Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/395[1]
EX/161
30/7/19
(Note d'information)

ASSEMBLÉE — 40e SESSION

COMITÉ EXÉCUTIF

Point 12 : Sûreté de l'aviation — Politique

CYBERSÉCURITÉ DE L'AVIATION — ALLER DE L'AVANT

(Note présentée par l'Association du transport aérien international)

RÉSUMÉ ANALYTIQUE	
La présente note présente le point de vue de l'Association du transport aérien international (IATA) sur la nécessité de réaliser des progrès coordonnés, proactifs et tangibles en matière de visibilité et de gestion des risques de cybersécurité de l'aviation.	
Objectifs stratégiques :	La présente note se rapporte à l'objectif stratégique : Sûreté
Incidences financières :	Aucune
Références :	

[1] Versions française, anglaise, arabe, chinoise, espagnole et russe fournies par l'Association du transport aérien international.

1. INTRODUCTION

1.1 La cybersécurité de l'aviation (sécurité informatique ayant trait au maintien d'opérations de vol sécuritaires, sûres et résilientes) demeure une priorité clé de l'industrie. La numérisation accrue et la connectivité contribuent à la transformation du service offert aux clients et à l'amélioration de l'ensemble des activités des exploitants réglementés, qu'il s'agisse d'efficience ou de fiabilité. Mais cette transformation n'apporte pas que des possibilités positives à l'industrie aérienne. Elle offre aussi des possibilités à ceux qui veulent nuire à cette industrie. Fondamentalement, le secteur de l'aviation est possiblement en meilleure posture que d'autres industries, en raison de sa culture de sécurité, de la visibilité du risque et des pratiques de conception et de formation axées sur la redondance en cas de défaillance. Cependant, la complexité et l'interdépendance du service et du système, souvent à l'échelle internationale, peuvent avoir un impact sur la capacité de comprendre et de gérer le risque de cybersécurité.

1.2 L'IATA soutient pleinement la position de l'OACI, qui constitue l'organisation la plus appropriée pour diriger un dialogue mondial cohérent et des actions en matière de cybersécurité de l'aviation. Sans leadership international clair en matière de cybersécurité, on risque la fragmentation des normes mondiales, un régime réglementaire complexe qui freinerait la croissance et l'innovation, ainsi qu'une moindre capacité d'évaluer et de gérer les risques de cybersécurité de l'aviation à l'intérieur et par-delà les frontières.

1.3 La production de la stratégie de l'OACI en matière de cybersécurité de l'aviation est une étape louable qui était attendue de longue date et elle est pleinement appuyée par l'IATA. Maintenant, il faudra du leadership, des actions et une gouvernance appropriée pour entériner la stratégie par un amendement à la Résolution A39-19 de l'Assemblée, *Cybersécurité dans l'aviation civile*, pour incorporer la référence correspondante. Par conséquent, tous les intervenants, incluant les responsables de la sécurité et de la sûreté, doivent y consacrer les ressources, le temps et les efforts nécessaires. De plus, étant donné ce qui précède, il importe d'encourager la ratification par les États de la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* et du *Protocole additionnel à la Convention pour la répression de la capture illicite d'aéronefs*. Cet engagement collaboratif devrait mener au développement de bonnes pratiques et de matériel d'orientation à partir desquels l'IATA, en principe, appuie la production de SARP sur la cybersécurité, suivie de leur mise en œuvre et de leur surveillance.

1.4 De façon plus générale, dans nos efforts pour assurer la sécurité de l'aviation, nous ne devons pas oublier les éléments vitaux de notre industrie, à savoir nos passagers et nos clients. Nous devons faire en sorte que tout au long du trajet, la cybersécurité, la vie privée, les données et les droits du client soient protégés. De plus, notre transparence dans ces matières nous permettra d'établir et de maintenir une relation de confiance avec ceux qui soutiennent notre industrie.

1.5 L'IATA a été proactive dans ses efforts de sensibilisation et de dialogue auprès des intervenants concernant les défis mondiaux liés à la cybersécurité de l'aviation. L'IATA a un groupe de travail spécial bien établi sur la cybersécurité (ACSTF), qui s'emploie à améliorer la compréhension, entretenir le dialogue et recenser les bonnes pratiques chez tous les intervenants du secteur de l'aviation. La maturité du groupe ACSTF a permis de créer un environnement de confiance dans lequel s'exerce un partage tangible d'information sur une multitude de sujets connexes. De plus, l'IATA a dirigé une table ronde innovante sur la cybersécurité de l'aviation à Singapour (avril 2019) à laquelle participaient des intervenants de tout le secteur de l'aviation. Lors de cette table ronde, les participants ont exploré les défis actuels de l'industrie aérienne, ce que la future cybersécurité devrait être et comment y arriver. Les conclusions font ressortir que bien qu'un travail important soit actuellement réalisé, il reste beaucoup à faire.

