Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A41-WP/74
EX/36
26/7/22

ASSEMBLÉE — 41e SESSION

COMITÉ EXÉCUTIF

Point 14 : Sûreté de l'aviation — Politique

ÉLABORATION D'UN CADRE POUR LA CYBERSÉCURITÉ

(Note présentée par la Tchéquie, au nom de l'Union européenne et de ses États membres[1], des autres États membres de la Conférence européenne de l'aviation civile[2], des États membres de la Commission africaine de l'aviation civile[3] et d'EUROCONTROL)

RÉSUMÉ ANALYTIQUE

La cybersécurité continue de gagner en importance, à mesure que les nouvelles technologies et une plus grande utilisation des technologies de l'information et des systèmes opérationnels numériques créent de nouvelles vulnérabilités ainsi que de nouvelles possibilités. Une meilleure connaissance du cyberdomaine révèle aussi un certain nombre de défis spécifiques, qui mettent en évidence la nécessité de promouvoir une approche distincte de la réduction des risques et d'avancer dans cette direction. L'importance croissante de la cybersécurité souligne aussi l'impérieuse nécessité que les États et l'OACI intensifient leurs efforts en vue d'élaborer un cadre pour la cybersécurité, et de développer une culture de la cybersécurité et la formation qui doit l'accompagner.

---

1 Allemagne, Autriche, Belgique, Bulgarie, Croatie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Suède et Tchéquie.

2 Albanie, Arménie, Azerbaïdjan, Bosnie-Herzégovine, Géorgie, Islande, Moldova, Monaco, Monténégro, Macédoine du Nord, Norvège, Royaume-Uni, Saint-Marin, Serbie, Suisse, Türkiye et Ukraine.

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

Suite à donner : L'Assemblée est invitée à : a) demander à l'OACI de réfléchir aux étapes nécessaires pour avancer vers des orientations relatives à l'évaluation des risques de cybersécurité pour l'aviation, compte tenu des acteurs concernés, de la nécessité d'une perspective transversale holistique et des facteurs particuliers décrits dans la présente note de travail ; b) demander à l'OACI d'achever la compilation des normes et pratiques recommandées (SARP) pertinentes et d'autres bases juridiques internationales sur lesquelles les États et organisations puissent s'appuyer pour prendre en compte les cyberrisques dans leur dispositif de l'aviation ; c) demander à l'OACI et à ses États membres d'intensifier leurs efforts pour promouvoir une culture et des activités dédiées à la cybersécurité qui favorisent le développement des ressources humaines et de la capacité nécessaires pour gérer la cybersécurité et la cyberrésilience de l'aviation civile ; d) demander à l'OACI d'envisager d'organiser des exercices de cybersécurité aux niveaux mondial et régional.	
Objectifs stratégiques :	La présente note de travail se rapporte à l'objectif stratégique *Sûreté et facilitation*.
Incidences financières :	
Références :	

1. INTRODUCTION

1.1 À sa 40e session, l'Assemblée de l'OACI a adopté la Résolution A40-10 – Cybersécurité *dans l'aviation civile*, qui aborde la cybersécurité selon une approche horizontale, transversale et fonctionnelle, réaffirme l'importance et l'urgence de protéger les systèmes et les données des infrastructures critiques de l'aviation civile contre les cybermenaces et invite les États à mettre en œuvre la Stratégie de cybersécurité de l'aviation (octobre 2019). Cette stratégie est mise en œuvre selon le plan d'action pour la cybersécurité et avec le concours du Groupe d'experts de la cybersécurité, nouvellement créé, qui s'appuie sur les travaux du Groupe d'étude du Secrétariat sur la cybersécurité.

1.2 La transformation numérique, qui produit de profonds effets sur l'économie et remodèle le secteur de l'aviation, confère à l'enjeu de la cybersécurité une importance toujours plus grande. La cybersécurité continue aussi d'interpeller tous les secteurs d'activité au terme de la pandémie de COVID-19. Les entreprises ont davantage recours aux modalités virtuelles pour mener leurs activités, ce qui peut les rendre plus vulnérables aux cybermenaces. D'où la nécessité d'intensifier les efforts pour élaborer un cadre de cybersécurité qui tienne compte de ses spécificités.

2. LA CYBERSÉCURITÉ COMPORTE DES ÉLÉMENTS PARTICULIERS À PRENDRE EN COMPTE DANS LA DÉFINITION D'UNE APPROCHE DE LA GESTION DES RISQUES

2.1 La cybersécurité doit faire face à un profil de menace unique, qui comprend non seulement les groupes terroristes cherchant à perpétrer des attaques directes faisant un très grand nombre de victimes, mais aussi à divers autres acteurs – grands groupes organisés, militants, pirates informatiques -- et motivations -- causer des perturbations, exercer des contraintes, faire une démonstration de force, attirer l'attention des médias ou se procurer des gains financiers. Ces attaques peuvent, intentionnellement ou non, toucher l'aviation civile et éventuellement même mettre en péril la sécurité et se répercuter sur le secteur directement ou indirectement.

2.2 La gestion des cyberrisques devrait aussi prendre en compte d'autres éléments comme le nombre important de prestataires de services non spécifiques à l'aviation qui interviennent dans le système de l'aviation et qui peuvent avoir une compréhension différente des besoins et des risques de cybersécurité.

2.3 Le cyberespace se caractérise aussi par une réglementation gouvernementale susceptible de chevaucher plusieurs secteurs, sans comporter de volet distinct pour l'aviation.

