



ASSEMBLÉE — 40^e SESSION

COMITÉ EXÉCUTIF

Point 12 : Sûreté de l'aviation — Politique

CYBERSÉCURITÉ

(Note présentée par les Émirats arabes unis)

RÉSUMÉ ANALYTIQUE

La cybersécurité reste une menace contre l'aviation civile. À l'instar d'autres organisations internationales, l'OACI œuvre activement à réduire le plus possible les probabilités et les conséquences des cyberattaques.

La communauté aéronautique doit cependant travailler de concert pour parer à cette menace croissante visant notre système d'aviation civile, car elle n'est que partiellement consciente du problème de cybersécurité en sécurité aérienne. Le Sommet de l'OACI sur la cybersécurité, tenu dans les É.A.U. en avril 2017, a bien démontré le manque de sensibilisation du secteur de la sécurité de l'aviation à ce problème. Les participants au Sommet pensaient que la rencontre était consacrée davantage à la sûreté de l'aviation qu'à la sécurité aérienne.

Suite à donner : L'Assemblée est invitée :

- à reconnaître que la Déclaration de l'A39 et de Doubaï sur la cybersécurité dans l'aviation civile a été un élément clé dans l'établissement de la Stratégie de cybersécurité et de la Résolution A39-19 amendée de l'Assemblée, intitulée « Cybersécurité dans l'aviation civile » et soumise à la présente session dans la note WP/28 ;
- à charger l'OACI de veiller à ce que des SARP sur la cybersécurité soient établies pour chacune des Annexes, en faisant activement appel aux experts de la sécurité aérienne ;
- à encourager les États à participer aux mécanismes de partage d'informations, décrits dans la note du Conseil (WP/28) sur la stratégie de cybersécurité de l'OACI.

<i>Objectifs stratégiques :</i>	La présente note de travail se rapporte aux Objectifs stratégiques : Sécurité, Capacité et efficacité de la navigation aérienne, et Développement économique du transport aérien.
<i>Incidences financières :</i>	
<i>Références :</i>	

1. INTRODUCTION

1.1 La cybersécurité continue de poser une grave menace contre l'aviation civile.

1.2 L'OACI et d'autres organisations internationales œuvrent activement à réduire le plus possible la probabilité et les conséquences d'une cyberattaque.

1.3 La communauté aéronautique doit cependant travailler de concert pour parer à cette menace croissante contre notre système d'aviation civile.

2. ANALYSE

2.1 L'Annexe 17 contient peu de dispositions sur les cybermenaces.

2.2 La cybersécurité est de nature pluridimensionnelle et relève de TOUTES les Annexes. Il importe donc de trouver un mécanisme approprié pour assurer la coordination dans tous les domaines de l'aviation (sécurité, sûreté, etc.).

2.3 Il serait souhaitable que l'OACI tienne compte de l'aspect pluridimensionnel de la cybersécurité en créant à cette fin une structure appropriée, en se conformant aux instructions du Conseil de mener une étude de faisabilité et une analyse d'écart aux fins d'établissement de la structure future du programme des travaux de l'OACI sur la cybersécurité.

2.4 La nouvelle structure devrait viser à promouvoir la résistance contre les cyberattaques dans tous les domaines du transport aérien : sécurité, sûreté et économie.

2.5 Il convient de se rappeler des cyberattaques lancées contre les compagnies aériennes ces dernières années. La sécurité et la sûreté n'en ont pas souffert, mais ces attaques peuvent quand même avoir des conséquences néfastes pour le transport aérien, en sapant la confiance des voyageurs et en appelant inutilement une attention négative du public sur le transport aérien.

