Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A39-WP/187[1]
EX/72
10/8/16

ASSEMBLÉE — 39e SESSION

COMITÉ EXÉCUTIF

Point 16 : Sûreté de l'aviation — Politique

STRATÉGIE DE CYBERSÉCURITÉ

[Note présentée par la Civil Air Navigation Services Organisation (CANSO)]

RÉSUMÉ ANALYTIQUE

La cybersécurité est l'un des sujets les plus pertinents et des plus débattus de l'aviation civile. L'évolution des systèmes aéronautiques entraîne des risques nouveaux, pertinents en raison de leurs conséquences possibles sur la sécurité et la continuité au regard de la dépendance accrue sur la technologie de l'information. Les systèmes de gestion de la circulation aérienne (ATM), mais aussi les systèmes de bord, les systèmes de gestion des aéroports, les systèmes de réservation, l'information aéronautique et l'information météorologique sont tout autant sensibles aux incidents de cybersécurité, qui concernent non seulement la protection des renseignements personnels, mais aussi et surtout la disponibilité et la continuité du service.

Suite à donner : L'Assemblée est invitée à convenir de la recommandation qui figure au paragraphe 5.

Objectifs stratégiques :	La présente note de travail se rapporte à l'Objectif stratégique C — *Sûreté et facilitation.*
Incidences financières :	Réduction des frais d'assurance ; atténuation des menaces et des risques par la résistance et la sécurité. Réduction des coûts de gestion de crise et des conséquences sociales.
Références :	Annexe 17 — *Sûreté* de la Convention de Chicago ; Doc 8973 ; Doc 9985 ; Doc 9854 ; Cyber Security Risk Assessment Guide (CANSO)

1. INTRODUCTION

1.1 L'aviation civile demeure une cible potentielle de haut niveau pour le crime et le terrorisme. L'obligation de la protéger contre les actes malveillants à son égard doit tenir compte de menaces sophistiquées, y compris de nature informatique. La société civile s'attend toujours à l'absence totale d'accidents et d'incidents imputables aux atteintes à la sûreté de l'aviation dans son ensemble. La confiance du consommateur final à l'égard du transport aérien repose sur cette attente. Le réseau de

[1] Versions française, anglaise, arabe, chinoise, espagnole et russe fournies par la CANSO.

transport aérien est essentiel à l'économie mondiale et aux échanges internationaux, le tourisme, l'investissement et la prospérité. Toute perturbation de son efficacité est susceptible d'entraîner d'importantes conséquences économiques et sociales partout dans le monde. Le développement de systèmes complexes, interopérables par leur nature même, dans un environnement mondial et multinational exige une approche méthodologique de la gouvernance de la sûreté, afin d'assurer la surveillance constante des ressources, l'intégration des processus entre la technologie de l'information (TI) et la sûreté logique et physique. Il faut à cette fin évaluer continuellement le niveau de menaces et la vulnérabilité potentielle, dans le but de prévenir les actes malveillants et d'y réagir. Une collaboration étroite est également nécessaire entre les acteurs de l'aviation, les États et les intervenants concernés. Le simple respect de la réglementation ne suffit pas, alors qu'il demeure nécessaire de faire preuve de vigilance pour protéger la vie humaine dans les airs et au sol et pour assurer la sûreté, la continuité, la résistance et la régularité du système. Le Groupe de travail sur la menace et les risques (TRWG) de l'OACI souligne également que le système mondial de l'aviation, en vertu de la complexité de son information et de ses communications, constitue assurément une cible potentielle de cyberattaques graves. L'objectif d'interopérabilité et l'ouverture des réseaux sur un concept d'exploitation axé réseau, rendus possibles par le partage en temps réel de l'information et des données opérationnelles, exposent le système à de nouvelles vulnérabilités.

1.2 L'OACI a déjà attiré l'attention sur le risque que la cybersécurité ne freine la mise en œuvre du Plan mondial de navigation aérienne (GANP) ; à ce titre, elle appuie une initiative conjointe avec les grands intervenants de l'aviation visant à évaluer systématiquement le cadre de cybersécurité actuel (le Groupe de haut niveau de l'industrie [IHLG] – cybersécurité, signé à Montréal le 5 décembre 2014).

1.3 Lors de la réunion du Groupe d'experts de la sûreté de l'aviation de l'OACI de mars 2016 (AVSECP/27), de nombreux États membres ont convenu du besoin d'actualiser les pratiques recommandées à l'annexe 17 (Sûreté) en ce qui a trait à la cybersécurité pour en faire une norme. Toutefois, les membres étaient majoritairement d'avis que la cybersécurité ne se limite pas au seul système de sûreté de l'aviation. Les membres ont souligné le besoin essentiel d'assurer une coordination appropriée, y compris par l'harmonisation avec d'autres annexes, à savoir les annexes 3, 6, 10, 11, 14 et 15. Qui plus est, la coordination avec d'autres groupes d'experts pertinents doit être réalisée avant d'actualiser les pratiques recommandées pour en faire une norme, et il est clairement nécessaire de consulter à cette fin la Commission de navigation aérienne (ANC) de l'OACI.

