Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/427
EX/176
2/8/19

ASSEMBLÉE — 40e SESSION

COMITÉ EXÉCUTIF

Point 12 : Sûreté de l'aviation — Politique

PROPOSITION RELATIVE À LA GOUVERNANCE DE LA CYBERSÉCURITÉ ET DE LA RÉSILIENCE À L'OACI

(Note présentée par les États-Unis d'Amérique)

RÉSUMÉ ANALYTIQUE

La cybersécurité et la résilience dans l'écosystème de l'aviation sont des questions multidisciplinaires qui influent ou influeront sur presque tous les aspects de l'aviation mondiale. Compte tenu de la complexité de la situation et de la dépendance vis-à-vis de l'information et de la communication numériques partagées, la nécessité de la cybersécurité et de la résilience se fait plus impérieuse avec chaque avancée technologique et la modernisation continue de l'écosystème de l'aviation.

Certes, l'OACI, les États membres et l'industrie travaillent avec diligence pour résoudre les problèmes de cybersécurité et de résilience, mais l'approche actuelle de l'Organisation n'est pas régie par une gouvernance appropriée et se concentre sur les secteurs pris individuellement et diverses compétences au lieu de considérer l'écosystème mondial de l'aviation dans son ensemble.

Pour remédier à ce problème, les États-Unis d'Amérique recommandent que l'OACI crée un comité technique du Conseil sur la cybersécurité et la résilience pour centraliser la gouvernance et examiner les questions de cybersécurité et de résilience de manière appropriée dans le cadre d'une approche holistique. Ce comité gérera les politiques et l'intégration des normes du secteur tout en évaluant l'élaboration éventuelle de normes techniques et de pratiques recommandées.

Suite à donner : L'Assemblée est invitée :
a) à demander au Conseil de l'OACI de créer un nouveau comité technique du Conseil sur la cybersécurité et la résilience, comme proposé dans la présente note de travail ;
b) à demander instamment aux États de soutenir le projet de stratégie de cybersécurité de l'OACI élaboré par le groupe d'étude du Secrétariat sur la cybersécurité ;
c) à exhorter les États à soutenir les travaux du groupe d'étude sur le cadre de confiance.

Objectifs stratégiques :	La présente note de travail se rapporte aux Objectifs stratégiques : Sûreté et facilitation, Capacité et efficacité de la navigation aérienne.
Incidences financières :	Aucune.
Références :	Doc 10075, *Résolutions de l'Assemblée en vigueur*, A39-18 et A39-19 Recommandation 5.4/1 de la 13e Conférence de navigation aérienne Note de travail A40-WP/28 – *Stratégie de cybersécurité de l'OACI* Doc 7559/10, Règlement intérieur du Conseil, règle 17 a)

1. INTRODUCTION

1.1 La cybersécurité et la résilience dans l'écosystème de l'aviation sont des questions multidisciplinaires qui influent ou influeront sur presque tous les aspects de l'aviation mondiale. Comme indiqué dans les résolutions A39-18 et A39-19 de la 39e session de l'Assemblée de l'OACI, le système aéronautique mondial devient de plus en plus complexe et de plus en plus intégré à travers les technologies de l'information et de la communication. Compte tenu de cette complexité et de la dépendance vis-à-vis de l'information et de la communication numériques partagées, la nécessité de la cybersécurité et de la résilience se fait plus impérieuse avec chaque avancée technologique et la modernisation continue de l'écosystème de l'aviation.

1.2 L'importance de la cybersécurité et de la résilience est également mise en évidence dans la recommandation 5.4/1 de la treizième Conférence de navigation aérienne de l'OACI, qui invite notamment les États et l'OACI à collaborer avec l'industrie afin de mieux prendre conscience des menaces et de coopérer de manière appropriée pour les atténuer. La deuxième Conférence de haut niveau de l'OACI sur la sûreté de l'aviation a également recommandé que l'Organisation élabore une stratégie complète de cybersécurité et entreprenne une étude de faisabilité de la création d'un groupe d'experts sur la cybersécurité.

1.3 Même si l'OACI avance dans l'élaboration de sa stratégie de cybersécurité (voir la note de travail A40-WP/28), la gouvernance de la cybersécurité et de la résilience au sein de l'Organisation reste insuffisante. L'absence d'une gouvernance appropriée entraîne des inefficacités et empêche l'échange d'informations, ce qui rend impossible l'examen approprié des questions de cybersécurité et de résilience dans le cadre d'une approche globale permettant la gestion centralisée des politiques, l'intégration des normes du secteur et l'élaboration potentielle de normes techniques et de pratiques recommandées (SARP).

2. ANALYSE

2.1 La gouvernance actuelle de l'OACI en ce qui concerne la cybernétique répartit les activités entre la Direction du transport aérien (ATB), qui supervise la cybersécurité, et la Direction de la navigation aérienne (ANB), qui supervise la cyberrésilience.

