Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

AN-Conf/13-WP/282
27/9/18
Français et anglais, seulement[1]

TREIZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 9 – 19 octobre 2018

COMITÉ A

Point 5 : Questions émergentes
5.4 : Cyberrésilience

MISE EN ŒUVRE DE MESURES POUR LA PROTECTION CONTRE LA CYBER MENACES

[Note présentée par l'Agence pour la Sécurité de la Navigation Aérienne en Afrique et à Madagascar (ASECNA), pour le compte de ses États membres[2]]

RÉSUMÉ ANALYTIQUE

La présente note met en exergue l'importance pour les États/fournisseurs de services de navigation aérienne (ANSP) de déployer des systèmes de gestion de la cyber sécurité et de résilience pour la gestion du trafic aérien (ATM) et les communications, la navigation et la surveillance (CNS) afin de favoriser leur intégration et leur interopérabilité, base de la construction des espaces aériens sans couture.

Elle vise à apporter à la Conférence un aperçu sur les actions engagées par l'ASECNA et les défis à relever, concernant la protection des systèmes ATM contre les nouvelles menaces telles que les cyber-attaques.

Suite à donner : La Conférence est invitée à :
a) Prendre note des actions engagées par l'ASECNA et les défis à relever concernant la protection des systèmes ATM contre les nouvelles menaces telles que les cyber-attaques ;
b) Encourager les États/ANSP à mettre en œuvre des démarches systémiques et structurées de gestion de la cyber sécurité et de résilience du système ATM afin de favoriser la coopération entre États/ANSP dans la mise en œuvre du plan de navigation aérienne.
c) Noter la disponibilité de l'ASECNA à partager cette expérience avec tout (ANSP).

[1] Versions française et anglaise fournies par l'ASECNA.
[2] Bénin, Burkina Faso, Cameroun, République centrafricaine, Tchad, Comores, Congo, Côte d'Ivoire, Guinée équatoriale, France, Gabon, Guinée-Bissau, Madagascar, Mali, Mauritanie, Niger, Sénégal, Togo

1. INTRODUCTION

1.1 Le secteur de l'aviation est dépendant des systèmes de technologie de l'information et de communication et cette dépendance va s'accroitre avec l'interopérabilité des données et des systèmes, ainsi que l'avènement de la gestion de l'information à l'échelle du système de gestion de l'information à l'échelle du système (SWIM), qui vont s'appuyer sur les technologies de l'information, soutenus par le protocole Internet (IP).

1.2 Les données échangées entre les systèmes (sol/sol, sol/air) y compris la mise en œuvre des communications de données entre installations ATS (AIDC), du système de messagerie ATS (AMHS), des données de système de surveillance du service de la circulation aérienne (ATS), seront des éléments déterminants pour assurer l'écoulement sûr, rapide et ordonnée du trafic aérien. Ainsi, pour les ANSP, l'intégrité et la confidentialité des données seront les facteurs essentiels pour la sécurité et l'efficacité de la navigation aérienne.

1.3 La menace que font peser les cyber-incidents sur l'aviation civile évolue rapidement et constamment. Les intentions malveillantes des cybers terroristes vont de la perturbation de la continuité des activités au vol des informations pour des motivations diverses. La menace peut facilement évoluer pour toucher des systèmes cruciaux d'aviation civile dans le monde entier.

1.4 Face à cette éventualité, une approche basée sur les risques dans le domaine de la sûreté de l'aviation civile s'avère indispensable si l'on veut se donner les moyens d'anticiper les cybers-incidents plutôt que de gérer leur occurrence.

2. ANALYSE

2.1 Les ANSP doivent déterminer les données et systèmes critiques qu'ils utilisent, effectuer des évaluations des risques de cyber sécurité et de résilience et mettre en œuvre des mesures pour les protéger contre les interventions illicites.

2.2 L'ASECNA a fait une évaluation de son niveau de maturité en 2016 et élaboré un plan d'actions pour la mise en œuvre d'une démarche systémique de gestion de la cyber sécurité et de résilience des systèmes CNS et ATM.

2.3 Le déroulement dudit plan d'actions se poursuit avec la mise en place de mesures opérationnelles et d'un système de management de la Sûreté (SMSu) prenant en compte la cyber sécurité et de résilience du système ATM et CNS.

2.3.1 Ainsi et conformément aux dispositions du Manuel de Sûreté de l'ATM (Doc 9985), l'ASECNA a mis en place des mesures opérationnelles pour la protection de ses systèmes ATM, notamment :

a) Les aides à la navigation aérienne au sol
b) Les communications air-sol
c) Les liaisons de données
d) Les systèmes de surveillance
e) Le système de navigation par satellite (GNSS)
f) Les données de plan de vol et des données de trafic

g) Les systèmes de TIC (Technologies de l'information et de la communication) pour la gestion du trafic aérien

h) Les systèmes d'information et de gestion de l'ASECNA (Intranet, Progiciel de Gestion Intégré « PGI », système de messagerie ASECNA).

2.3.2 La mise en œuvre du système de management de la Sûreté (SMSu) de l'ASECNA est faite à travers le système de management intégré (SMI) de l'ASECNA, intégrant plusieurs domaines (sécurité, sûreté, qualité, environnement, santé et sécurité au travail et système d'information), car la performance en protection contre la cybercriminalité peut être impactée par les risques émanant des autres domaines. Des actions sont en cours pour développement des processus et procédures complémentaires à ceux existants, y compris les actions de formation et de sensibilisation relatives aux dispositions des Doc 8873 et 9985 de l'OACI.

2.4 Dans le cadre de la mise en œuvre du plan mondial de navigation aérienne à travers les ASBU, l'ASECNA a engagé des programmes d'investissement pour la mise en œuvre de l'AIDC, de l'AMHS, mais aussi des échanges de données surveillance avec certains fournisseurs de service de la région et les menaces malveillantes peuvent constituer des facteurs bloquants pour l'aboutissement de ces actions de coopération.

3. CONCLUSION

3.1 Un des enjeux majeurs est de mettre en place des mécanismes de gestion et de partage de l'information de sécurité et de sûreté, prenant en compte les spécificités de l'Agence qui fournit les services de navigation aérienne dans un espace aérien intégré de 18 États membres, avec des procédures harmonisées et des systèmes ATM interconnectés et intégrés. Lesdits mécanismes doivent être également conformes aux particularités de chaque État relatives à la sûreté.

3.2 Par ailleurs, il conviendra de mettre en œuvre des mesures de protection des équipements et services compte tenu de l'interopérabilité des systèmes ATM des centres opérationnels à l'échelle africaine. L'interconnexion et l'interopérabilité des systèmes de navigation aérienne, exposent ces systèmes à un plus grand risque en matière de cyber attaque.

3.3 Les mesures à mettre en place doivent intégrer l'ampleur du phénomène du terrorisme dans certains États de la région Afrique-océan Indien (AFI).

— FIN —