Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/219[1]
EX/82
5/8/19

ASSEMBLÉE — 40e SESSION

COMITÉ EXÉCUTIF

Point 12 : Politique de sûreté de l'aviation

PROPOSITION RELATIVE À LA STRUCTURE DE GOUVERNANCE DE L'OACI SUR LA CYBERSÉCURITÉ

[Note présentée par le Conseil international de coordination des associations d'industries aérospatiales (ICCAIA)]

RÉSUMÉ ANALYTIQUE

La cybersécurité dans l'aviation civile est un sujet vaste, complexe et pluridisciplinaire qui englobe à la fois les technologies de l'information, la sécurité de l'aviation classique, la gestion de la sûreté et les effets sur les opérations aériennes. La cybersécurité étant un domaine transversal, les différents groupes d'experts et groupes d'étude de l'OACI ne sont pas à mêmes de coordonner des activités de ce type. Il apparaît nécessaire de mettre en place une entité de l'OACI, gouvernée par les États membres et soutenue par le secteur, qui ne sera pas contrainte par la structure organisationnelle existante de l'OACI. Cette entité devrait assurer la bonne coordination de toutes les activités liées à la cybersécurité dans l'ensemble de l'OACI, ainsi que l'interface avec les autres disciplines concernées. Elle serait chargée de l'élaboration d'une stratégie commune de l'OACI en matière de cybersécurité et d'harmoniser et de guider les travaux réalisés par les groupes d'experts et les groupes d'étude existants.

Suite à donner : L'Assemblée est invitée à :

a) demander au Conseil de créer une entité chargée de la cybersécurité de l'aviation civile, gouvernée par les États membres avec l'appui du secteur, qui pourra opérer de manière transversale afin de consolider et d'harmoniser les activités liées à la cybersécurité dans l'ensemble de l'OACI ;
b) demander au Conseil d'approuver la stratégie en matière de cybersécurité élaborée par le Groupe d'étude du Secrétariat sur la cybersécurité (SSGC), tout en reconnaissant que le SSCG n'était pas structuré pour prendre en compte la nature horizontale et transversale de la cybersécurité ;
c) appeler la Secrétaire générale à se coordonner avec les États membres et les acteurs du secteur pour harmoniser les procédures de gestion des risques liés à la cybersécurité, en tenant compte des travaux d'harmonisation déjà entrepris au niveau régional ou national ; et
d) demander au Conseil d'inviter instamment les États des différentes régions à développer des compétences en matière de gestion des crises de cybersécurité, et à se coordonner à l'échelle internationale afin d'empêcher la perte de passagers due à des incidents locaux de cybersécurité de l'aviation.

[1] Versions française, anglaise, arabe, chinoise, espagnole et russe fournies par l'ICCAIA.

Objectifs stratégiques :	La présente note de travail se rapporte aux Objectifs stratégiques suivants : sûreté ; capacité et efficacité de la navigation aérienne ; sécurité et facilitation
Incidences financières :	Les activités visées dans la présente note seront entreprises sous réserve des ressources prévues au budget-programme ordinaire de 2020-2022 et/ou provenant de contributions extrabudgétaires.
Références :	Doc 10075, Résolutions de l'Assemblée en vigueur (au 6 octobre 2016)

1. INTRODUCTION

1.1 La cybersécurité dans l'aviation civile est un sujet vaste, complexe et multidisciplinaire, qui englobe à la fois la gestion des technologies de l'information, la sécurité de l'aviation classique, la gestion de la sûreté et les effets sur les opérations aériennes.

1.2 Les activités de cybersécurité étaient traditionnellement traitées au cas par cas et à l'échelle locale. Il convient aujourd'hui au contraire de renforcer la coordination afin de s'assurer que tous les aspects sont pris en compte, sans lacunes ni recoupements. En outre, la cybersécurité concernant de nombreuses activités de l'OACI, il convient de garantir une bonne coordination entre toutes les disciplines afin de faciliter la mise en place et le fonctionnement d'un processus complet de conception et de prise de décision tenant notamment compte de la sûreté aéronautique, ainsi que de la sécurité physique et de la cybersécurité de l'aviation.

1.3 La cybersécurité étant un domaine transversal, les différents groupes d'experts et groupes d'étude de l'OACI ne sont pas à mêmes de coordonner des activités de ce type. Il apparaît nécessaire de mettre en place une entité de l'OACI, gouvernée par les États membres et soutenue par le secteur, qui ne sera pas contrainte par la structure organisationnelle et politique existante de l'OACI. Cette entité devrait assurer la bonne coordination de toutes les activités liées à la cybersécurité dans l'ensemble de l'OACI, ainsi que l'interface avec les autres disciplines concernées. Elle serait chargée de l'élaboration d'une stratégie commune de l'OACI en matière de cybersécurité et d'harmoniser et de guider les travaux réalisés par les groupes d'experts et les groupes d'étude existants.

1.4 L'idée est de réduire les frais généraux et les incidences sur l'organisation, tout en tirant le meilleur parti possible des structures existantes pour réaliser ces travaux et d'envisager cette entité comme étant chargée d'établir une stratégie et une vision et d'assurer des fonctions de direction et d'orientation. Elle serait constituée de représentants d'États membres de l'OACI ainsi que d'experts de la sécurité individuelle et sectorielle, qui travailleraient de concert pour formuler des recommandations conjointes à des fins de décision.

