Organisation de l'aviation civile internationale

AN-Conf/13-WP/62
27/8/18

NOTE DE TRAVAIL

TREIZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 9 – 19 octobre 2018

COMITÉ A

Point 5 : Questions émergentes
5.4 : Cyberrésilience

PROMOUVOIR LA CYBERRÉSILIENCE PAR LA SENSIBILISATION GÉNÉRALE ET DANS LE CADRE D'EXERCICES À L'ÉCHELLE RÉGIONALE

(Note présentée par les États-Unis)

RÉSUMÉ ANALYTIQUE

Conformément à la Résolution A39-19, *Cybersécurité dans l'aviation civile* de l'Assemblée de l'OACI, la Federal Aviation Administration (Administration fédérale de l'aviation) (FAA) a travaillé en collaboration avec des partenaires de l'OACI et des partenaires régionaux afin de déterminer les menaces et les risques associés aux éventuels cyberincidents contre les vols et les systèmes critiques de l'aviation civile et d'encourager le développement d'une compréhension commune entre partenaires pour ce qui est de l'atténuation des cybermenaces, des cyber-risques et des cyberincidents.

Ainsi, la FAA a proposé un modèle d'exercice de cybersimulation régional dans lequel certains scénarios feraient l'objet de discussions dirigées permettant un échange d'idées ouvert et stimulant sur plusieurs aspects d'un hypothétique cyberincident simulé. Ce type d'exercice sert à accroître la sensibilisation générale, à valider les plans et procédures actuels et à évaluer les systèmes et les activités qui relèvent du cadre d'intervention et de reprise à la suite de cyberincidents.

Suite à donner : La Conférence est invitée à :
a) soutenir le concept d'exercice de cybersimulation régional, effectué en coopération avec les bureaux régionaux de l'OACI et les États membres, comme le décrit le paragraphe 2.6 ;
b) demander à l'OACI de créer un répertoire de scénarios et d'enseignements qui soit mis à la disposition des États membres pour les aider à élaborer ce type d'exercice.

1. INTRODUCTION

1.1 Les voyageurs aériens, l'industrie aéronautique, les fournisseurs de services de navigation aérienne (ANSP) et les Autorités de l'aviation civile (AAC) dépendent de plus en plus des communications et des opérations en réseau-centrique. Par conséquent, les États doivent prendre les mesures qui s'imposent pour moderniser l'infrastructure informatique et réseau en reliant les usagers, les systèmes et les données de façon à permettre un accès continu et sécurisé, à l'abri des cyberincidents.

1.2 Les cyberincidents peuvent toucher la communauté mondiale de l'aviation ou des systèmes individuels à de nombreux niveaux. Ils peuvent mettre en danger les communications et les échanges d'informations entre diverses parties prenantes de l'aviation, avec des conséquences sur la sécurité et la sûreté et une dégradation de la continuité des activités aéronautiques. La possibilité de partager l'information cybernétique et l'application de méthodes normalisées solides pour sécuriser l'échange de données et d'informations renforcent l'aptitude de la communauté aéronautique à se protéger et à limiter les incidences de cyberincidents.

1.3 Pour consolider la position de l'aviation civile en matière de sûreté, la FAA a entrepris d'identifier les risques pour la cybersécurité qui peuvent avoir des incidences sur la sécurité et perturber le fonctionnement du Système national de l'espace aérien (NAS) et d'élaborer des stratégies d'atténuation à l'échelle de l'écosystème de l'aviation. Cette stratégie transversale permet aux éléments du NAS de fonctionner comme un seul système afin que les voyageurs aériens, les compagnies aériennes, les secteurs militaires des États-Unis, l'aviation générale et les aéroports aient accès à des services sûrs et efficaces.

1.4 Au-delà de la portée des stratégies nationales d'atténuation des risques de cybersécurité, et conformément à la Résolution A39-19, *Cybersécurité dans l'aviation civile* de l'Assemblée de l'OACI, la FAA a travaillé avec des partenaires de l'OACI ainsi qu'avec des partenaires régionaux pour déterminer les menaces et les risques associés à d'éventuels cyberincidents contre les vols et les systèmes critiques de l'aviation civile. Ensemble, ils ont encouragé le développement d'une compréhension commune entre partenaires des mesures d'atténuation des cybermenaces, des cyber-risques et des cyberincidents.

