Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A39-WP/99
EX/45, TE/26
26/7/16

ASSEMBLÉE — 39e SESSION

COMITÉ EXÉCUTIF
COMMISSION TECHNIQUE

Point 16 : Sûreté de l'aviation — Politique
Point 36 : Sécurité de l'aviation et soutien à la mise en œuvre de la navigation aérienne

CYBER-RÉSILIENCE DANS L'AVIATION CIVILE

(Note présentée par les États-Unis et la Slovaquie au nom de l'Union européenne, de ses États membres[1] et des autres États membres de la Conférence européenne de l'aviation civile[2], et par EUROCONTROL)

RÉSUMÉ ANALYTIQUE

Le système d'aviation civile consiste en une mosaïque de composants, systèmes et réseaux interconnectés. Il y a eu au fil des ans une augmentation du risque de survenue de cyber-incidents qui pourraient compromettre les communications et les échanges d'informations entre les diverses parties prenantes de l'aviation, influer sur la sécurité et la sûreté et porter atteinte à la continuité de l'activité aéronautique. L'OACI a reconnu l'importance de définir une approche appropriée de la cybersécurité dans l'aviation civile, mais des efforts supplémentaires sont encore nécessaires afin d'accroître la sensibilisation à l'échelle mondiale et de développer davantage mondialement des approches cohérentes de la cyber-résilience pour le système d'aviation.

Suite à donner : L'Assemblée est invitée :

a) à demander que l'OACI étudie de manière exhaustive la question de la cyber-résilience dans l'aviation civile ;
b) à demander que l'OACI et ses États contractants promeuvent la sensibilisation aux menaces et vulnérabilités cybernétiques dans l'aviation civile, notamment par l'inclusion de la dimension de cyber-résilience dans les processus et activités pertinents comme la conception des systèmes, les procédures ATM et la gestion de la sécurité et la sûreté de l'aviation ;
c) à demander que l'OACI facilite, en toute sécurité, le partage d'informations entre les États et les parties prenantes pertinentes sur les menaces et vulnérabilités cybernétiques et les mesures d'atténuation ;
d) à demander que l'OACI étudie les mesures à prendre pour l'élaboration de principes directeurs pour la gestion des menaces et vulnérabilités cybernétiques actuelles et futures, depuis l'identification jusqu'à l'atténuation, en tenant compte des mesures pertinentes existantes en place dans les États et des normes de l'industrie ;
e) à demander que l'OACI charge les groupes d'experts et comités d'experts existants de tenir compte, le cas échéant, de ces lignes directrices dans l'accomplissement de leurs travaux.

[1] Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie et Suède.

[2] Albanie, Arménie, Azerbaïdjan, Bosnie-Herzégovine, Géorgie, Islande, L'ex-République yougoslave de Macédoine, Monaco, Monténégro, Norvège, République de Moldova, Saint-Marin, Serbie, Suisse, Turquie et Ukraine.

Objectifs stratégiques :	La présente note de travail se rapporte aux Objectifs stratégiques : Sécurité, Capacité et efficacité de la navigation aérienne, Sûreté et Facilitation.
Incidences financières :	Les activités dont il est question dans la note de travail ci-jointe de l'Assemblée seront entreprises sous réserve de la disponibilité des ressources budgétaires dans le budget-programme 2017-2019 et/ou de contributions extrabudgétaires.
Références :	Doc 10022, *Résolutions de l'Assemblée en vigueur* (au 4 octobre 2013) Annexe 17 — *Sûreté — Protection de l'aviation civile internationale contre les actes d'intervention illicite*

1. INTRODUCTION

1.1 Le système d'aviation consiste en une mosaïque de composants, systèmes et réseaux interconnectés. De nouveaux développements, comme l'introduction progressive des RPAS et l'évolution continue du système ATM (p. ex. la SWIM) renforcent cette interconnectivité et l'intégration des systèmes. En dépit des mesures préventives de sûreté prises jusqu'ici, l'exposition du système d'aviation à des cyber-incidents a augmenté.

1.2 L'importance d'une approche appropriée de la cyber-sûreté dans l'aviation a été reconnue à l'échelle mondiale. Toutefois, des efforts restent à faire afin d'accroître la sensibilisation à l'échelle mondiale et de développer davantage des approches mondialement cohérentes de la cyber-résilience pour le système d'aviation.

1.3 Les cyber-incidents peuvent toucher la communauté mondiale de l'aviation ou des systèmes individuels à de nombreux niveaux. Ces incidents pourraient mettre en danger les communications et les échanges d'informations entre les diverses parties prenantes de l'aviation, avec des conséquences sur la sécurité et la sûreté et une dégradation de la continuité des activités aéronautiques. La possibilité de partager l'information cybernétique et l'application de méthodes normalisées solides pour sécuriser l'échange de données et d'informations renforceraient l'aptitude de la communauté aéronautique à se protéger et à limiter les effets de cyber-incidents.

2. ANALYSE

2.1 Alors que plusieurs initiatives ont été élaborées aux niveaux local, national, régional et mondial, il serait utile d'adopter une approche normalisée, uniforme et cohérente des risques inhérents à l'environnement changeant de cyber-menaces dans l'aviation.