— — — — —

APPENDICE

DÉCLARATION DE DOUBAÏ

DÉCLARATION SUR LA CYBERSÉCURITÉ DANS L'AVIATION CIVILE DOUBAÏ, ÉMIRATS ARABES UNIS 4 – 6 AVRIL 2017

Nous, hauts fonctionnaires et représentants des États et des organisations régionales et internationales participant au Sommet sur la cybersécurité dans l'aviation civile convoqué par l'Organisation de l'aviation civile internationale (OACI) à Doubaï (Émirats arabes unis) du 4 au 6 avril 2017, pour répondre au problème des cyberattaques contre l'aviation civile ;

Rappelant la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* et le *Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs* faits à Beijing le 10 septembre 2010 (les Instruments de Beijing) ;

Rappelant en outre la Résolution A39-19 de l'Assemblée de l'OACI : Cybersécurité dans l'aviation civile, ainsi que l'importance et l'urgence de protéger les systèmes d'infrastructures et les données critiques contre les cyberattaques, notamment en adoptant les mesures ci-après :

- a) mettre en œuvre des stratégies nationales, régionales et mondiales sur la cybersécurité dans l'aviation civile fondées sur une vision commune ;
- b) renforcer la résistance du système mondial d'aviation contre les cybermenaces susceptibles de compromettre la sécurité, la sûreté et l'efficacité de l'aviation civile ;
- c) réaffirmer le rôle primordial de l'OACI comme forum du plus haut niveau pour faire face collectivement aux problèmes de cybersécurité dans l'aviation civile.

Conscients des difficultés dans la protection de l'aviation civile contre les cybermenaces dans l'environnement exigeant et en évolution constante de la cybersécurité dans l'aviation civile ;

Notant que, lors de nombreux cyberincidents affectant la sûreté et la sécurité de l'aviation civile, les parties intéressées se sont concentrées sur les intentions malveillantes, les interruptions des activités commerciales et le vol d'informations à des fins politiques, financières ou autres ;

Reconnaissant que les cyberincidents peuvent nuire aux systèmes d'aviation civile critiques dans le monde avec des répercussions catastrophiques, notamment la disponibilité de systèmes de technologies d'information et de communications, ainsi que l'intégrité et la confidentialité des données, autant d'éléments dont dépend de plus en plus le secteur de l'aviation ;

Considérant la nécessité de faciliter et d'encourager les initiatives mondiales en matière de cybersécurité, afin d'agir de façon collaborative, complète et interdisciplinaire.

Déclarons ce qui suit :

1. Il relève de la responsabilité des États d'agir de façon à réduire les risques posés par les cybermenaces, à renforcer leurs capacités et capacités de faire face à ces menaces contre l'aviation civile et à assurer qu'un cadre législatif approprié soit mis en place pour prendre des mesures contre les auteurs de ces cyberattaques ;
2. Les capacités de cybersécurité appliquées à l'aviation ne devraient être utilisées qu'à des fins pacifiques et uniquement dans le but de renforcer la sécurité, l'efficacité et la sûreté ;
3. La collaboration et les échanges entre les États et les autres parties prenantes sont une condition sine qua non pour l'établissement d'un cadre mondial efficace et coordonné afin de lutter contre les problèmes de cybersécurité dans l'aviation civile ;
4. Les questions de cybersécurité doivent faire l'objet d'un examen approfondi et coordonné entre toutes les disciplines pertinentes au sein des autorités de l'aviation d'État ;
5. Les cyberattaques contre l'aviation civile doivent être considérées comme une infraction aux principes et aux dispositions de développement sûr et ordonné de l'aviation civile internationale ;
6. La ratification et l'entrée en vigueur des Instruments de Beijing assureront qu'une cyberattaque contre l'aviation civile internationale sera considérée comme une infraction, et auront un effet dissuasif important contre les activités susceptibles de compromettre la sécurité aérienne en exploitant les cybervulnérabilités ; il est donc impératif que tous les États et l'OACI s'efforcent d'assurer l'entrée en vigueur rapide et l'adoption universelle des Instruments de Beijing, comme il a été demandé dans la Résolution A39-10 de l'Assemblée de l'OACI, Promotion de la Convention et du Protocole de Beijing de 2010 ; et

Réitérons notre engagement à créer un système d'aviation civile solide, efficace et durable.

Faite à Doubaï, Émirats arabes unis, ce 5 avril 2017.