Vingt-et-unième réunion du Groupe régional AFI de planification et de mise en œuvre (APIRG/21)
(Nairobi, Kenya, 9 – 11 octobre 2017)

Point 5 de l'ordre du jour : Carences régionales de navigation aérienne

5.2. Initiatives de l'Industrie et autres questions de navigation aérienne

Cyber Sécurité &Résilience des services de navigation aérienne

(Note présentée par le Secrétariat)

SOMMAIRE

La présente note de travail expose les menaces et les défis rencontrés dans le domaine de la Sécurité et la résilience systèmes de navigation aérienne dans la région AFI et appelle à l'élaboration des politiques de prévention et d'atténuation, ainsi que l'identification et la mise en œuvre des mesures appropriées afin de minimiser l'impact de ces menaces.

La suite à donner figure au paragraphe 3.

RÉFÉRENCES :

- Annexe 17 — *Sûreté - Protection de l'aviation civile internationale contre les actes d'intervention illicite*
- Doc 9750, *Plan mondial de navigation aérienne, 5e édition*
- Doc. 9854, *Concept opérationnel de l'ATM*
- Doc 8973–Diffusion restreinte, *Manuel de la Sureté de l'Aviation*
- Circ. 330, *Coopération Civile/Militaire dans la gestion du trafic aérien*
- Doc 9855, *Lignes directrices sur l'utilisation d'Internet dans les applications aéronautiques*

Objectifs stratégiques et KPI de la Stratégie ASBU :

Objectifs stratégiques: A – *Sécurité,* **B** – *Capacité et efficacité de la navigation aérienne,* ***C*** *– Sûreté*

PIA et modules du Bloc 0 de l'ASBU : Tous les PIA et modules applicables à CNS et l'ATM

1. INTRODUCTION

1.1 La croissance ininterrompue du trafic aérien nécessite la mise en place d'infrastructures et de systèmes de plus en plus complexes avec un échange accru d'informations entre les différentes parties prenantes.

1.2 Les infrastructures et les systèmes ATM sont utilisés afin de tirer avantage de la flexibilité et de l'efficacité-coût des technologies émergentes ouvertes disponibles basées sur les protocoles Internet. Toutefois, ces technologies ouvertes accroissent aussi la vulnérabilité aux cyber-attaques associées aux systèmes ANS connectés.

1.3 Par conséquent, il est important pour les Etats de la région AFI de s'assurer que les risques et menaces de cyberattaque qui pèsent sur les systèmes de navigation aérienne sont atténués à travers la mise en place d'un cadre réglementaire approprié et l'identification et la mise en œuvre de mesures appropriées par toutes les parties impliquées dans la fourniture ou l'exploitation des services de navigation aérienne.

2. DISCUSSION

2.1 L'efficacité dans la fourniture des services de navigation aérienne du futur est basée sur l'échange et la gestion à l'échelle mondiale des informations utilisées par les divers processus et services ATM.

2.2 Le Plan mondial de navigation aérienne (**GANP Doc. 9750**) a été élaboré dans le cadre du concept de la Stratégie d'amélioration par blocs des systèmes de l'aviation (**ASBU**) composée de liens avec plusieurs éléments dont la mise en œuvre de certains accorde la priorité à l'échange d'informations :

a) **B0-FICE : Interopérabilité, efficience et capacité accrues grâce à l'intégration sol-sol** pour améliorer la coordination entre les organes des services de la circulation aérienne (ATSU) en utilisant les communications de données entre installations des services de la circulation aérienne (**AIDC**) définies par le Document 9694 de l'OACI ;

b) **B0-DATM** : **Amélioration des services grâce à la gestion des informations aéronautiques numériques** avec introduction du traitement et de la gestion numériques de l'information aéronautique par la mise en œuvre de l'AIS/AIM, en utilisant le modèle AIXM, la transition à la publication électronique d'information aéronautique (eAIP) et l'amélioration de la qualité et de la disponibilité des données ;

