Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/172[1]
EX/70
1/8/19

ASSEMBLÉE — 40e SESSION

COMITÉ EXÉCUTIF

Point 12 : Sécurité de l'aviation — Politique

CYBERRÉSILIENCE

[Note présentée par la Civil Air Navigation Services Organisation (CANSO)]

RÉSUMÉ ANALYTIQUE

La cybersécurité constitue un enjeu majeur pour l'aviation et ne cesse de prendre de l'importance en raison des diverses initiatives, telles que la gestion des informations à l'échelle du système (SWIM), qui augmentent l'interopérabilité et l'ouverture des systèmes. À l'heure actuelle, le groupe d'étude du secrétariat sur la cybersécurité (SSGC) de l'OACI examine les mesures que celle-ci devrait prendre pour assurer la cyberrésilience. Cette responsabilité est confiée à la Direction du transport aérien de l'OACI (ATB), avec le soutien de la Direction de la navigation aérienne de l'OACI (ANB).

Le pouvoir de gouvernance des États, de la Commission de la navigation aérienne (ANC) et du Conseil de l'OACI est donc limité. Le SSGC est actuellement composé d'une cinquantaine de participants. Le processus semble manquer de rapidité, dû à l'incapacité d'un groupe d'étude de secrétariat (GSS) à proposer des SARP (normes et pratiques recommandées) et à son absence de mandat pour coordonner l'activité de l'ensemble des commissions ou groupes de travail liés à la cybersécurité. Le SSGC vise à fournir des conseils, tandis que le suivi est laissé à l'appréciation du Secrétariat général.

Compte tenu de l'importance de la cyberrésilience et du besoin d'une action rapide, un moyen plus efficace de s'attaquer au problème est nécessaire. Pour améliorer la gouvernance et accélérer le processus d'introduction d'instructions et, le cas échéant, de SARP, le SSGC actuel devrait être converti en groupe d'experts OACI sous la supervision du Conseil de l'OACI. Le nouveau « Groupe d'étude-cadre de confiance » devrait être placé sous la supervision de ce nouveau Groupe d'experts sous la forme d'un groupe de travail.

Un nouveau Groupe d'experts sur la résilience, la sûreté et la sécurité cybernétiques (CRSSP) devrait proposer des SARP et instructions neuves ou adaptées pour assurer la cohérence et l'homogénéité de toutes les activités cybernétiques liées à l'aviation au sein des groupes d'experts de l'OACI et des autres groupes d'experts.

[1] Versions française, anglaise, arabe, chinoise, espagnole et russe fournies par la CANSO.

Suite à donner : L'Assemblée est invitée : a) à reconnaître la nécessité d'une approche multidisciplinaire rapide et bien gérée de la cybersécurité ; b) à exhorter le Conseil de l'OACI à créer un « Groupe d'experts sur la résilience, la sûreté et la sécurité cybernétiques » (CRSSP) sous la gouvernance du Conseil de l'OACI et du Comité du transport aérien (ATC) ; c) à exhorter le Conseil de l'OACI à créer un groupe de travail subordonné au nouveau CRSSP pour établir les bases du Cadre de confiance de l'aviation.	
Objectifs stratégiques	La présente note de travail se rapporte aux Objectifs stratégiques : *Sécurité* ; *Capacité et efficacité de la navigation aérienne* ; *Sécurité et facilitation.*
Incidences financières :	
Références :	

1. INTRODUCTION

1.1 À l'instar des autres industries ayant adopté « la révolution numérique », l'aviation doit préserver la confiance des parties prenantes en discernant précisément les vulnérabilités et les opportunités, et en comprenant les menaces adverses. Une fois connecté et numérisé, le secteur de l'aviation civile doit faire face, notamment, aux défis suivants :

1.2 Les systèmes et services de l'industrie de l'aviation étant de plus en plus connectés, les systèmes sont de plus en plus vulnérables et exposés aux attaques rivales potentielles.

1.3 Vu l'importance croissante de la technologie et de l'environnement cybernétique pour l'industrie de l'aviation, une réforme mondiale sera nécessaire pour comprendre et surmonter les différences culturelles entre les deux industries. Le développement d'une culture commune et l'examen commun des défis et des solutions potentielles exigeront une coopération interdisciplinaire.

1.4 La perception de la menace liée à un environnement numérique sera essentielle à la compréhension et à la gestion des risques. Il est nécessaire que tous les acteurs de l'industrie de l'aviation atteignent le même niveau de perception et de compréhension afin de s'attaquer au risque potentiel et de promouvoir un dialogue collaboratif qui valorise les perspectives multiples.

1.5 L'industrie de l'aviation jouit de décennies d'expérience dans la résolution des problèmes de sûreté et de sécurité, mais le défi que pose la cybersécurité est relativement nouveau. La mise au point et le remplacement des systèmes d'aviation pourraient prendre plus de temps que de développer des capacités, et ainsi compromettre la précision de l'évaluation des risques et des modèles de menace.