2.2 L'ATB est responsable de l'élaboration des SARP et de la modification de l'Annexe 17 — *Sûreté*. Elle soutient en outre les travaux du Groupe d'experts sur la sûreté de l'aviation et du Comité de l'intervention illicite (UIC), y compris la création du Groupe d'étude du Secrétariat sur la cybersécurité (SSGC). Celui-ci coordonne les travaux sur la cybersécurité, les examens tels que celui des annexes de l'OACI visant à renforcer les SARP relatives à la cybersécurité et la promotion générale du partage de l'informations au sein de la communauté aéronautique.

2.3 L'approche de l'ATB fonctionne bien lorsque la cybersécurité est considérée comme un sujet unique centré sur la protection des systèmes essentiels contre les interférences illicites, comme indiqué à la section 4.9 de l'Annexe 17. Toutefois, l'aviation mondiale est un écosystème global comprenant de nombreux systèmes interconnectés qui influent directement sur des opérations sortant du cadre des attributions de l'ATB et de l'UIC en matière de cybersécurité.

2.4 L'ANB quant à elle, est responsable de l'élaboration et de la modification des SARP dans 17 annexes différentes traitant de la sécurité ainsi que de la capacité et de l'efficacité de la navigation aérienne. Elle appuie en outre les travaux de la Commission de navigation aérienne et de ses groupes d'experts techniques, notamment la création du groupe de travail INNOVA et du groupe d'étude sur le cadre de confiance. Celui-ci joue le rôle de coordonnateur pour le développement des interconnexions de

réseaux cyberrésilients à travers un cadre de confiance permettant le transfert mondial de données et d'informations aéronautiques essentielles aux opérations.

2.5 L'approche de l'ANB fonctionne bien lorsqu'on considère uniquement le transfert de données et d'informations opérationnelles. Toutefois, elle ne tient pas compte de la sûreté des systèmes non connectés au réseau opérationnel, mais pouvant avoir une incidence dans d'autres domaines touchant la sûreté ou l'efficacité.

2.6 Alors que la cybersécurité et la résilience sont clairement toutes deux des sujets de préoccupation de l'OACI, la structure de gouvernance actuelle divise la sécurité et la résilience, ce qui nuit à l'écosystème global de l'aviation. Les États membres et l'industrie ont pris conscience de ce problème et ont formulé des recommandations en vue de la création d'un nouveau « groupe d'experts » sur la cybernétique. Toutefois, les groupes d'experts de l'OACI ont pour objectif spécifique de proposer des solutions à des problèmes spécialisés ou d'élaborer des SARP (Doc 7984, *Instructions pour les groupes d'experts de la Commission de navigation aérienne).* La cybersécurité et la résilience sont des questions plus multidisciplinaires et plus globales que les « problèmes spécialisés » et, à l'heure actuelle, il faudrait utiliser les normes du secteur applicables à la cybernétique au lieu d'élaborer de nouvelles SARP ou une nouvelle annexe de l'OACI.

2.7 Au vu de ces considérations, la cybersécurité et la résilience devraient être reconnues pour leur impact sur l'ensemble de l'écosystème de l'aviation et donc être élevées et gérées de manière centralisée par le Conseil de l'OACI dans le cadre d'un comité technique créé à cet effet.

2.8 Conformément à la règle 17 a) de la section III du *Règlement intérieur du Conseil* (Doc 7559/10), les États-Unis d'Amérique proposent de créer un comité technique du Conseil sur la cybersécurité et la résilience. Ce document indique que le Conseil peut instituer d'autres commissions, comités ou groupes de travail, permanents ou temporaires. Un nouveau comité du Conseil peut être conçu pour examiner les aspects techniques, économiques, sociaux et juridiques de l'aviation civile internationale, dont la promotion ou la résolution nécessitent des compétences dont le Conseil ne dispose pas autrement.

2.9 Le comité technique proposé travaillera sous le contrôle direct du Conseil, qui élaborera également son mandat et sa composition conformément aux « *Instructions pour le Comité sur la cybersécurité et la résilience* ». Le SSGC et le groupe d'étude du cadre de confiance se réorganiseront sous le nouveau comité technique en tenant pleinement compte des tâches, des efforts et des coûts nécessaires pour assurer une bonne gestion dudit comité. Grâce à cette approche, le comité proposé utilisera de manière appropriée des spécialistes de diverses disciplines, y compris de la structure de travail de l'OACI, tout en évitant les inefficacités et les problèmes de communication dus à la répartition de questions complexes et interdépendantes entre plusieurs directions et bureaux ayant des priorités variées.

3. CONCLUSION

3.1 La cybersécurité et la résilience influent énormément sur l'ensemble de l'écosystème de l'aviation mondiale. L'approche proposée dans la présente note de travail permettra d'élever cette question essentielle pour la confier à un comité technique du Conseil capable de travailler sur des mesures multidisciplinaires et de tirer parti des compétences de plusieurs directions de l'OACI et de la communauté aéronautique, tout en maintenant le rythme des innovations malgré des menaces sans cesse plus nombreuses.

3.2 L'Assemblée est invitée à approuver les mesures figurant dans le résumé analytique.

— FIN —