1.6 De plus, l'IATA a entamé le processus de développement de sa stratégie de l'industrie sur la cybersécurité de l'aviation, et d'une feuille de route pour la mettre en œuvre. L'objectif de la stratégie est de permettre à l'IATA, au nom de ses membres et de l'industrie en général, de mettre davantage l'accent sur les défis et les possibilités qui s'offrent en matière de cybersécurité, les actions tangibles qui vont faire avancer les choses et la collaboration nécessaire pour y arriver.

2. DISCUSSION

2.1 Selon les chiffres actuels sur la croissance, on devrait voir doubler le nombre de passagers d'ici 2037, et une bonne partie de cette croissance se fera dans la région Asie-Pacifique[2]. Cette croissance s'accompagne de pressions et de risques et la cybersécurité de l'aviation doit être considérée comme l'un de ces risques. On ne doit pas sous-estimer le caractère critique de la sécurité, de la sûreté et de la résilience technologique dont dépend cette croissance.

2.2 Un cyberincident en aviation peut avoir des conséquences sur la sécurité, la sûreté, les services opérationnels, les finances ou la croissance. Mais il a aussi un impact sur la confiance des passagers envers le service même que nous offrons. Au cours des ans, l'industrie aérienne a démontré sa résilience aux incidents de sécurité et de sûreté et elle a su restaurer la confiance des passagers grâce à des mesures et un engagement manifestes. À la suite d'un incident de cybersécurité, restaurer la confiance sera un cran plus difficile que ce que l'industrie a vécu auparavant. C'est pourquoi nous devons non seulement améliorer la cybersécurité, mais aussi entretenir un dialogue ouvert sur les défis auxquels nous faisons face et sur les efforts que nous faisons.

2.3 Dans nos efforts d'avancement technologique, nous devons trouver un équilibre entre, d'une part, les gains d'efficience et l'amélioration du service au moyen de technologies connectées et, d'autre part, la cybersécurité, la sûreté et la résilience de ces technologies. Nous ne pouvons plus accepter d'incorporer à l'industrie aérienne n'importe quelle technologie sans qu'elle soit sûre par sa conception, déployée selon une gestion de la vulnérabilité proactive et souple et dans un contexte de transparence en matière de cybersécurité entre les fournisseurs et les utilisateurs.

2.4 Parallèlement aux activités de l'industrie en vue d'améliorer la cybersécurité, des efforts doivent être déployés pour en réduire les coûts. Comme nous sommes une industrie internationale réunissant une vaste gamme d'organisations, tout ce qui peut être fait pour alléger la complexité, le coût ou le défi de gérer adéquatement la cybersécurité doit être fait, de sorte qu'aucun pays (ou aucune compagnie) ne soit laissé de côté.

2.5 L'industrie doit faire davantage pour accroître de façon proactive la visibilité du risque de cybersécurité et la vulnérabilité qui en découle. Cela suppose une collaboration ouverte et proactive entre tous les intervenants : pairs, nations, organisations multinationales, autres industries et chercheurs. En tant qu'industrie, nous devons établir clairement qui sont nos adversaires et qui n'en sont pas ; ceux qui veulent nous aider à comprendre le risque ne sont pas nos adversaires. Des recherches privées, légitimes, dans l'ensemble de l'industrie sur les vulnérabilités du matériel informatique et des logiciels ont fait naître une communauté de recherche active et dynamique agissant en toute bonne foi pour aider plusieurs secteurs industriels à accroître la cybersécurité.

[2] IATA, communiqué de presse, 24 octobre 2018. *L'IATA prévoit 8,2 milliards de voyageurs aériens en 2037*. https://www.iata.org/pressroom/pr/Documents/2018-10-24-02-fr.pdf.