2. ANALYSE

2.1 Une entité centralisée chargée de la cybersécurité a le potentiel de résoudre une partie des problèmes recensés dans l'introduction, puisqu'elle pourrait répondre au besoin de gouvernance multidisciplinaire mondial de l'aviation qui caractérise les activités de cybersécurité au sein de l'OACI. Le type d'entité de l'OACI doit être choisi avec soin afin de pouvoir pleinement répondre aux besoins et objectifs de la communauté de l'aviation civile mondiale. Les avantages et les inconvénients des différentes organisations (groupes d'experts ou Comité du Conseil, par exemple) doivent être soigneusement pesés en tenant compte des besoins et objectifs décrits dans la présente note.

2.2 Avec les ressources adéquates, cette entité centralisée chargée de la cybersécurité présenterait plusieurs avantages :

- une plus large palette d'expérience des membres et d'expertise du secteur, tout particulièrement sur le plan de la cybersécurité dans l'aviation civile ;

- une approche harmonisée de la gestion des risques avec un ensemble de méthodologies approuvées par toutes les parties prenantes, s'appuyant sur l'expérience acquise aux niveaux régional et national ;

- la possibilité de créer des groupes de travail ou d'attribuer des missions aux entités existantes, en vue de concentrer les efforts sur l'élaboration de normes et pratiques recommandées, de documents d'orientation, de programmes, ainsi que sur le renforcement des capacités, l'assistance et la formation, selon les besoins ;

- la prise en compte de tous les problèmes de cybersécurité (sûreté des vols, opérations, maintenance, cybercriminalité, etc.) au sein d'une seule et même entité ; et

- une équipe diversifiée d'experts en cybersécurité et de spécialistes de la sûreté et des opérations représentant toutes les parties prenantes concernées de l'ensemble des gouvernements et du secteur. Il conviendrait d'inclure au minimum des aérodromes, des compagnies aériennes, des constructeurs et fournisseurs aéronautiques, des techniciens de maintenance et fournisseurs de services de navigation aérienne.

2.3 Compte tenu du caractère transversal et multidisciplinaire de la cybersécurité, il est recommandé d'instaurer une coordination élargie entre les différentes disciplines liées à la sûreté et la sécurité aéronautiques grâce aux solides liens qui existent entre la Commission de navigation aérienne, le Comité de l'intervention illicite, les groupes d'étude et les groupes d'experts. Cette entité parfaitement au fait de l'évolution rapide de la cybersécurité et de ses interactions avec les nouvelles technologies doit être en mesure de tirer parti de la participation de tous les experts mondiaux, qui comptent notamment des particuliers et des organisations au-delà de la liste actuelle des « organisations invitées » (https://www.icao.int/about-icao/Pages/Invited-Organizations.aspx).

2.4 Si l'on reconnaît que les concepts présentés dans la stratégie de cybersécurité élaborée par le Groupe d'étude du Secrétariat sur la cybersécurité (SSGC) constituent une base adéquate sur laquelle s'appuyer, cette entité chargée de la cybersécurité aura pour mission de concevoir et de faire appliquer un plan d'action portant sur toutes les problématiques liées à tous les domaines de la cybersécurité de l'aviation civile, tout en défendant la vision, la perspective et la stratégie de cybersécurité de l'OACI. L'entité de l'OACI chargée de la cybersécurité devra s'appuyer sur les nombreuses initiatives déjà engagées aux niveaux régional et national en vue d'accélérer la conception et l'adoption de normes et orientations. Cette entité chargée de la cybersécurité pourrait entre autres :

2.4.1 Consolider la stratégie du SSGC et harmoniser les travaux entrepris par les différents groupes et groupes d'experts (TFSG, AVSEC, etc.) en vue d'établir des principes, mesures et actions de cybersécurité au sein d'un cadre reposant sur huit piliers :

- Coopération internationale
- Gouvernance
- Législation et réglementations efficaces

- Politiques
- Partage des informations
- Déclaration mondiale des risques relatifs à la cybersécurité dans l'aviation
- Gestion des incidents, impact opérationnel et poursuite des activités
- Renforcement des capacités, formation et culture axée sur la cybersécurité

2.4.2 Faire avancer les travaux du Groupe de travail sur les menaces et les risques (WGTR), procéder à l'évaluation des risques relatifs à la cybersécurité dans l'aviation civile, éventuellement en tant que groupe de travail de cette nouvelle entité ou en étant affecté aux bureaux appropriés. Il est impératif de mettre en place une orientation et des critères afin de garantir des résultats d'analyses comparables lorsque ceux-ci sont utilisés par différents États membres et organisations.

2.4.3 Collaborer avec le groupe d'étude sur le cadre de confiance pour favoriser l'aboutissement des travaux et, au terme des deux premières années d'existence, poursuivre l'harmonisation et l'évolution en répartissant correctement les missions entre les bureaux ou selon les besoins.

3. CONCLUSION

3.1 La coordination et la coopération internationales sont nécessaires pour harmoniser les politiques et les réglementations afin de faciliter l'interopérabilité de la cybersécurité et la continuité des opérations dans le monde. Les différents groupes d'experts et groupes d'étude de l'OACI ne sont pas à même de coordonner des activités de cybersécurité. Il apparaît nécessaire de mettre en place une entité de l'OACI, gouvernée par les États membres et soutenue par le secteur, qui ne sera pas contrainte par la structure organisationnelle existante de l'OACI. Cette entité devrait assurer la bonne coordination de toutes les activités liées à la cybersécurité dans l'ensemble de l'OACI, ainsi que l'interface avec les autres disciplines concernées.

— FIN —