1.5 La FAA a proposé un modèle d'exercice de cybersimulation régional dans lequel certains scénarios feraient l'objet de discussions dirigées permettant un échange d'idées ouvert et stimulant sur plusieurs aspects d'un hypothétique cyberincident simulé. Ce type d'exercice sert à accroître la sensibilisation générale, à valider les plans et procédures actuels ainsi qu'à évaluer les systèmes et les activités qui relèvent du cadre d'intervention et de reprise à la suite de cyberincidents.

2. ANALYSE

2.1 La 39e Session de l'Assemblée de l'OACI, dans sa Résolution A39-19, invite notamment les États :

a) à 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) à encourager le développement d'une compréhension commune entre les États membres pour ce qui est des cybermenaces et des cyber-risques, et l'élaboration de critères communs pour établir la criticité des ressources et des systèmes qui nécessitent une protection ;

c) à 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 ;

d) à 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 ;

e) à 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.

2.2 Les travaux avancent à l'OACI à mesure que le Groupe de travail INNOVA établit des méthodes communes et convenues dans le but de protéger la communauté aéronautique des risques de cybersécurité au moyen d'un cadre regroupant les exigences réglementaires. Néanmoins, certains États ont fait part de leurs préoccupations quant à la création et à la mise en œuvre de programmes de cybersécurité.

2.3 Ces préoccupations, auxquelles s'ajoute la grande quantité de communications et de données partagées entre la FAA, les autorités de l'aviation civile et les fournisseurs de services de navigation aérienne dans les Caraïbes, ont décidé la FAA à organiser un exercice de simulation sur la cybersécurité pour aider à l'élaboration de meilleures pratiques régionales en cas de menaces contre la cybersécurité aérienne. Il pourra servir de modèle pour d'autres simulations régionales de ce type, s'il y a lieu.

2.4 Cet exercice consiste en une discussion dirigée sur certains scénarios qui s'est déroulée dans un contexte structuré mais détendu. Échange d'idées ouvert et stimulant sur plusieurs aspects d'un hypothétique cyberincident simulé, l'exercice permet d'accroître la sensibilisation générale, de valider les plans et procédures actuels ainsi que d'évaluer les systèmes et les activités qui relèvent du cadre d'intervention et de reprise à la suite de cyberincidents dans la région Caraïbes. Il a également porté sur les politiques, les plans, les besoins en effectif, le partage d'informations et la coordination gouvernementale, ainsi que l'identification de lacunes, ou encore de flous ou de recoupements dans les responsabilités.

2.5 La FAA et les États des Caraïbes rassemblés dans le cadre de cet exercice ont pu consolider leur cyberrésilience en s'assurant que les systèmes et les réseaux d'information, indépendants comme partagés, fonctionnaient correctement.

2.6 L'exercice consistait en une discussion de haut niveau centrée sur les politiques et les pratiques, et qui avait pour objectifs :

a) le développement et la promotion d'une compréhension commune des cybermenaces, des vulnérabilités et des risques en découlant dans tout l'écosystème de l'aviation ;

b) l'identification de lacunes dans les politiques et les opérations des États ;

c) l'identification et le soutien de partenariats et de mécanismes régionaux de partage d'informations sur les menaces émergentes et les interventions en cas d'incident.

3. CONCLUSION

3.1 Tandis que l’OACI progresse dans le développement d’un cadre regroupant les exigences réglementaires pour renforcer la cybersécurité, les États et les régions ont encore du travail à faire à leur niveau. Si les États travaillent de concert en partenariats régionaux, en utilisant un modèle efficace pour développer une compréhension commune et déterminer les lacunes dans les politiques et la réglementation, ils peuvent commencer à créer un cadre de base qui leur permettra de promouvoir la cybersécurité et d’atténuer les cyberincidents.

— FIN —