2.6 Le secteur de l'aviation a le devoir d'écouter, d'évaluer et d'agir de façon appropriée face à tout problème potentiel de sécurité qui lui est signalé ; nous devons traiter les avertissements de vulnérabilité en matière de cybersécurité de la même manière. L'industrie aérienne doit prendre des mesures pour gagner la confiance de la communauté des chercheurs et établir avec elle des relations de façon à développer de part et d'autre une entente collaborative. L'IATA soutient cet effort, ainsi que les mesures et les lois qui favorisent et protègent la capacité des chercheurs de bonne foi d'appuyer l'industrie aérienne.

2.7 Lors de la table ronde sur la cybersécurité de l'aviation organisée par l'IATA en avril 2019 à Singapour, des participants de l'ensemble de l'industrie ont souligné les progrès accomplis ainsi que les domaines qui nécessitent plus d'efforts. Les points saillants sont les suivants :

2.7.1 Points de vue sur l'état actuel de la cybersécurité de l'aviation :

a) L'étendue et la complexité du risque de cybersécurité de l'aviation représentent un problème pour certaines organisations en termes de compréhension, d'établissement de priorités et d'action.

b) En raison de la nature interdépendante et mondiale de l'industrie aérienne, on évalue que le nombre de cyberincidents pourrait augmenter rapidement et avoir des conséquences internationales.

c) Il subsiste des incohérences et des lacunes dans le secteur de l'aviation lorsqu'il s'agit de détecter, gérer et communiquer les vulnérabilités sur le plan de la cybersécurité, ce qui entraîne une faible visibilité du risque actuel.

2.7.2 Points de vue des participants sur la vision future idéale de la cybersécurité de l'aviation à l'horizon 2030 et sur les moyens d'y arriver :

a) Culture de cybersécurité. Tout comme la culture de la sécurité ou de la sûreté physique, il faut dans l'ensemble du secteur de l'aviation une culture de la cybersécurité.

b) Transparence et confiance. Il faut, entre tous les intervenants de l'industrie aérienne, davantage de transparence, et donc de confiance mutuelle, pour ce qui concerne les questions de cybersécurité, comme l'accès aux données de cybersécurité pour assurer le développement de bonnes pratiques et la gestion des vulnérabilités. À cette fin, le secteur de l'aviation peut adopter l'approche qu'il a déjà suivie en matière de sécurité et de sûreté, rendant semblables l'approche et la philosophie de façon compréhensible pour tous.

c) Consensus et uniformité. Dans l'ensemble de l'industrie, nous devons établir une plus grande uniformité de la cybersécurité, des normes et de la gouvernance. Il faudra du leadership sur les plans organisationnel et individuel, ainsi que la volonté d'un dialogue ouvert entre tous les intervenants.

d) Communication et collaboration. Pour mieux gérer le risque de cybersécurité à l'échelle mondiale, des liens forts doivent être créés au sein de l'industrie aérienne et avec les intervenants de l'extérieur susceptibles d'aider. Cela encouragera la collaboration dans tous les domaines, qu'il s'agisse de bonnes pratiques ou de gestion des vulnérabilités potentielles.

e) Main-d'œuvre. Par un dialogue sur les problèmes de cybersécurité et les possibilités qui s'offrent à l'industrie aérienne, nous devons inspirer la nouvelle génération de personnes et d'organisations qui sont en mesure d'apporter leur soutien en relevant le défi de la cybersécurité. De plus, il faut enseigner au personnel à reconnaître et à gérer les risques de cybersécurité, suscitant davantage de vigilance et de résilience.

2.8 Deux autres sujets ont été discutés lors de la table ronde de l'IATA sur la cybersécurité de l'aviation.

2.8.1 Enquêter sur les aspects de cybersécurité des accidents et incidents. Lors des enquêtes sur les accidents et les incidents d'aviation, il y a très peu de visibilité pour les préoccupations de cybersécurité. Alors que plusieurs systèmes d'aviation sont connectés et numériques, il a semblé à plusieurs qu'il fallait accentuer les efforts pour comprendre les moyens d'acquérir, de protéger et d'analyser les données pertinentes de cybersécurité. À défaut, l'industrie sera très peu en mesure d'assurer pour elle-même et pour les consommateurs la capacité de gérer le risque de cybersécurité.

2.8.2 En résumé, il y a beaucoup à faire pour améliorer la cybersécurité, la sûreté et la résilience de l'industrie aérienne. Mais parallèlement à ces défis, il existe un grand potentiel de collaboration et d'action dans l'ensemble du secteur, en partenariat étroit avec tous les intervenants. Il faut maintenant de l'engagement, du leadership et de l'action.

— FIN —