1.4 La CANSO souhaite insister sur l'importance de la protection de toute l'information numérique et de tous les systèmes informatiques de l'aviation dans son ensemble. Il s'agit d'une condition essentielle pour assurer la protection et la sécurité du grand public, des passagers, des équipages, du personnel au sol, des appareils et des installations aéronautiques contre les actes malveillants perpétrés en vol ou au sol. Des mesures particulières pourraient s'avérer nécessaires pour mieux appliquer ce concept dans les États moins développés, comme le prévoit l'initiative « Aucun pays laissé de côté » de l'OACI.

2. BESOIN DE EN MATIÈRE DE CYBERSÉCURITÉ

2.1 La CANSO remarque une certaine confusion quant à la définition du terme « cybersécurité ». Il désigne à la fois la menace que représentent les antagonistes et le besoin d'évaluer et d'éliminer les vulnérabilités des systèmes de TI. De plus, il renvoie à la mise en œuvre de plans d'urgence efficace dans l'optique de la résistance.

2.2 La CANSO insiste sur le fait qu'une stratégie sécuritaire saine pour l'aviation civile devrait non seulement tenir compte du degré de maturité technologique, mais surtout adopter une approche méthodologique de protection afin de réaliser l'objectif principal, c'est-à-dire la sûreté aéronautique. Cet objectif ne peut être atteint au moyen d'une démarche remontant aux plus hauts échelons de l'organisation afin de la couvrir dans son ensemble, en tenant compte des facteurs humains.

2.3 Cet objectif est clairement énoncé dans le *Concept opérationnel d'ATM mondiale* (Doc OACI 9854), où le rôle de la sûreté est jugé essentiel et représenté de façon novatrice (traduction) :

> *« La sûreté se rapporte à la protection contre les menaces d'actes malveillants (p. ex., terrorisme) ou d'incidents non intentionnels (p. ex., erreur humaine, catastrophes naturelles) ayant des répercussions sur les appareils, les personnes ou les installations au sol. L'assurance d'une sécurité adéquate constitue une attente majeure du milieu de l'ATM. Le système d'ATM doit par conséquent contribuer à la sécurité et il convient donc de le protéger, ainsi que les renseignements connexes, contre les menaces pour sa sécurité. »*

2.4 Selon cette perspective – liée aux normes majeures en sécurité de la TI –, l'objectif d'assurer la disponibilité, l'intégrité et la confidentialité se rapporte à l'obligation générale des États signataires de voir à la protection des principaux éléments constitutifs de l'aviation civile, comme le veut la Convention de Chicago et plus particulièrement l'annexe 17 (Sûreté) de l'OACI.

3. UNE NOUVELLE APPROCHE

3.1 La CANSO met en évidence le fait que la protection des actifs pertinents, essentielle à la sécurité de l'aviation civile, peut différer d'un intervenant à l'autre (par exemple, gouvernements, FSNA, transporteurs aériens, aéroports, constructeurs, forces armées, etc.), en fonction des objectifs de chacun. Il est néanmoins possible de définir, à partir de besoins précis, certains sujets de cybersécurité qui sont communs à tous les acteurs du milieu de l'aviation :

a) Veiller à ce que les renseignements sensibles ne soient accessibles qu'aux personnes autorisées, afin de prévenir les intrusions illégales attribuables à des menaces extérieures, indépendamment de l'activité principale de l'exploitant.

b) Remplir l'obligation – qui relève du bon sens et de la bonne foi – de déterminer et d'éliminer les vulnérabilités des systèmes essentiels, par mesure normale de vigilance et de prudence.

c) Étendre la gestion des risques aux risques qui découlent de la dépendance croissante sur les ressources de TI appartenant à un exploitant individuel.

d) Mettre en place une procédure de gestion des interventions appropriées pour traiter les incidents et les situations de crise, y compris par la planification de mesures d'urgence.

e) Évaluer les impacts des atteintes à la (cyber) sécurité, non seulement à l'égard de l'exploitant individuel, mais aussi du secteur dans son ensemble, dans le cadre du programme national de sûreté de l'aviation civile.

3.2 En d'autres mots, la cybersécurité ne diffère pas de l'approche classique de la sûreté aéronautique; elle doit plutôt être vue comme un prolongement naturel des principes de base énoncée à l'annexe 17 (Sûreté) et dans les documents d'orientation, où sont traitées les menaces et les vulnérabilités les plus courantes en matière de sécurité physique.