c) **B1-DATM : Amélioration du service grâce à l'intégration de la totalité de l'information ATM numérique** pour une intégration accrue des informations et appuyer un nouveau concept d'échange d'information ATM favorisant l'accès en ligne d'outils basés sur les protocoles et les modèles d'échange tels que l'**AIXM, FIXM, IWXXM**;

d) **B1-SWIM: Amélioration des performances par l'application de la gestion globale de l'information (SWIM)** pour créer l'intranet de l'aviation, basé sur des modèles normalisés de données, et des ***protocoles internet*** afin de maximiser l'interopérabilité

2.3 Cet échange d'informations mondial, tout en améliorant l'efficacité, la capacité et la flexibilité des opérations et augmentant la productivité, accroit la vulnérabilité aux cyber-attaques comme la tendance est d'utiliser des technologies émergentes ouvertes disponibles.

2.4 Les menaces et les vulnérabilités qui pèsent sur le système ANS sous forme de cyberattaques vont s'accroître puisque les systèmes actuels et futurs qui vont être mis en œuvre, nécessitent l'échange accru d'informations faisant recours à des **technologies de l'information accessibles au grand public**, **un réseau partagé** et des infrastructures informatiques .

2.5 La menace est à la fois très réelle, grave et susceptible d'émaner de diverses sources internes ou externes étant donné que les infrastructures des systèmes ATM sont composes de personnes, de procédures, des informations, de ressources, d'installations (***Unités des services de la circulation aérienne*** *et* ***aéroports***), d'équipement (***Communications, Navigation, et Surveillance (CNS)***). Par conséquent, dans le cadre du Programme national de sûreté de l'aviation civile, les Etats et les opérateurs doivent élaborer et mettre en œuvre des stratégies et des plans de sûreté afin d'assurer la continuité des opérations en dépit de la menace qui peut affecter la sécurité et la résilience du système de la navigation aérienne.

Coordination au niveau national

2.6 Plusieurs documents OACI abordent de la sûreté de l'ATM. Dans la Circulaire 330 de l'OACI sur la Coopération Civile/Militaire dans la gestion du trafic Aérien, la Sureté de l'ATM est définie comme étant : « ***La contribution du système ATM à la sûreté de l'aviation civile, à la sécurité et à la défense nationales et à l'application de la loi, ainsi qu'à la protection du système ATM contre les menaces à la sûreté et les vulnérabilités*** ».

2.7 La sûreté de l'aviation relève de la responsabilité des États. À cet égard, l'Annexe 17 (**3.1.1**) dispose : « ***Chaque État contractant établira et mettra en œuvre un programme national écrit de sûreté de l'aviation civile destiné à protéger les opérations de l'aviation civile contre les actes d'intervention illicite, au moyen de règlements, de pratiques et de procédures qui tiennent compte de la sécurité, de la régularité et de l'efficacité des vols*** ».

2.8 Dans le cadre du Programme national de sûreté de l'aviation civile, il incombe aux États (Annexe 17 – 4.9.1 et 4.9.2) « *de veiller à ce que des mesures appropriées soient élaborées pour* ***protéger la confidentialité, l'intégrité et la disponibilité des systèmes et données informatiques et de communications critiques utilisés*** *aux fins de l'aviation civile contre des interventions qui peuvent compromettre la sécurité de l'aviation civile et d' encourager les entités qui participent à la mise en œuvre de divers aspects du programme national de sûreté de l'aviation civile, ou qui en sont chargées, à* ***identifier leurs systèmes et données informatiques et de communications critiques****, y compris les* ***vulnérabilités*** *de ces systèmes et les* ***menaces pesant sur eux****, et d'élaborer et* ***mettre en œuvre des mesures de protection****, notamment en matière de* ***sûreté intégrée****, de* ***sûreté de la chaîne d'approvisionnement****, de* ***séparation des réseaux*** *et de* ***contrôle d'accès à distance****, selon qu'il convient* ».

