



ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 13 : Sûreté de l'aviation — Politique

CRÉATION DE GROUPES RÉGIONAUX DE CYBERSÉCURITÉ DE L'AVIATION DANS LES BUREAUX RÉGIONAUX DE L'ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE (OACI)

[Note présentée par la République bolivarienne du Venezuela avec l'appui de 16 États membres de la Commission latino-américaine de l'aviation civile (CLAC)²].

RÉSUMÉ ANALYTIQUE

Du fait de sa dimension transnationale et de la transformation numérique rapide qu'elle connaît, l'aviation est devenue un secteur fortement interconnecté, qui dépend de réseaux informatiques divers et complexes. Pour que ces réseaux soient d'une efficacité optimale et restent adaptés au nouveau contexte mondial de l'aviation, il est indispensable d'adopter des technologies nouvelles et plus performantes. Cette dépendance aux réseaux informatiques expose le secteur de l'aviation à des cyberrisques constants, évolutifs et de plus en plus diversifiés, qui peuvent compromettre la sécurité et la sûreté de l'aviation. Ainsi, la cybersécurité n'est plus une préoccupation isolée mais un défi qui demande une action collective et coordonnée, débouchant sur des solutions adaptées aux capacités individuelles des États, aux réalités régionales et à l'ampleur grandissante des cybermenaces.

Suite à donner : L'Assemblée est invitée à :

- a) charger le Conseil de demander au Secrétariat de constituer et de mettre en place des groupes régionaux de cybersécurité de l'aviation dans les régions de l'OACI. Il s'agit là d'une mesure stratégique indispensable pour préserver l'intégrité, la sécurité, la sûreté et la continuité du transport aérien, qui favorisera une approche plus résiliente et proactive des cybermenaces, comme le prévoit le plan d'action pour la cybersécurité de l'OACI ;
- b) veiller à ce que ces groupes régionaux de cybersécurité de l'aviation soient composés de professionnels spécialisés dans la cybersécurité, qui soient à même de formuler des recommandations sur les mesures de sûreté et les meilleures pratiques à adopter, en se basant sur les travaux du Groupe d'experts de la cybersécurité et sur les besoins régionaux ;
- c) noter que, pour une adoption appropriée des stratégies élaborées par le Groupe d'experts de la cybersécurité dans chaque région, la cybersécurité de l'aviation nécessite une spécialisation technique spécifique, distincte des autres domaines, et une coordination avec d'autres groupes régionaux.

¹ Version espagnole fournie par la République bolivarienne du Venezuela.

² Belize, Bolivie (État plurinational de), Brésil, Colombie, Cuba, El Salvador, Équateur, Guatemala, Honduras, Jamaïque, Mexique, Nicaragua, Panama, Paraguay, République dominicaine et Uruguay.

<i>Objectifs stratégiques :</i>	La présente note se rapporte à l'objectif stratégique <i>Chaque vol est sûr et sécurisé.</i>
<i>Incidences financières :</i>	Il est proposé que les activités visées dans la présente note soient entreprises dans les limites des ressources disponibles dans le budget ordinaire pour la période triennale en cours et/ou au moyen de contributions extrabudgétaires.
<i>Références :</i>	Annexe 17 – Sûreté de l'aviation <i>Plan d'action pour la cybersécurité</i> de l'OACI - 5.1.1 ; 5.8.1 ; 6.3.1 ; 9.3.1 ; 11.1.5. <i>Stratégie pour la cybersécurité de l'aviation</i> de l'OACI (coopération internationale)

1. INTRODUCTION

1.1 L'aviation civile est un secteur fortement interconnecté qui s'appuie sur un large ensemble de technologies. L'infrastructure aéronautique mondiale repose aujourd'hui en grande partie sur des réseaux informatiques complexes qui, s'ils permettent d'optimiser l'efficacité du secteur, exposent également celui-ci à des cybermenaces de plus en plus diversifiées et sophistiquées, qui évoluent constamment et peuvent donner lieu à des vols d'informations sensibles ainsi qu'à des perturbations de l'exploitation et de systèmes essentiels de navigation, de communication et de surveillance, ou gravement compromettre la réputation de l'aviation et la confiance dans sa sécurité, pour ne citer que quelques conséquences.

