Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A39-WP/17
EX/5
30/5/16

ASSEMBLÉE — 39e SESSION

COMITÉ EXÉCUTIF

Point 16 : Sûreté de l'aviation — Politique

LA CYBERSÉCURITÉ DANS L'AVIATION CIVILE

(Note présentée par le Conseil de l'OACI)

RÉSUMÉ ANALYTIQUE

L'aviation civile internationale dépend dans une large mesure de la disponibilité des systèmes de technologies de l'information et des communications (TIC), ainsi que de l'exactitude et de la confidentialité des données, pour fonctionner dans de bonnes conditions d'efficacité, de sécurité et de sûreté. La protection et la résistance des systèmes aéronautiques contre les cybermenaces et les cybervulnérabilités ne peuvent être renforcées que par une approche harmonisée, mondiale et fondée sur la collaboration qui fait intervenir l'expertise collective de la sûreté de l'aviation, de la navigation aérienne, de la sécurité des TIC et des autres communautés concernées.

En 2013, l'OACI, le Conseil international des aéroports (ACI), la Civil Air Navigation Services Organisation (CANSO), l'Association du transport aérien international (IATA) et le Conseil international de coordination des associations d'industries aérospatiales (ICCAIA) ont créé un Groupe de haut niveau de l'industrie (IHLG) pour servir de mécanisme de coopération de haut niveau pour les questions d'intérêt et d'importance communs, notamment la cybersécurité. À cet égard, l'ILHG a estimé que la cybersécurité dans l'aviation civile était une question horizontale hautement prioritaire nécessitant des mesures harmonisées et coordonnées de la part de toutes les parties prenantes concernées.

Soucieux de favoriser davantage une approche concertée et cohérente pour la gestion des cyber-menaces et des cyber-risques, l'OACI et les membres de l'IHLG ont élaboré un projet de résolution, présenté en appendice, qui vise à traiter la cybersécurité dans l'aviation civile par une approche horizontale, transversale et fonctionnelle. Les objectifs sont de réaffirmer l'importance et l'urgence de protéger les systèmes et les données des infrastructures critiques de l'aviation civile contre les cybermenaces et les cybervulnérabilités et d'obtenir de l'OACI, des États membres et des parties prenantes de l'industrie, un engagement mondial à prendre des mesures concrètes en vue de se pencher sur la questions de la cybersécurité dans l'aviation civile et d'atténuer les menaces et les risques connexes de manière collaborative et systématique.

Suite à donner : L'Assemblée est invitée à adopter le projet de résolution concernant la *cybersécurité dans l'aviation civile*, qui figure en appendice.

Objectifs stratégiques :	La présente note se rapporte aux Objectifs stratégiques A — *Sécurité*, B — *Capacité et efficacité de la sécurité aérienne*, et C — *Sûreté et facilitation*.
Incidences financières :	Les activités visées dans la présente note seront entreprises sous réserve des ressources prévues au budget du Programme ordinaire de 2017-2019 et/ou provenant de contributions extrabudgétaires.
Références :	Doc 10022, *Résolutions de l'Assemblée en vigueur* (au 4 octobre 2013)

– – – – – – – – – – – –

APPENDICE

PROJET DE RÉSOLUTION DE L'ASSEMBLÉE : CYBERSÉCURITÉ DANS L'AVIATION CIVILE

Résolution 16/xx : Cybersécurité dans l'aviation civile

L'Assemblée,

Considérant que le système mondial de l'aviation est un système éminemment complexe et intégré constitué de technologies de l'information et des communications essentielles à la sécurité et à la sûreté des vols d'aviation civile,

Notant que le secteur de l'aviation dépend de plus en plus de la disponibilité des systèmes de technologies de l'information et des communications, ainsi que de l'intégrité et de la confidentialité des données,

Consciente que la menace représentée par les cyberincidents pour l'aviation civile évolue rapidement et continuellement, que les responsables de ces menaces sont animés d'intentions malveillantes et concentrent leurs efforts sur la perturbation de la continuité des activités et le vol d'informations pour des motivations politiques, financières ou autres, et que cette menace peut facilement évoluer et porter atteinte aux systèmes critiques de l'aviation civile dans le monde entier,

