Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/295
TE/119
1/8/19

ASSEMBLÉE — 40e SESSION

COMMISSION TECHNIQUE

Point 30 : Autres questions à examiner par la Commission technique

APPLICATION DES CONTRÔLES DE CYBERSÉCURITÉ DE L'ÉTAT À L'AVIATION

(Note présentée par la Nouvelle-Zélande)

RÉSUMÉ ANALYTIQUE

La présente note de travail porte sur l'élaboration de cadres de cybersécurité de l'aviation de l'OACI dans le contexte des contrôles existants de cybersécurité non spécifiques à un secteur utilisés par les États. Elle propose que l'OACI concentre ses efforts sur l'élaboration de principes solides et convenus à partir desquels les États peuvent aborder les questions de cybersécurité.

Suite à donner : L'Assemblée est invitée à :

a) noter que la mise en œuvre de normes mondiales harmonisées excessivement prescriptives en matière de cybersécurité de l'aviation peut entrer en conflit avec les cadres nationaux de cybersécurité des États et limiter leur capacité à se conformer aux SARP de l'OACI ;
b) encourager l'OACI à se concentrer sur l'élaboration d'orientations fondées sur des principes en ce qui concerne la cybersécurité du secteur de l'aviation afin d'aider les États à intégrer ce secteur dans leurs cadres nationaux, en tenant compte des normes de sûreté de l'information établies telles que la série ISO 27000 ;
c) encourager l'OACI à fournir des orientations sur l'objet et l'application du cadre de confiance.

Objectifs stratégiques :	La présente note de travail se rapporte aux Objectifs stratégiques : Sûreté et facilitation, et Sécurité.
Incidences financières :	Aucune
Références :	AN-Conf/13-WP/270 : Notion de système de systèmes dans la cybersécurité en aviation (28/09/2018)

1. INTRODUCTION

1.1 Avec les progrès technologiques continus et la complexité croissante des systèmes aéronautiques, la sécurité et la sûreté du système aéronautique mondial dépendent de plus en plus de contrôles efficaces en matière de cybersécurité.

1.2 La nécessité de ces contrôles est commune à un large éventail de secteurs et n'est nullement limitée à l'aviation. Sans une cybersécurité efficace, les organisations auront du mal à fournir des produits et des services numériques de manière à préserver la confiance de leurs clients et de leurs parties prenantes.

1.3 Les États ont un rôle à jouer pour faire en sorte que les organisations et les secteurs importants au plan national atteignent des niveaux de cybersécurité toujours élevés. L'approche adoptée variera d'un État à l'autre en fonction des menaces, des capacités et des intérêts en matière de sûreté nationale.

1.4 Alors que les types de contrôles de sûreté mis en place par les diverses organisations dépendront généralement de leurs besoins et de leurs capacités, ainsi que de ceux du secteur dans lequel elles opèrent, les intérêts de sûreté nationale imposeront des exigences primordiales. L'intérêt national d'un État prendra toujours le pas sur celui d'un secteur ou d'une organisation en particulier.

1.5 L'aviation mondiale est fortement tributaire de la sécurité et de la sûreté de la transmission numérique des informations entre les membres de la communauté aéronautique, et notamment entre les États. La note de travail AN-Conf/13-WP/270 présentée à la treizième Conférence de navigation aérienne a introduit le concept d'une approche de « système de systèmes » en matière de cybersécurité. Cette approche considère que le système aéronautique mondial est composé d'un certain nombre de sous-systèmes exploités par une série de parties prenantes et que ceux-ci doivent être considérés de manière globale pour créer un environnement opérationnel sûr.

1.6 Le cadre de confiance de l'OACI a été élaboré pour permettre l'établissement de liens de communication de confiance entre les parties prenantes. Il repose sur les principes suivants :

1.6.1 L'interopérabilité entre toutes les parties prenantes est assurée par un cadre confiance commun et une architecture permettant des services de messagerie intégrés et efficaces à l'échelle mondiale.

1.6.2 La résilience des communications est optimisée en utilisant des concepts de conception qui limitent l'étendue de la menace. Cela inclut la compartimentation du réseau et des applications, ainsi que la superposition de couches de protection dans l'infrastructure et la limitation du nombre de systèmes participants.

1.6.3 De solides caractéristiques d'identification, d'authentification, d'autorisation, d'intégrité et de confidentialité.

1.7 Le concept de cadre de confiance a certes du mérite, mais son objet et son application potentielle ne sont pas clairement définis. Une élaboration plus poussée de ce cadre nécessitera un examen minutieux des intérêts des États en matière de sûreté nationale pour permettre de définir clairement son rôle.