2.9 Le *Manuel de sûreté de la gestion du trafic aérien* (Doc 9985-AN/492 — Diffusion restreinte) dispose que *« la protection des infrastructures du système ATM renvoie à la protection des infrastructures du système ATM à travers la sûreté des informations et des communications, la sûreté physique, et la sûreté du personnel. Il concerne aussi la continuité du service lors des urgences ou des catastrophes.*

Par conséquent, le programme de sûreté de l'ATM pour la protection des infrastructures doit comporter les aspects suivants :

a) Sûreté physique ;

b) Sûreté du personnel ;

c) ***Sûreté des technologies de l'information et de la communication (TIC)*** *;*

d) Planification des mesures d'urgence pour répondre aux questions de sûreté pour la reprise après les sinistres et la continuité des opérations ».

2.10 Avec des parties prenantes multidisciplianires, la mise en œuvre de la sécurité et la résilience de la gestion du trafic aérien nécessite une étroite collaboration entre les entités nationales. Bien que la question de la sûreté nationale de l'aviation soit abordée dans le cadre de l'AVSEC, l'élaboration de politiques et stratégies nationales pour résoudre la question de la sûreté de l'ATM, surtout la composante sécurité et résilience, manque de visibilité dans la région AFI.

2.11 Par conséquent, il est souhaitable de créer clairement un cadre national (réglementation, politique, stratégie et plan) pour la prise en compte de cette question dans le Programme national de sécurité de l'aviation civile

Coordination internationale

2.12 L'exploitation de l'ATM sans discontinuité dans la région AFI nécessite l'interconnexion et l'interopérabilité des systèmes (CNS/ATM) ce qui peut engendrer des cyberattaques internationales, d'où la nécessité d'une coopération de haut niveau entre les États bien que la sûreté relève de la responsabilité des États.

2.13 L'autorité responsable de la sûreté de l'aviation civile doit assurer la coordination des procédures avec les autorités compétentes des États voisins, et des accords doivent être conclus pour l'échange des informations de sûreté. Les centres ATS doivent déjà avoir conclu des lettres d'accord avec des organes ATS voisins au sein d'un même Etat ou situés dans des Etats différents et détaillant les procédures pour les communications et la coordination. Si ces lettres n'abordent pas encore les procédures liées au cyber Sécurité et Résilience, elles doivent être mises à jour dans le cadre de la planification des procédures de sûreté de l'ATM.

2.14 Cette approche collaborative et coopérative est nécessaire afin d'assurer que les politiques et les instruments de sûreté de la gestion et l'ATM sont susceptibles de faire face à un large éventail d'actes d'interférence illicite, de terrorisme et d'autres événements qui font peser des menaces sur les installations et les systèmes ou pourraient nuire à la capacité du système ATM à fournir les services.

3 SUITE À DONNER PAR LA RÉUNION

3.1 La réunion est invitée à :

a) Prendre acte des informations fournies dans la présente note de travail et mettant en évidence l'importance de la sûreté de l'ATM, surtout la cyber sécurité et la Résilience de l'ATM, dans la région AFI ;

b) Encourager les États qui ne l'ont pas encore fait à élaborer un cadre national (réglementation, politique, stratégie et plan) afin d'inclure cette question dans le Programme national de sûreté de l'aviation civile ;

c) Exhorter les États à mettre en place et maintenir des procédures de coordination avec les Etats voisins afin d'assurer que les politiques et dispositions de gestion de la sûreté de l'ATM pourront s'opposer à toute un éventail d'actes d'intervention illicite, surtout ceux liés aux cyberattaques ;

d) Prier l'OACI de maintenir son appui à travers la fourniture des outils d'orientation, la formation, des ateliers/séminaires sur la sûreté de l'ATM, surtout la cyber Sécurité et la résilience de l'ATM. .

-FIN-