Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A41-WP/374
EX/170
2/8/22

ASSEMBLÉE — 41e SESSION

COMITÉ EXÉCUTIF

Point 14 : Sûreté de l'aviation – Politique

ÉTAT DE PRÉPARATION DU PERSONNEL EN MATIÈRE DE CYBERSÉCURITÉ DANS LES SERVICES DE NAVIGATION AÉRIENNE EN TEMPS NORMAL COMME EN PÉRIODE DE CRISE

[Note présentée par la Commission africaine de l'aviation civile (CAFAC) au nom de 54 États africains[1]]

RÉSUMÉ ANALYTIQUE

La cybersécurité et la cyber-résilience de l'aviation ont gagné en importance au fil du temps, et les cyber-attaques perpétrées avant et pendant la pandémie de COVID-19 ont montré à maintes reprises qu'il était urgent de s'en préoccuper. Outre l'impact catastrophique de la COVID-19 sur l'économie mondiale de façon générale, et sur l'aviation en particulier, il y a eu un nombre accru de cyber-attaques pendant la pandémie. Le renforcement des capacités, la formation et la culture de la cybersécurité constituent l'un des principaux piliers de la Stratégie de cybersécurité de l'OACI et il faut également tenir compte de l'importance que revêtent les infrastructures de navigation aérienne dans le secteur de l'aviation. Par conséquent, la présente note souligne qu'il est fondamental de se pencher sur le renforcement des capacités, la formation et la culture de la cybersécurité aussi bien en temps normal qu'en période de crise.

Suite à donner : L'Assemblée est invitée à :

a) prendre note des renseignements fournis dans la présente note ; et
b) demander à l'OACI de confier au Groupe d'experts de la cybersécurité la tâche de proposer des initiatives en matière de renforcement des capacités, de formation et de culture de la cybersécurité en période de crise.

Objectifs stratégiques :	La présente note de travail se rapporte à l'objectif stratégique *Sûreté et facilitation*

[1] Afrique du Sud, Algérie, Angola, Bénin, Botswana, Burkina Faso, Burundi, Cabo Verde, Cameroun, Comores, Congo, Côte d'Ivoire, Djibouti, Égypte, Érythrée, Eswatini, Éthiopie, Gabon, Gambie, Ghana, Guinée, Guinée-Bissau, Guinée équatoriale, Kenya, Lesotho, Libéria, Libye, Madagascar, Malawi, Mali, Maroc, Maurice, Mauritanie, Mozambique, Namibie, Niger, Nigéria, Ouganda, République centrafricaine, République démocratique du Congo, République-Unie de Tanzanie, Rwanda, Sao Tomé-et-Principe, Sénégal, Seychelles, Sierra Leone, Somalie, Soudan, Soudan du Sud, Tchad, Togo, Tunisie, Zambie et Zimbabwe

Incidences financières :	
Références :	*Stratégie pour la cybersécurité de l'aviation* *Plan d'action pour la cybersécurité* Résolution A40-10 de l'Assemblée – Cybersécurité dans l'aviation civile Doc 9985, *Manuel de sûreté de la gestion du trafic aérien*

1. INTRODUCTION

1.1 La technologie et les cyber-systèmes sont devenus essentiels dans la société moderne et font partie intégrante de nombreuses activités qui dépendent désormais des technologies de l'information. Par conséquent, la cybersécurité et la cyber-résilience de l'aviation sont devenues de plus en plus importantes avec le temps, et les cyber-attaques perpétrées avant et pendant la pandémie de COVID-19 ont montré à maintes reprises qu'il était urgent de s'en préoccuper.

1.2 Compte tenu du fait que la cybersécurité est par nature multidimensionnelle et multidisciplinaire, et sachant que les cyber-attaques peuvent se produire simultanément dans de nombreux domaines différents et se propager rapidement, il est devenu impératif d'adopter une approche commune et de définir une stratégie mondiale en matière de cybersécurité. L'OACI a donc décidé d'élaborer et de publier la Stratégie pour la cybersécurité de l'aviation dans le but d'établir un cadre de cybersécurité solide et durable.