2. ANALYSE

2.1 Les intérêts nationaux d'un État imposent des limites à la nature des cadres de cybersécurité pouvant être mis en œuvre par chaque secteur et chaque organisation. Lorsqu'il y a des exigences réglementaires et des normes en matière de sûreté de l'information, celles-ci prendront le pas sur les normes spécifiques à chaque secteur et à chaque organisation.

2.2 Dans ces conditions, la capacité d'un État de se conformer aux SARP normatives de l'OACI en matière de cybersécurité de l'aviation sera probablement limitée par ses propres cadres de sûreté nationale. L'ampleur de cette contrainte variera considérablement d'un État à l'autre et en fonction du degré de prescription des SARP elles-mêmes.

2.3 De même, il est peu probable qu'une approche extrêmement prescriptive et extrêmement normalisée puisse réglementer efficacement un domaine dans lequel la technologie et l'environnement de la menace évoluent tous deux rapidement. Des exigences mondiales trop prescriptives peuvent entraver la capacité d'un État à réagir au changement, et ne pas convenir aussi à différents types d'opérations.

2.4 Malgré les besoins divergents des États en matière de cybersécurité et les problèmes liés à l'imposition d'exigences internationales extrêmement prescriptives, il est nécessaire de disposer d'un ensemble de principes cohérents et convenus pour régir le transfert sûr d'informations entre parties prenantes.

2.5 Pour appuyer l'application de ces principes, des éléments indicatifs de l'OACI devraient être élaborés en vue d'aider les États à appuyer la cybersécurité de l'aviation comme partie intégrante des cadres nationaux. À cet effet, une approche basée sur la performance ou sur des principes sera probablement la plus efficace.

2.6 Avec l'adoption d'une approche fondée sur des principes, chaque État pourra adapter les orientations de l'OACI de manière à permettre la mise en place d'un cadre de confiance global conforme aux exigences nationales. Les normes existantes de sûreté de l'information basées sur des principes, telles que la série ISO 27000, constituent la base de ces orientations. Idéalement, quatre domaines d'intérêt seraient abordés :

2.6.1 **La gouvernance** : promouvoir la cybersécurité au niveau des hauts responsables afin de protéger les actifs numériques les plus importants de l'organisation. Les membres des conseils d'administration et les hauts dirigeants sont responsables en dernier ressort des conséquences de tout incident informatique, y compris de l'impact sur la confiance des parties prenantes et des clients.

2.6.2 **L'investissement :** investir dans la cybersécurité pour réduire les risques au minimum et optimiser les rendements. Un accord au niveau de la gouvernance sur le goût du risque de l'organisation et l'identification des actifs clés sont des premières étapes essentielles pour faire en sorte que l'investissement soit bien orienté et équilibré.

2.6.3 **La préparation** : préparer l'organisation à détecter les incidents de cybersécurité, ainsi qu'à y réagir et à s'en remettre. La question n'est pas de savoir « si » mais « quand » une organisation connaîtra un incident de cybersécurité. La préparation aux incidents permet aux organisations de réduire le risque global de cybersécurité grâce à une récupération rapide et efficace.

2.6.4 **La chaîne d'approvisionnement :** maintenir la surveillance et la sensibilisation aux risques de cybersécurité dans la chaîne d'approvisionnement de l'organisation. Ce domaine est particulièrement important dans le secteur de l'aviation, car la fourniture d'équipements et de services

met souvent en jeu de longues chaînes d'approvisionnement. Cela inclut la composante technique de la conception des systèmes et l'aspect facteur humain de la conception des processus.

2.7 Des orientations bien formulées, basées sur la performance et fondées sur les normes de sûreté de l'information établies, seraient utiles aux différentes organisations du secteur de l'aviation et encourageraient une approche cohérente couvrant les éléments essentiels de contrôles efficaces de cybersécurité.

2.8 L'élaboration de ces orientations devrait également tenir compte des cas où certains contrôles minimums sont nécessaires et la manière dont ils devraient être effectués en tenant compte des cadres appliqués par les différents États.

2.9 L'élaboration du cadre de confiance de l'OACI offre l'occasion d'établir des protocoles pour l'échange d'informations entre parties prenantes, mais des précisions supplémentaires s'avèrent nécessaires en ce qui concerne l'objet et l'application de ce cadre.

2.10 Cette élaboration devrait être envisagée conjointement avec les cadres de cybersécurité mis en œuvre par les parties prenantes. La sûreté de l'échange de données est étroitement liée à celle de la source de ces données, et cela dépend de l'adoption de contrôles efficaces par les organisations et les États.

— FIN —