1.6 Les investissements dans la gestion du trafic aérien (ATM) rapportent déjà d'importants bénéfices, mais l'utilisation de technologies de pointe telles que les systèmes de positionnement mondial (GPS), la communication numérique et la surveillance dépendante automatique en mode diffusion (ADS-B) nous contraint à gérer les vulnérabilités qui découlent de ces technologies et encourager la cyberrésilience.

2. DISCUSSION

2.1 Au cours des dernières années, l'OACI a fait des recherches sur la cybersécurité et la cyberrésilience dans différents domaines. Le Groupe d'experts de la sûreté de l'aviation (AVSECP) s'est penché sur les vulnérabilités du système d'aviation liées aux actes d'ingérence illégale. Le GT sur les menaces et les risques de l'AVSECP a déclaré à plusieurs reprises que le risque de cyber-activités d'ingérence illégale est faible.

2.2 Pour mener des recherches sur la possibilité d'un réseau de confiance dans l'aviation, le Secrétariat de l'OACI a mis en place l'équipe de découverte « INNOVA ». Ce groupe d'experts a créé un concept d'opérations (CONOPS) pour un réseau mondial aérien résilient et interopérable. En mai 2019, le groupe INNOVA a été transformé en Groupe d'étude-cadre de fiducie (TFSG). Ce groupe élargit ses travaux à travers différents groupes de travail définissant les exigences d'identification ainsi que les besoins actuels et futurs d'un tel réseau. Un autre groupe de travail subordonné au TFSG développe un concept de cadre commun de confiance numérique et est chargé d'orienter l'évolution afin de faciliter un échange d'informations sécurisé, résilient et homogène dans un environnement numériquement connecté pour permettre les opérations actuelles et futures.

2.3 L'OACI a créé le Groupe d'étude du secrétariat sur la cybersécurité (SSGC) sous la direction du Directeur adjoint de la sûreté aérienne et de la facilitation (DA/ASF). Le SSGC est surveillé par le Groupe de haute direction du secrétariat concernant les problèmes communs de sûreté et de sécurité, lequel est présidé par le Secrétaire général de l'OACI.

2.4 L'approche actuelle au sein de l'OACI ne permet pas une approche efficace et holistique. Un groupe d'étude du secrétariat doit transmettre ses conclusions aux groupes spéciaux distincts de l'OACI, lesquels évalueront et décideront si la création d'une SARP est requise à ce sujet. De plus, toutes les SARP liées aux technologies de l'information (TI) sont réparties sur la quasi-totalité des 19 annexes de l'OACI. Il serait plus efficace de créer un Groupe d'experts sur la résilience, la sûreté et la sécurité cybernétiques (CRSSP) qui relèverait directement du Comité du transport aérien (ATC) et du Comité de l'intervention illicite (UIC). Ce nouveau groupe d'experts établirait une approche multidisciplinaire et holistique pour l'ensemble de l'OACI et consoliderait l'ensemble des travaux de l'OACI sur les problèmes cybernétiques.

2.5 Le CRSSP devrait envisager la rédaction d'une annexe dédiée aux problèmes liés à la résilience, à la sûreté et à la sécurité cybernétiques dans le secteur de l'aviation, et fournir des conseils à ce sujet. L'avantage d'une annexe dédiée est que tous les problèmes d'ordre cybernétique seraient regroupés comme dans l'annexe 19 relative à la gestion de la sécurité. Un autre avantage sera la possibilité, pour les États, de transmettre directement toutes les SARP et leurs éventuelles modifications aux experts TI. Elle soulignerait également l'importance de la résilience, de la sûreté et de la sécurité cybernétiques dans le monde de l'aviation.

2.6 Le TFSG actuel devrait travailler directement sous la supervision du CRSSP en tant que groupe de travail distinct.

3. CONCLUSION

3.1 La méthode de travail actuelle de l'OACI pour traiter les problèmes de résilience, de sûreté et de sécurité cybernétiques n'est pas suffisamment coordonnée et manque d'efficacité.

3.2 La création d'un groupe d'experts multidisciplinaire pour tous les problèmes liés à la résilience, la sûreté et la sécurité cybernétiques améliorerait la coordination et l'efficacité des enquêtes et des défenses contre les problèmes de résilience, de sûreté et de sécurité cybernétiques dans le secteur de l'aviation. Pour assurer une supervision efficace et une approche multidisciplinaire, le Groupe d'experts devrait relever directement du Conseil de l'OACI, de l'ATC et de l'UIC. Les résultats du Groupe d'experts devraient être discutés lors de réunions combinées entre l'ATC et l'UIC afin de garantir une coordination holistique.

3.3 La création d'une annexe distincte pour les problèmes liés à la résilience, à la sûreté et à la sécurité cybernétiques soulignera l'importance de ces facteurs pour le système de numérisation de l'aviation et fournira un aperçu complet de toutes les SARP associées par l'intermédiaire des annexes de l'OACI.

3.4 L'Assemblée est invitée à approuver les actions du Résumé analytique.

— FIN —