1.3 Cette stratégie comprend sept piliers : coopération internationale, gouvernance, législation et règlements efficaces, politique de cybersécurité, partage de l'information, gestion des incidents et planification d'urgence, mais aussi **renforcement des capacités, formation et culture de cybersécurité**.

1.4 La 40e session de l'Assemblée de l'OACI a permis d'adopter la résolution A40-10 – *Cybersécurité dans l'aviation civile* présentant une approche horizontale, transversale et fonctionnelle pour aborder la question de la cybersécurité. Dans cette résolution, les États sont invités à mettre en œuvre la Stratégie de cybersécurité de l'OACI car il est fondamental et urgent de protéger les systèmes et les données des infrastructures critiques de l'aviation civile contre les cyber-menaces.

1.5 Le Plan d'action de l'OACI pour la cybersécurité (CyAP) a été élaboré pour proposer une série de principes, de mesures et d'activités permettant d'atteindre les objectifs des sept piliers de la stratégie. Ce cadre de coopération solide sous-tend la collaboration entre États, secteur aéronautique, parties prenantes et OACI dans le but de développer les capacités d'identification, de prévention, de détection, de riposte et de reprise en cas de cyber-attaque contre l'aviation civile.

1.6 Le Groupe d'experts de la cybersécurité vient d'être établi dans le cadre du nouveau mécanisme de gouvernance mis en place pour aborder les questions de cybersécurité au sein de l'OACI. Les activités prévues dans son mandat correspondent au Programme des travaux de cybersécurité de l'aviation, l'objectif du Groupe étant d'élaborer des dispositions, notamment des normes et pratiques recommandées (SARP) mais aussi des procédures visant à protéger l'aviation civile contre les cyber-menaces, tout en tenant dûment compte des incidences économiques, opérationnelles et autres que peuvent avoir de telles dispositions.

1.7 L'OACI a élaboré des éléments indicatifs pour la culture de la cybersécurité (« culture de la cybersécurité dans l'aviation civile »).

2. ANALYSE

2.1 L'apparition de la pandémie de coronavirus en 2019 (COVID-19) a modifié notre mode de vie de manière définitive. Les États ont pris de nombreuses mesures (distanciation sociale, apprentissage à distance, travail à distance, etc.) pour enrayer la propagation de la COVID-19 en limitant les contacts physiques entre les personnes. Cela a entraîné une évolution très rapide en matière de télétravail, visioconférences, transformation numérique, innovation et autres technologies en ligne qui constituent désormais la « nouvelle normalité ». Par ailleurs, outre l'impact catastrophique de la COVID-19 sur l'économie et la société internationales, il y a eu pendant la pandémie un nombre accru de cyber-attaques qui ont elles aussi touché la société et les entreprises.

2.2 Les services de navigation aérienne font partie des infrastructures essentielles dans le domaine de l'aviation. Ils doivent par conséquent accorder une attention particulière à la transition des systèmes analogiques au sol vers des systèmes numériques basés dans l'espace devant permettre aux installations de navigation aérienne de s'adapter à la densité toujours croissante du trafic aérien.

2.3 Le renforcement des capacités, la formation et la culture de la cybersécurité sont au cœur de la Stratégie de cybersécurité visant à rendre cyber-résilients les systèmes d'aviation. Cependant, le cadre actuel ne permet pas à l'OACI de traiter de la cybersécurité en cas de crise comme celle de la pandémie de COVID-19 ou d'autres pandémies ou crises à venir.

3. CONCLUSION

3.1 Le renforcement des capacités, la formation et la culture de la cybersécurité sont des éléments essentiels pour la cyber-résilience des systèmes d'aviation, aussi bien en temps normal qu'en période de crise. Par conséquent, une résolution de l'OACI devrait porter sur la question fondamentale de la cybersécurité et le nouveau Groupe d'experts de la cybersécurité devrait en tenir compte dans ses travaux.

— FIN —