Reconnaissant que tous les problèmes de cybersécurité qui compromettent la sécurité de l'aviation civile ne sont pas illégaux et/ou intentionnels, et devraient donc être traités par l'application de systèmes de gestion de la sécurité,

Réaffirmant l'importance et l'urgence de protéger les systèmes et les données des infrastructures critiques de l'aviation civile contre les cybermenaces,

Considérant la nécessité de travailler de façon collaborative en vue de l'élaboration d'un cadre mondial efficace et coordonné permettant aux parties prenantes de l'aviation civile de relever les défis en matière de cybersécurité, et de prendre des mesures à court terme pour renforcer la résistance du système mondial de l'aviation aux cybermenaces qui peuvent compromettre la sécurité de l'aviation civile,

Reconnaissant la valeur des initiatives, plans d'action, publications et autres médias conçus pour faire face aux problèmes de cybersécurité de manière collaborative et approfondie,

Rappelant les initiatives des dirigeants du Conseil international des aéroports (ACI), de la Civil Air Navigation Services Organisation (CANSO), de l'Association du transport aérien international (IATA), du Conseil international de coordination des associations d'industries aérospatiales (ICCAIA) et de l'OACI qui attestent la nécessité de travailler ensemble et d'être guidés par une vision, une stratégie et une feuille de route communes pour renforcer la protection du système mondial de l'aviation contre les cybermenaces et sa résistance à celles-ci,

Reconnaissant la nature multiforme et multidisciplinaire des défis et des solutions en matière de cybersécurité,

1. *Invite* les États et les parties prenantes de l'industrie à prendre les mesures suivantes pour contrer les cyber-menaces auxquelles est confrontée l'aviation civile :

    a) Déterminer les menaces et les risques associés aux éventuels cyberincidents contre les vols et les systèmes critiques de l'aviation civile, et les graves conséquences que peuvent entraîner de tels incidents ;

b) Définir les responsabilités des organismes nationaux et des parties prenantes de l'industrie en ce qui concerne la cybersécurité dans l'aviation civile ;

c) 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 ;

d) 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 ;

e) 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 ;

f) Sur la base d'une compréhension commune des cybermenaces et des cyberrisques, adopter une approche souple et fondée sur les risques pour la protection des systèmes critiques d'aviation grâce à la mise en œuvre de systèmes de gestion de la cybersécurité ;

g) Encourager une solide culture générale en matière de cybersécurité dans les organismes nationaux et dans l'ensemble du secteur de l'aviation ;

h) Déterminer les conséquences judiciaires des activités qui compromettent la sécurité de l'aviation en exploitant les cybervulnérabilités ;

i) Promouvoir l'élaboration et la mise en œuvre de normes, stratégies et meilleures pratiques internationales relatives à la protection des systèmes critiques de technologies de l'information et des communications utilisés aux fins de l'aviation civile contre des interventions qui peuvent compromettre la sécurité de l'aviation civile ;

j) Établir des politiques et affecter des ressources, au besoin, afin que, en ce qui concerne les systèmes d'aviation critiques : la sécurité soit intégrée à la conception des architectures de systèmes ; les systèmes soient résistants ; les méthodes de transfert de données soient sécurisées, assurant ainsi l'intégrité et la confidentialité des données ; la surveillance des systèmes et les méthodes de détection et de compte rendu d'incidents soient mises en œuvre ; des analyses techniques des cyberincidents soient réalisées ;

k) Collaborer à l'élaboration du cadre de cybersécurité de l'OACI selon une approche horizontale, transversale et fonctionnelle qui met à contribution la navigation aérienne, la communication, la surveillance, l'exploitation technique et la navigabilité des aéronefs et d'autres disciplines pertinentes.

2. *Charge* la Secrétaire générale :

a) d'aider les États et l'industrie à prendre ces mesures et de leur faciliter la tâche en ce sens ;

b) de veiller à ce que les questions de cybersécurité soient dûment examinées et coordonnées dans toutes les disciplines pertinentes de l'OACI.

— FIN —