ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

Quatrième réunion du Sous-groupe Gestion de l'infrastructure et de l'information de l'APIRG (IIM/SG4)

(Réunion virtuelle, 31 août - 3 septembre 2021)

Point 4 de l'ordre du jour : ***État d'avancement de la mise en œuvre des projets régionaux adoptés par l'APIRG***

WP4.2E - Rapport d'étape du projet IIM SG COM 5 « Évaluation de la cyber-résilience des services de la navigation aérienne de l'AFI

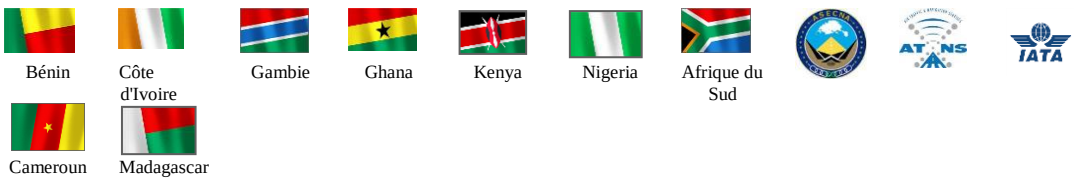
'Document présenté par la Côte d'Ivoire)

RÉSUMÉ
Le présent document de travail présente les progrès du projet IIM SG COM 5 « Évaluation de la cyber-résilience des services de la navigation aérienne de l'AFI » et les défis rencontrés. L'action attendue de la réunion au paragraphe 3.
REFERENCES : ▪ Plan mondial de navigation aérienne (GANP) ▪ Rapport de la 3ème réunion de l'CPP (IIM SG/4 de l'APIRG) ▪ Stratégie de la cybersécurité de l'OACI ▪ Plan d'action de la cybersécurité de l'OACI
Le présent document de travail est lié aux Objectifs stratégiques suivants de l'OACI : A – Sécurité, et B - Capacité et efficacité de la navigation aérienne **KPI et Modules B0 de l'ASBU concernés :** Tous ceux applicables à la CNS et au Spectre.

1. INTRODUCTION

1.1 Le projet IIM SG COM 5 a été lancé fin 2017 pour traiter la cyber-sécurité et la cyber-résilience des systèmes de navigation aérienne et de gestion de l'information dans la région AFI.

1.2 L'équipe du projet est composée d'experts en TIC, en cybersécurité et en ANS des États et organisations de l'AFI :



1.3 Le présent document présente les progrès réalisés par le projet de Plan directeur de l'IIM. Il détaille les réalisations, les défis rencontrés par l'équipe et les recommandations éventuelles.

2. DISCUSSIONS

2.1 Portée

2.1.1 Les objectifs du projet IIM COM 5 sont les suivants :

- évaluer les cyber-menaces pour les systèmes de navigation aérienne.
- promouvoir la cybersécurité et une culture de résilience parmi les parties prenantes dans la région AFI :
    - les CAA chargées de la supervision des ANSP,
    - Les ANSP fournissant des services devant être protégés contre les cyber-attaques ; et
    - les contreparties opérant à proximité d'aéroports (telles que les compagnies aériennes, les exploitants d'aéroport, etc.) et pouvant interagir avec des logiciels susceptibles d'affecter les ANS en termes de cyber-risques.
- élaborer un cadre de cyber-résilience (directives) pour l'utilisation volontaire par les organisations/États membres ANSP de l'AFI pour:
    - harmoniser la manière dont la cyber-résilience et la sécurité sont mises en œuvre et renforcer la capacité de chaque État membre à élaborer une politique de cyber-résilience des ANS.

2.2 **Actions menées** (Principales réalisation)

2.2.1 Documents du projet

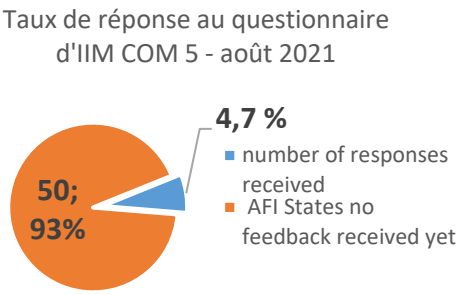
2.2.1.1 Tous les documents de lancement/planification du projet (description du projet, termes de référence et organisation/plan), soumis en 2019, avaient été mis à jour en 2021 (joints en Annexes A, B et C).

2.2.1.2 La matrice des liens entre les projets et l'estimation des coûts des projets sont en cours d'élaboration et devraient être finalisées d'ici la fin septembre 2021.

2.2.1.3 Une plateforme collaborative a été mise en place pour le projet sur les équipes Microsoft afin de partager toutes les conversations, les fichiers et les résultats attendus du projet.