2.2 Promouvoir la sensibilisation à la cyber-résilience dans l'aviation, à l'échelle mondiale

2.2.1 Dans certains secteurs économiques, comme la banque, les menaces et vulnérabilités cybernétiques sont bien connues et des contre-mesures ont été mises en œuvre afin d'atténuer les risques cernés. Cependant, dans le domaine de l'aviation, les risques cybernétiques ne sont pas toujours bien compris par tous les États et toutes les parties prenantes, et ils ne sont pas non plus traités d'une manière uniforme et systématique.

2.2.2 Il faut augmenter la sensibilisation aux menaces et vulnérabilités cybernétiques dans le secteur de l'aviation au niveau mondial afin de garantir que tous les États et parties prenantes puissent identifier les risques qui peuvent survenir et les atténuer.

2.2.3 Cette sensibilisation accrue pourrait notamment être formalisée par l'adaptation de processus existants, par exemple au moyen de l'élaboration d'une approche de sûreté intégrée dès le stade de la conception ou la mise en œuvre d'une formation spécialisée. En outre, et en collaboration avec les initiatives de sûreté (p. ex. les systèmes de gestion de la sûreté, lorsqu'ils sont disponibles, ou les programmes nationaux de sûreté de l'aviation civile), la dimension de cyber-résilience devrait être prise en compte dans le contexte des activités de gestion de la sécurité, au niveau de l'organisation (dans le cadre de son système de gestion de la sécurité – SGS), ainsi qu'au niveau de l'État ou au niveau régional (dans le cadre du programme national de sécurité – PNS) et, le cas échéant, dans le contexte d'un programme régional de sécurité de l'aviation.

2.3 Promouvoir le partage de l'information sur les incidents et menaces cybernétiques et les approches normalisées

2.3.1 Aucune organisation à elle seule ou groupe de parties prenantes à lui seul ne sera en mesure de se protéger par ses propres moyens contre une intrusion électronique intentionnelle. En outre, les cyber-menaces changent constamment et nul ne peut prétendre être à l'abri de tous les risques connexes possibles. Pour réagir efficacement à des cyber-incidents, il faut donc que les États et parties prenantes partagent l'information pertinente et harmonisent les modalités de protection et de conservation de l'intégrité des données et des échanges d'information. Le partage des informations aiderait les États et les parties prenantes à mieux se préparer à faire face à des cyber-incidents et à prendre des mesures appropriées pour les atténuer. Les informations partagées peuvent comprendre l'occurrence des incidents, les vulnérabilités, les menaces, les tendances et les schémas observés, les évaluations des risques partagés, les plans de traitement des risques, les moyens efficaces d'atténuation (techniques, opérationnels ou organisationnels) ou les activités d'assurance de la sûreté dont il a été prouvé qu'elles procurent des protections efficaces.

2.3.2 Dans le monde aéronautique, plusieurs initiatives ont déjà été lancées qui font la promotion du partage des informations de sûreté (et souvent d'informations sensibles), notamment au niveau régional et au niveau mondial, mais il reste à développer davantage et à compléter cette dynamique pour appuyer la cyber-résilience du système global d'aviation. Ces initiatives peuvent être basées sur des plateformes existantes d'échange d'informations comme l'ISAC (le Centre de partage et d'analyse d'informations) et la CERT (Équipe d'intervention en cas d'urgence informatique) et peuvent nécessiter que soient mis en place des protocoles communs de partage d'informations sur les cyber-incidents, conformément aux règlements nationaux et régionaux sur la protection des informations sensibles.

2.3.3 Il faut également améliorer les méthodes de protection des données et d'échange d'informations entre toutes les parties prenantes pertinentes. La normalisation de contrôles techniques qui offriront des méthodes plus solides d'authentification et d'autorisation des données pour la communauté aéronautique mondiale devrait être encouragée.

2.4 Promouvoir une « approche commune de la gestion des risques en aviation »

2.4.1 Dans l'aviation, il y a de nombreuses méthodologies pour évaluer les risques, dont la plupart sont axées sur la caractérisation et l'évaluation des menaces et des vulnérabilités. Il peut y avoir accord sur les éléments qui sont nécessaires pour caractériser les risques (p. ex. la probabilité

d'occurrence et l'ampleur de l'impact), mais les évaluations de détails spécifiques sont suffisamment diverses pour qu'on obtienne des résultats comparables, cohérents et même uniformes. Toutefois, face à des cyber-incidents récurrents qui peuvent suivre des schémas similaires, il est utile de définir des principes et méthodes communs pour identifier, évaluer et atténuer les risques.

2.4.2 Ces « principes communs » devraient faciliter l'identification des menaces et des vulnérabilités, permettre d'évaluer les risques et d'offrir des outils d'atténuation. Un exemple serait la définition formelle de l'ampleur de la sûreté, par une description du contexte dans lequel les évaluations de risque sont effectuées, et la définition de cette ampleur aiderait à identifier les systèmes d'information aéronautiques critiques comme le prévoient les dispositions actuelles de l'Annexe 17. Un autre exemple consisterait à examiner des « scénarios de menace » de bout en bout, comprenant les menaces, l'architecture du système à l'étude et les facteurs qui causent la survenue d'effets indésirables. Cette démarche inclut également les vulnérabilités connues dans le scénario de menace, qui peuvent appeler des mesures d'atténuation proportionnelles à la gravité de l'impact.

2.4.3 Des « principes communs » d'évaluation des risques en aviation, une fois définis et adoptés, seraient également et idéalement appliqués au cadre de l'OACI lors de l'élaboration ou de l'amendement des normes et pratiques recommandées (SARP).

— FIN —