1.2 Il est donc nécessaire de mettre au point des mécanismes et des canaux efficaces pour atténuer ou réduire les cyberrisques dans le secteur. En effet, du fait de la dimension transnationale de l'aviation, une cyberattaque ciblant un pays peut avoir des répercussions et des conséquences dans toute une région, voire dans le monde entier. La cybersécurité n'est donc plus une préoccupation isolée qui ne concerne que la sûreté de l'aviation, mais un défi qui exige une action collective et coordonnée, dépassant les frontières nationales et prenant en compte les réalités et caractéristiques de chaque région.

1.3 Les cybermenaces présentent des caractéristiques particulières qui les distinguent des autres menaces auxquelles sont habituellement exposées la sécurité et la sûreté aériennes : elles évoluent à un rythme nettement plus soutenu, comme en témoigne l'émergence rapide de nouveaux vecteurs d'attaque et de nouvelles vulnérabilités pouvant venir de n'importe quelle partie du monde et être exploités en tout point du globe. Par ailleurs, il est généralement difficile d'identifier les agresseurs, qui parviennent parfois à rester anonymes, et de cerner les attributs qui les caractérisent. Contrairement aux autres menaces ou risques, les cybermenaces ne nécessitent généralement pas une présence ou une proximité physique, ce qui modifie considérablement les paradigmes de détection, d'intervention et d'enquête.

1.4 L'OACI a encouragé la collaboration en matière de cybersécurité dans le cadre de discussions menées sur ce sujet au sein de groupes régionaux ou d'initiatives analogues en rapport avec la sécurité. Pour les questions qui touchent à la cybersécurité, il est néanmoins important d'adopter une approche horizontale et intersectorielle, et d'intégrer ce thème dans les différents domaines de l'aviation. Les discussions sur la cybersécurité portent souvent sur des détails techniques complexes, qui demandent une compréhension approfondie de l'infrastructure informatique et des opérations aériennes.

1.5 Il est donc indispensable de prendre conscience que la cybersécurité de l'aviation a atteint un niveau de complexité et de gravité qui justifie que la question fasse l'objet d'un traitement spécialisé et d'une attention particulière, et soit abordée dans le cadre de concertations spécifiques, entre spécialistes professionnels ayant un profil technique particulier et coordonnant leurs travaux avec ceux de groupes ou

d'initiatives analogues travaillant sur la sûreté aérienne, ainsi qu'avec d'autres groupes régionaux qui examinent des questions en rapport avec la cybersécurité aérienne.

2. ANALYSE

2.1 Le rôle des groupes d'experts régionaux qu'il est proposé de constituer serait principalement de relayer les travaux du Groupe d'experts de la cybersécurité de l'OACI (CYSECP) et de traduire la stratégie mondiale en actions concrètes au niveau régional, en veillant à ce que la cybersécurité de l'aviation - qui est une question transversale et multidisciplinaire - soit prise au sérieux dans chaque région, et traitée de manière appropriée et réaliste. Pour que cela soit possible, il est essentiel de prendre en considération les travaux de fond accomplis par les experts du Groupe, qui ont consacré des efforts considérables à l'élaboration de manuels, de lignes directrices et de meilleures pratiques adaptés au domaine complexe qu'est l'aviation, et de tirer parti de ces travaux.

2.2 La portée et l'application des travaux du CYSECP sont souvent méconnus des États ou sous-exploités par ceux-ci. À cet égard, les groupes régionaux de cybersécurité de l'aviation de l'OACI assumeraient un rôle vital en diffusant les lignes directrices mondiales, qu'ils seraient chargés d'adapter et de mettre en œuvre dans les différents contextes régionaux. Les États pourraient ainsi bénéficier directement de l'expérience du Groupe d'experts et des outils qu'il élabore, ce qui accélérerait le développement du dispositif de cybersécurité de l'aviation de chaque région.

2.3 Il est urgent de mettre en place officiellement des groupes régionaux de cybersécurité de l'aviation dont la structure, l'organisation et les objectifs seraient inspirés de ceux du Groupe d'experts, et reprendraient un modèle de coopération qui renforce la résilience collective, non seulement en favorisant l'échange d'informations et les formations spécialisées, mais aussi en permettant une action souple et coordonnée. Il sera ainsi possible d'adopter une approche plus ciblée et plus efficace, fondée sur la protection des infrastructures informatiques et des opérations aériennes, et de préserver ainsi l'intégrité, la sécurité et la continuité de l'aviation dans nos régions.

— FIN —