3.3 Les cybermenaces qui pèsent sur l'aviation seront vraisemblablement l'une des principales questions liées à la sécurité de tout nouveau programme de modernisation, qu'il s'agisse du ciel unique européen (SES), de la recherche en ATM du SES (SESAR), du Next Generation Air Transportation System (NEXTGEN, États-Unis) et d'autres programmes de dimension régionale. Il semble s'agir de l'un des principaux facteurs déterminants dans d'autres parties du secteur de l'aviation. Étant une ressource essentielle, l'information doit être traitée comme tout autre actif fondamental pour la surviabilité et la réussite des systèmes d'ATM. Tous ces programmes, non seulement d'ATM mais aussi ceux concernant les exploitants d'appareils, les aéroports, les forces armées et autres, seront fondés sur le concept du System Wide Information Management (SWIM), qui facilite l'échange opérationnel axé sur le réseau d'information et de services dans le système global. Le concept du SWIM améliorera la prise de décision collaborative, en fournissant une information de meilleure qualité en fonction du besoin de savoir, au bon moment et au bon destinataire. Le SWIM est le principal catalyseur de l'environnement technologique futur de l'aviation et son infrastructure connexe doit être considérée comme une infrastructure essentielle, dont la sécurité sera prise en compte comme paramètre de conception obligatoire.

3.4 À cet égard, si la sécurité générale demeure une obligation pour les États signataires, avec ses implications en matière de souveraineté nationale, de défense, de renseignement et d'application de la loi, la nécessité de tenir compte des particularismes du milieu de l'aviation appelle à une action plus efficace.

3.4.1 Les initiatives pertinentes à l'échelle régionale sont en cours ou déjà mises en œuvre. Voici, à titre d'information, quelques résultats récents : En ce qui concerne la position de l'Union européenne sur la cybersécurité de l'ATM, la dernière version du règlement de la CE (1035/2011) annonce clairement qu'il existe une relation nette entre les vulnérabilités sécuritaires, et prescrit des exigences contraignantes en matière de cybersécurité. La Federal Aviation Administration (FAA) des États-Unis, dans sa proposition au Sénat américain, déclare un objectif pertinent en matière de cybersécurité (sec. 4109) visant des objectifs ambitieux, notamment un vaste ensemble de mesures visant à assurer la cybersécurité. D'autres États ciblent également leurs efforts de réglementation sur la cybersécurité de l'aviation dans le même esprit.

3.4.2 En raison de l'importance de la cybersécurité pour l'aviation civile, la CANSO appuie sans réserve toute initiative visant à réaliser la pleine intégration de la cybersécurité aux programmes de sécurité aéronautique nationaux et régionaux et se met à l'entière disposition des intervenants pour y participer activement.

4. CONCLUSION

4.1 La cybersécurité de l'aviation est un sujet à traiter avec méthodologie et réalisme, compte tenu des conséquences possibles sur le secteur dans son ensemble et sur la confiance du grand public.

4.2 La CANSO défend une initiative internationale renouvelée, placée sous la houlette de l'OACI et suivant une démarche efficace et durable, conforme au principe « Aucun pays laissé de côté ».

4.3 L'initiative du Groupe de haut niveau de l'industrie (cybersécurité), qui s'inscrit dans la foulée du plan d'action en cybersécurité signé en décembre 2014, travail à l'élaboration d'un cadre favorisant la coopération volontaire dans le domaine. Ce programme emmené par l'industrie devrait être complété et appuyé par les autorités de réglementation ainsi qu'une prise en considération plus poussée de la question horizontale de la cybersécurité dans l'aviation civile.

5. RECOMMANDATIONS

5.1 L'Assemblée est invitée à charger le Secrétariat de l'OACI d'intégrer urgemment la cybersécurité dans la sûreté de l'aviation de façon saine, durable et efficace. L'Assemblée est invitée à souscrire aux recommandations suivantes :

Il est recommandé que l'Assemblée :

a) tienne compte du contenu du présent rapport et y adhère, en reconnaissant sa pertinence et ses répercussions possibles sur l'aviation civile ;

b) convienne que l'OACI élabore une nouvelle stratégie sur la cybersécurité de l'aviation comme domaine vertical dans les documents d'orientation sur la sûreté et les problèmes de l'aviation, dans le but d'harmoniser les initiatives actuelles aux niveaux régional et national ;

c) recommande aux États membres de concentrer leur attention sur les vulnérabilités des systèmes et des réseaux et non sur les seules menaces, et de prendre en considération les applications pour l'ensemble du secteur de l'aviation civile ;

d) recommande l'établissement d'un forum ou les entreprises d'aviation pourraient partager leurs pratiques exemplaires dans un environnement sécurisé de confiance de telle sorte que les outils et les techniques qui améliorent la sécurité de la technologie des actifs technologiques actuels et futurs soient partagés par le plus grand nombre ;

e) recommande aux États membres de prendre connaissance des initiatives récentes présentées lors d'AVSECP/27 à fin d'élever au niveau de normes les pratiques recommandées 4.9.1 et 4.9.2 de l'annexe 17 ;

f) prenne connaissance du *Cyber Security and Risk Assessment Guide*[2] *de la CANSO*.

— FIN —

[2] https://www.canso.org/canso-cyber-security-and-risk-assessment-guide