2.2.2 Évaluation de la cyber-résilience actuelle des ANS dans la région AFI *(questionnaires de base du projet)*

Le principal défi auquel le projet est confronté est lié à l'enquête du projet par questionnaire et aux réponses des États (peu de réponses reçues à ce jour).



2.2.3 Cadre de la cyber-sécurité et de la cyber-résilience de l'ANS de l'AFI

2.2.3.1 Pour rappel, le cadre de cybersécurité et de résilience de l'ANS de l'AFI donne des lignes directrices générales sur la manière d'évaluer les risques, les menaces et la vulnérabilité en matière de cybersécurité des services de la navigation aérienne et des méthodes d'atténuation de ces risques. Ce cadre est basé sur la Stratégie de cybersécurité de l'aviation et sur les normes et cadres de cybersécurité éprouvés (série ISO 27000, NIST, etc.) Le cadre de cybersécurité et de résilience de l'ANS, soumis au Président et au Secrétariat du Sous-groupe IIM en février 2020, est en cours de mise à jour pour en assurer l'alignement sur la Stratégie de cybersécurité de l'aviation, le Plan d'action de cybersécurité de l'OACI et les initiatives actuelles de cybersécurité de l'aviation (en tenant compte de ce qui est pertinent/approprié pour la région AFI).

2.2.4 Campagne de sensibilisation à la cybersécurité et à la résilience de l'ANS

2.2.4.1 L'équipe du projet élabore un plan de communication destiné à sensibiliser à la cybersécurité et à la résilience.

2.2.4.2 Ce plan de communication doit inclure :

- Une sélection de quelques messages courts et clés sur la cybersécurité/résilience de l'aviation civile, devant être présentés sur une seule diapositive. Ces messages pourraient également être affichés sur le site Web de l'IACI (voir Secrétariat de l'IIM SG).
- Élaboration d'un dépliant électronique sur les conseils de base en matière de cybercriminalité, d'affiches de sensibilisation à la cyber-sécurité et de contenus visuels.

2.3 **Suite à donner** (Aperçu de la prochaine période devant être couverte par le prochain rapport)

2.3.1 Objectif n° 1 : « Concrétiser les choses » :

2.3.1.1 l'équipe du projet a organisé plusieurs réunions avec l'industrie (avec une grande expertise dans la gestion de la circulation aérienne et la cybersécurité de l'aviation).

2.3.1.2 Avec l'aide de l'industrie, ou d'autres partenariats dans le monde, les actions/tâches suivantes ont été identifiées et seront planifiées au cours du 2ème semestre 2021 :

a) élaborer des scénarios concrets de cyber-attaques qui susciteront des réactions spécifiques de la part des organisations/États, grâce à ces simulations de scénarios
b) fournir des exemples réels de cyber-attaques (combinaison d'approches informatiques et télématiques)
c) organiser des séminaires ou des webinaires (par exemple pour les cadres supérieurs), partager la culture de la cybersécurité, former, sensibiliser les gens (comment éduquer les gens à être conscients des menaces) et renforcer les capacités de réponse aux cyber-menaces pour les systèmes informatiques soutenant les opérations de l'ATM.

2.3.2 Objectif n° 2 : « Finaliser les principales activités du projet » d'ici novembre 2021 : cadre et évaluation de la cyber-résilience actuelle des de l'ANS de l'AFI

d) Mettre à jour la Cyber sécurité et la résilience de l'ANS de l'AFI avec les derniers apports/informations du Groupe de travail sur les systèmes de la navigation aérienne (WG-ANS) du Groupe d'étude sur la cybersécurité (SSGC) du Secrétariat de l'OACI, les initiatives de la CANSO, de l'IATA et d'EUROCONTROL.
e) finaliser l'enquête du questionnaire de base du projet (plus de réponses nécessaires).
f) finaliser le lien entre les projets IIM et AAO
g) élaborer une estimation des coûts du projet avant la prochaine réunion de l'APIRG.

2.3.3 Objectif n° 3 : « Communiquer sur la cyber-résilience de l'ANS (pour sensibiliser) » d'ici octobre 2021

3. MESURES ATTENDUES DE LA RÉUNION

3.1 La réunion est invitée à :

a) Prendre note des progrès réalisés à ce jour par l'équipe du projet et des défis rencontrés.
b) Encourager la participation des États aux projets de la région AFI.
c) Soutenir les actions concrètes déjà entreprises ou en cours par les États et les organisations pour répondre aux cyber-attaques contre les systèmes informatiques soutenant la gestion de la circulation aérienne, et
d) Soumettre les réponses aux Questionnaires des projets.

----- FIN -----