



NOTE DE TRAVAIL

ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 13 : Sûreté de l'aviation — Politique

PLANS D'URGENCE ET EXERCICES DE CYBERSÉCURITÉ COMME MOYENS DE
RENFORCER LA RÉSILIANCE AUX CYBERMENACES

(Note présentée par la République du Brésil)

RÉSUMÉ ANALYTIQUE

La note de travail met l'accent sur la nécessité d'établir des plans d'urgence pour les systèmes essentiels utilisés par l'aviation civile, comme l'indique le Plan d'action pour la cybersécurité de l'OACI correspondant au pilier 6 de la Stratégie de cybersécurité de l'aviation de l'OACI, ainsi que sur l'amélioration des plans à la suite d'exercices de formation simulant des cyberattaques basés sur les caractéristiques réelles des systèmes et sur des faits déjà observés qui pourraient conduire à ces attaques, comme l'indique le Plan d'action pour la cybersécurité de l'OACI correspondant au pilier 7 de la Stratégie. Elle souligne l'évolution des cyberattaques dans l'aviation civile ainsi que l'importance des exercices et des plans d'urgence connexes.

Suite à donner : L'Assemblée est invitée à encourager les États membres à :

- favoriser l'établissement de plans de gestion des cyberincidents concernant les infrastructures essentielles de l'aviation ;
- organiser régulièrement des exercices de cybersécurité, avec la participation des pouvoirs publics et des parties prenantes du secteur privé.

<i>Objectifs stratégiques :</i>	La présente note de travail se rapporte à l'objectif stratégique <i>Chaque vol est sûr et sécurisé</i>
<i>Incidences financières :</i>	Sans objet.
<i>Références :</i>	Pilier 6 (Gestion des incidents et planification d'urgence) et pilier 7 (Renforcement des capacités, formation et culture de cybersécurité) de la Stratégie de cybersécurité de l'aviation de l'OACI.

1. INTRODUCTION

1.1 Les cybermenaces constituent un défi important et croissant pour le secteur de l'aviation civile, système mondial intrinsèquement interconnecté où les vulnérabilités peuvent contribuer à la propagation rapide de logiciels malveillants et entraîner des répercussions généralisées à l'échelle planétaire. Si les progrès technologiques ont procuré de nombreux avantages à l'aviation, ils ont également donné lieu à l'émergence d'un paysage de cybermenaces en constante évolution en raison de la forte dépendance envers les infrastructures numériques. Reconnaissant ce besoin urgent d'assurer la cyberprotection et la cyberrésilience des systèmes aéronautiques essentiels, la Stratégie de cybersécurité de l'aviation de l'OACI définit des principes, des mesures et des actions fondés sur sept piliers fondamentaux.

1.2 La présente note de travail entend donc donner un aperçu de certaines mesures prises par le Brésil pour renforcer la cyberrésilience dans les situations où les piliers 6 (gestion des incidents et planification d'urgence) et 7 (renforcement des capacités, formation et culture de cybersécurité) de la Stratégie de cybersécurité de l'aviation de l'OACI peuvent contribuer à la cyberprotection des actifs importants qui servent au contrôle du trafic aérien. En intégrant ces deux piliers, l'aviation civile peut mettre en place une défense complète et adaptable qui, loin de se contenter de réagir aux menaces, prévient et atténue de façon proactive leurs incidences, la sécurité et la fiabilité continues du transport aérien s'en trouvant garanties.

1.3 Le pilier 6 comprend des procédures de reprise solides, assorties de plans d'urgence clairs et éprouvés qui permettent de lancer immédiatement les procédures de restauration des systèmes et des données compromis, de façon à assurer une perturbation minimale du contrôle du trafic aérien, des opérations au sol et des services aux passagers. Il s'agit notamment de sauvegardes, de systèmes de rechange et de mesures de reprise détaillées.

1.4 Le pilier 7 traite de la sensibilisation et de la formation de toutes les parties prenantes intervenant dans le contrôle du trafic aérien, en dotant chacun, des contrôleurs aériens au personnel de maintenance au sol, des moyens nécessaires pour réagir à un cyberincident et en leur expliquant leur rôle dans le maintien d'un environnement sûr et sécurisé. Une culture solide de cybersécurité signifie que chacun comprend qu'il est potentiellement en première ligne de défense. De même, l'apprentissage et l'adaptation continus sont importants, car il faut reconnaître que le paysage des cybermenaces est en constante évolution et s'engager à s'adapter aux nouvelles stratégies et technologies de cybersécurité. Il s'agit donc de ne jamais se reposer sur ses lauriers et de chercher en permanence à s'améliorer.

1.5 Ces principes sont essentiels pour resserrer la collaboration entre les autorités chargées de la cybersécurité de l'aviation civile et les autres parties prenantes afin de réagir aux cyberattaques, en établissant un scénario solide dans lequel les plans d'urgence constituent un moyen de faire face à ces actions malveillantes. Le document devrait traiter de la coordination de l'ensemble des acteurs, en présentant tous les mécanismes qui seront disponibles pour rétablir le fonctionnement normal après la compromission de chaque système, et en soulignant les exigences essentielles à la mise en œuvre des mesures d'intervention, ce qui contribuera à rendre l'écosystème de l'aviation mondiale plus sûr et plus résilient.

