



ASSEMBLÉE — 40^e SESSION

COMITÉ EXÉCUTIF

Point 12 : Sûreté de l'aviation — Politique

PROPOSITION CONCERNANT LA CRÉATION DE POINTS DE CONTACT (POC) EN MATIÈRE DE CYBERSÉCURITÉ

(Note présentée par la République bolivarienne du Venezuela)

RÉSUMÉ ANALYTIQUE

Dans la Résolution A39-19, *Cybersécurité dans l'aviation civile*, l'Assemblée invitait les États membres et les parties prenantes de l'industrie à prendre des mesures pour contrer les cybermenaces auxquelles est confrontée l'aviation civile, notamment : développer une compréhension commune entre les États membres pour ce qui est des cybermenaces et des cyberrisques, encourager la coordination des gouvernements et de l'industrie quant aux stratégies, politiques et plans relatifs à la cybersécurité, échanger des informations afin de déceler les vulnérabilités critiques auxquelles il faut remédier, et développer, à l'échelle nationale et internationale, des partenariats et des mécanismes gouvernements-industrie, et jouer un rôle dans lesdits partenariats et mécanismes, afin que soient systématiquement partagées les informations sur les cybermenaces, les incidents, les tendances dans ce domaine et les efforts d'atténuation. Ce qui précède exige que les États élaborent et mettent en œuvre des mécanismes fiables de communication pour veiller à ce que l'aviation civile ne soit pas perturbée par des cyberattaques.

Suite à donner : L'Assemblée est invitée à charger le Conseil de demander au Secrétariat de concevoir et de mettre sur pied un réseau de points de contact (PoC) en matière de cybersécurité qui fonctionnerait de façon rapide, efficace et sûre pour relever les défis mondiaux que représentent les cybermenaces et assurer l'application des spécifications contenues dans l'Annexe 17 – *Sûreté*, de la Convention relative à l'aviation civile internationale.

<i>Objectifs stratégiques :</i>	La présente note de travail se rapporte à l'Objectif stratégique Sûreté et facilitation.
<i>Incidences financières :</i>	Les activités visées dans la présente note seront entreprises sous réserve des ressources prévues au budget-programme ordinaire de 2020-2022 ou provenant de contributions extrabudgétaires.
<i>Références :</i>	Annexe 17 – <i>Sûreté</i> Doc 10075, <i>Résolutions de l'assemblée en vigueur</i> (au 6 octobre 2016) Résolution A39-19, <i>Cybersécurité dans l'aviation civile</i>

¹ Version espagnole fournie par la République bolivarienne du Venezuela.

1. INTRODUCTION

1.1 La connectivité de l'aviation civile à l'échelle internationale exige de travailler de façon collaborative pour élaborer un cadre mondial efficace et coordonné permettant aux parties prenantes de l'aviation civile de relever les défis en matière de cybersécurité. Des mesures à court, moyen et long terme sont également nécessaires pour renforcer la résistance du système mondial de l'aviation aux cybermenaces qui peuvent compromettre la sécurité de l'aviation civile.

2. ANALYSE

2.1 Dans la Résolution A39-19, *Cybersécurité dans l'aviation civile*, l'Assemblée invitait les États membres et les parties prenantes de l'industrie à adopter des mesures pour contrer les cybermenaces auxquelles est confrontée l'aviation civile, en particulier :

- a) encourager le développement d'une compréhension commune entre les États membres pour ce qui est des cybermenaces et des cyberrisques, et l'élaboration de critères communs pour établir la criticité des ressources et des systèmes qui nécessitent une protection ;
- b) encourager la coordination des gouvernements et de l'industrie quant aux stratégies, politiques et plans relatifs à la cybersécurité dans l'aviation, ainsi que le partage d'informations pour aider à déceler les vulnérabilités critiques auxquelles il faut remédier ;
- c) développer, à l'échelle nationale et internationale, des partenariats et des mécanismes gouvernements-industries, et jouer un rôle dans lesdits partenariats et mécanismes, afin que soient systématiquement partagées les informations sur les cybermenaces, les incidents, les tendances dans ce domaine et les efforts d'atténuation. Cela exige que les États élaborent et mettent en œuvre des mécanismes fiables de communication pour veiller à ce que l'aviation civile ne soit pas perturbée par des cyberattaques.

2.2 Un autre aspect important de la coordination internationale a trait aux mesures qu'il faut prendre lorsque des cyberincidents ont une incidence sur le fonctionnement sûr et ordonné du système d'aviation civile. Selon la nature des incidents, il sera crucial de communiquer avec les autorités compétentes, l'autorité de l'aviation civile et les fournisseurs de systèmes pour partager les informations avec les autres usagers qui peuvent être touchés et de préserver la confidentialité au niveau institutionnel pour prévenir d'autres dommages.

2.3 La notification et le partage en temps opportun de renseignements spécifiques peuvent permettre de retarder ou de prévenir des incidents semblables qui pourraient toucher d'autres États ou partenaires de l'industrie. À cet effet, les informations pertinentes devraient être communiquées le plus tôt possible au moyen de plateformes et de mécanismes établis d'avance.

2.4 Les États devraient travailler de concert avec les organismes nationaux et internationaux pertinents pour mettre en place une démarche coopérative visant à alerter sur des activités anormales dans les systèmes, des activités humaines suspectes et des attaques contre l'intégrité des données afin de protéger des cyberattaques les systèmes des technologies de l'information et des communications, l'information aéronautique et les données critiques.

2.5 De même, les recommandations et conclusions finales devraient être communiquées aux États et aux exploitants de l'aviation afin qu'ils puissent apporter les ajustements nécessaires à leurs mécanismes et programmes respectifs de gouvernance de la cybersécurité.

3. CONCLUSION

3.1 Ce qui précède exige que les États élaborent et mettent en œuvre des mécanismes fiables de communication pour veiller à ce que l'aviation civile ne soit pas perturbée par des cyberattaques. À cet égard, et vu la nature spécialisée de la sécurité des systèmes des TIC, et que, bien souvent, les organismes compétents en matière de cybersécurité ne sont pas nécessairement ceux qui sont compétents pour les questions de sûreté de l'aviation, l'Assemblée est invitée à charger le Conseil de proposer au Secrétariat de concevoir et de mettre sur pied un réseau de points de contact (PoC) en matière de cybersécurité qui fonctionnera de façon rapide, efficace et sûre pour relever les défis posés à l'échelle mondiale par les cybermenaces et leurs possibles conséquences sur la sûreté de l'aviation civile.