibilité de l'information pour un développement sécurisé du secteur. Les cybermenaces qui pèsent sur l'aviation civile sont en constante évolution et mettent en péril la sécurité et la continuité des opérations. Les menaces peuvent reposer sur des motifs politiques, financiers, terroristes ou autres. En réponse à la diversité des menaces, un cadre de référence a été établi, qui repose sur sept piliers :

- a) coopération internationale ;
- b) gouvernance ;
- c) lois et règlements effectifs ;
- d) politiques en matière de cybersécurité ;
- e) partage de l'information ;
- f) gestion des incidents et planification des interventions d'urgence ;
- g) renforcement des capacités et formation ;
- h) culture de la cybersécurité.

2. ANALYSE

2.1 Le secteur de l'aviation civile et ses parties prenantes comprennent les aéroports, les communications, la navigation et la surveillance (CNS), et les fournisseurs de services de gestion du trafic aérien (ATM), de services de gestion du trafic de systèmes d'aéronef non habité (UTM) et de services météorologiques (MET), les fabricants et les distributeurs d'équipements, les organismes de maintenance et les entreprises de transport aérien, qui sont tous interconnectés par les technologies de l'information et de la communication. Cette situation complique le traitement et la gestion sécurisés des données et des informations, ce qui présente un risque pour la sécurité des vies humaines. C'est pourquoi le travail d'équipe, la coordination et le partage de renseignements sur les menaces devraient avoir lieu entre les parties prenantes et entre les États souverains.

2.2 Ces derniers disposent d'agences et/ou d'entités responsables de la politique de cybersécurité au niveau le plus stratégique, dont le travail est effectué par des équipes d'intervention informatique d'urgence (CERT). Aux niveaux inférieurs, les équipes CSIRT sectorielles coordonnent et adoptent des protocoles d'intervention en cas de cyberincidents, surtout dans les entités et/ou les secteurs dotés d'infrastructures critiques. L'aviation civile constitue un tel secteur et il serait donc logique de mettre en place une équipe CSIRT spécialisée.

2.3 Compte tenu de ce qui précède, nous proposons que l'OACI élabore des orientations pour la création d'une équipe CSIRT de l'aviation civile, ainsi que des procédures, dans chaque État, dans le but commun d'améliorer la posture de cyberrésilience de l'aviation civile.

3. CONCLUSION

3.1 La Conférence est invitée à accepter les recommandations suivantes :

Recommandation 4.2/x – Orientations sur la création d’une équipe d’intervention en cas d’atteinte à la sécurité informatique dans l’aviation civile (CSIRT) et de procédures connexes

L’OACI est invitée à élaborer des orientations et des procédures à l’intention de tous les États membres sur la création d’une équipe CSIRT pour l’aviation civile, et en attribuer les fonctions, sous la tutelle de l’Organisation.

— FIN —