2.4 Les considérations qui précèdent mettent en évidence la nécessité de définir une approche spécifique de l'évaluation des risques de cybersécurité, dans laquelle :

a) les compétences nécessaires, en particulier en ce qui concerne les vulnérabilités et les mesures d'atténuation des risques, doivent être associées à une connaissance et une expérience de l'aviation et des technologies de l'information ;
b) la portée de l'évaluation doit être clairement définie et centrée sur la sécurité, la sûreté et la résilience des fonctions critiques, en englobant, de façon transversale, les différents exploitants, entités et disciplines ;
c) l'évaluation des risques peut déceler de possibles failles du point de vue (mondial) de la sécurité de l'information, afin de dûment y remédier.

3. ÉLABORER UN CADRE DE CYBERSÉCURITÉ QUI PRENNE EN COMPTE LES SPÉCIFICITÉS DE L'AVIATION

3.1 Dans l'élaboration d'un cadre de cybersécurité, le secteur de l'aviation doit définir des approches qui non seulement chevauchent les limites traditionnelles des disciplines de l'aviation (comme la nécessité à la fois d'une perspective globale (p. ex., ATM) et d'une perspective individuelle, par vol), mais tiennent également compte du positionnement différent des secteurs extérieurs à l'aviation et de la réglementation gouvernementale (non spécifique à l'aviation) évoquée aux paragraphes 2.2 et 2.3 ci-dessus. C'est impératif pour assurer la cohérence et éviter le double emploi, les lacunes et, pour les États et les exploitants, une charge de réglementation ou de supervision inutile dans la mise en œuvre du cadre de cybersécurité.

3.2 Le secteur de l'aviation est bien placé pour tirer parti du rôle, des responsabilités et des procédures du dispositif actuel de l'aviation internationale. Les SARP de l'OACI relatives à la sûreté et à la sécurité de l'aviation constituent une base solide sur laquelle les pouvoirs publics et les organisations peuvent s'appuyer. Il en va de même des mécanismes de partage d'information et de compte rendu. Il existe aussi des instruments internationaux de droit aérien concernant la criminalisation des actes mettant en péril la sécurité, qui peuvent être utilisés dans une certaine mesure.

3.3 Les États et organisations sont encouragés à examiner les documents pertinents de l'OACI relatifs à la cybersécurité et à mettre en œuvre les SARP correspondantes. Il importe également que les États et organisations repensent leurs dispositifs actuels de sûreté et de sécurité de l'aviation ainsi que l'architecture de droit pénal de l'aviation dans une optique numérique afin de maintenir l'actualité et la bonne coordination des rôles et responsabilités.

4. CRITICITÉ DE L'ÉLÉMÉNT HUMAIN DANS LA CYBERSÉCURITÉ

4.1 L'élément humain est au cœur de la cybersécurité, comme en témoigne la Stratégie de cybersécurité de l'aviation de l'OACI (2019).

4.2 La transformation numérique et l'interconnectivité croissantes du système de l'aviation appellent une intensification des efforts pour répondre à une demande de plus en plus importante en matière de sensibilisation, de formation, d'actualisation des cursus universitaires et de personnel doté de compétences transversales en aviation et en cybersécurité.

4.3 Le Secrétariat de l'OACI a lancé un premier cours sur la cybersécurité et la cyberrésilience, intitulé « Fondements de la cybersécurité de l'aviation – animation et gestion technique », ainsi qu'un cours sur la gestion des risques de sûreté dans l'ATM, élaboré en partenariat avec EUROCONTROL. Il y aurait lieu de prendre exemple sur ces initiatives louables et d'en tirer les enseignements.

4.4 Comme cela est observé dans la Stratégie de cybersécurité de l'aviation de l'OACI, les exercices de cybersécurité sont un moyen utile de tester l'état de cyberrésilience et de déterminer les améliorations à y apporter, et ils sont par conséquent vivement encouragés. Indépendamment des exercices menés au niveau de chaque État européen, l'Europe a acquis une expérience au niveau régional dont elle peut

faire profiter la communauté internationale de l'aviation.[4] L'OACI est encouragée à étudier les possibilités d'organiser de tels exercices.

4.5 Comme l'a mis en évidence l'*Année de la culture de la sûreté*, il est essentiel d'élargir la notion de culture de la sûreté et de la sécurité au-delà du monde physique. Les États et organisations sont encouragés à s'inspirer des réalisations de l'Année de la culture de la sûreté pour promouvoir une culture de la cybersécurité et partager les meilleures pratiques à cet égard. L'OACI devrait favoriser les initiatives en ce sens, notamment en élaborant des éléments indicatifs.

— FIN —

[4] « Cyber Europe 2018 », organisé par l'Agence de l'Union européenne pour la cybersécurité (ENISA), s'adresse aux professionnels et aux organisations intervenant dans des activités de sécurité de l'information dans le secteur de l'aviation ; la Cellule européenne de coordination de l'aviation en situation de crise (CECAC) a organisé un exercice de gestion de crise en 2018 à la suite d'une cyberattaque visant le logiciel d'un dispositif de poursuite de surveillance et elle prépare un exercice de gestion de crise pour 2022 qui simulera une panne de grande ampleur de l'infrastructure européenne de réseaux numériques à la suite d'une cyberattaque ; l'Agence de l'Union européenne pour la sécurité aérienne organise également des exercices de cybersécurité.