2. ANALYSE

2.1 Chaque jour, les médias font état de tentatives de cyberattaques, dont quelques-unes aboutissent et d'autres ne sont même pas signalées parce qu'elles ont été déjouées grâce aux différentes mesures de protection mises en place par les entreprises et les organisations pour affronter ces attaques

quotidiennes. Cette réalité n'est pas différente dans le secteur de l'aviation. Les attaquants recherchent principalement des vulnérabilités non corrigées pour tenter d'envahir les systèmes, de les modifier et d'y voler des informations, généralement aux fins de réaliser des gains financiers.

2.2 Le Brésil, par l'intermédiaire de la DECEA, s'emploie à mettre en place des mesures visant à rendre plus résilient le système brésilien de contrôle de l'espace aérien face aux cybermenaces qui prennent chaque jour davantage d'ampleur. Ainsi, en accord avec la conception qu'a l'OACI de cette question et conformément à deux des piliers cités dans la stratégie de cybersécurité de l'Organisation, la DECEA encourage des exercices destinés à former les équipes d'intervention en cas d'incident issues des organismes de contrôle de l'espace aérien. Outre leur contribution à la formation des équipes, ces exercices permettent aussi de déceler les failles de cybersécurité résultant de la combinaison de systèmes et d'applications mis au point pour répondre aux exigences des activités de contrôle du trafic aérien. Les résultats de ces exercices de formation sont réunis dans des rapports qui sont adressés aux équipes chargées d'améliorer les systèmes et le plan d'urgence.

2.3 S'agissant des exercices, chaque simulation de situation est accompagnée d'informations détaillées fournies par les experts chargés de la maintenance de chaque système afin de garantir la fiabilité des situations qui reposent sur des événements réels. Il s'ensuit que les actions se rapprochent davantage d'une situation réelle et permettent une évaluation plus précise afin de dégager des améliorations efficaces pour les mesures adoptées, pour chaque système (failles relevées) et pour le plan lui-même.

2.4 Un autre pilier de la stratégie de cybersécurité de l'OACI, qui concerne la gestion des incidents et les plans d'urgence, sert de base à la préparation des plans d'urgence associés à chaque système essentiel utilisé pour contrôler l'espace aérien brésilien. Toutes les informations nécessaires pour orienter les actions vers le rétablissement des fonctionnalités offertes par chaque système aux différents niveaux du contrôle du trafic aérien sont décrites dans le document, tout comme les différents acteurs participant aux interventions, la coordination requise étant assurée afin de minimiser les indisponibilités et les incidences sur les usagers du transport aérien.

2.5 Les plans d'urgence sont élaborés sur la base de normes internationales, comme la norme ISO/IEC 27031, et sont adaptés aux spécificités de chaque emplacement. Ce faisant, il est possible de regrouper les détails des fonctionnalités des systèmes à chaque emplacement pour maintenir ces fonctionnalités même en cas de cyberattaques, de façon à préserver la résilience et le contrôle de l'environnement.

2.6 Il importe de préciser que la DECEA participe aussi à l'exercice national brésilien de cybersécurité, qui se déroule sous la responsabilité du ministère de la Défense et vise à protéger les systèmes essentiels du pays. Dans le cadre de cet exercice national, la DECEA apporte l'expertise acquise dans ses unités de contrôle de l'espace aérien en matière de sécurité du transport aérien et reçoit des informations d'autres secteurs qui disposent eux aussi de systèmes essentiels et ont besoin de mesures de protection et de résilience. Les activités mises au point dans le cadre de cet exercice national majeur contribuent à corroborer et à améliorer les plans d'urgence, qui doivent être constamment actualisés face aux nouvelles menaces quotidiennes.

2.7 Le Brésil invite les États membres de l'OACI et le secteur de l'aviation à soutenir et à organiser des exercices de cybersécurité afin de réunir des experts gouvernementaux et de l'industrie en vue du partage des pratiques optimales et des connaissances relatives à la formation des cyberexperts dans le domaine de la riposte aux cyberattaques et à l'élaboration de plans d'urgence en matière de cybersécurité plus fiables pour protéger les infrastructures et systèmes essentiels de l'aviation.

3. **CONCLUSION**

3.1 Les cybermenaces constituent un défi permanent et le secteur de l'aviation civile, dont le réseau mondial est complexe, est également vulnérable. La position proactive du Brésil, illustrée par les initiatives de la DECEA, est cohérente avec la Stratégie de cybersécurité de l'aviation de l'OACI, en particulier ses piliers 6 et 7. L'accent mis sur des plans d'urgence solides, guidés par des normes internationales comme l'ISO/IEC 27031 et adaptés aux spécificités locales, conjugués à des exercices de cybersécurité réguliers et réalistes, renforce considérablement la cyberrésilience. Ces initiatives permettent non seulement de former les équipes d'intervention en cas d'incident et de détecter les vulnérabilités, mais aussi de promouvoir une culture solide de cybersécurité chez l'ensemble des parties prenantes. En faisant part de son expertise et en collaborant à des exercices nationaux et internationaux, le Brésil souligne la nécessité cruciale d'une adaptation continue et d'une action collective pour protéger l'écosystème de l'aviation mondiale contre les cyberrisques en constante évolution.

— FIN —