Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/28
EX/13
25/6/19

ASSEMBLÉE — 40e SESSION

COMITÉ EXÉCUTIF

Point 12 : Sûreté de l'aviation — Politique

STRATÉGIE DE CYBERSÉCURITÉ DE L'OACI

(Note présentée par le Conseil de l'OACI)

RÉSUMÉ ANALYTIQUE

La présente note propose une stratégie exhaustive de cybersécurité et, afin d'en souligner l'urgence et l'importance, inclut un amendement de la Résolution A39-19 de l'Assemblée (*Cybersécurité dans l'aviation civile*) appuyant sa mise en œuvre par les États membres. La stratégie se fonde sur la vision de l'OACI pour une cybersécurité mondiale – vision selon laquelle le secteur de l'aviation devrait être résilient face aux cyberattaques, et rester sûr et fiable à l'échelle mondiale, tout en continuant d'innover et de croître. Elle devra s'appuyer sur un plan d'action à élaborer au moyen de mécanismes appropriés. La stratégie est le résultat des délibérations du Groupe d'étude du Secrétariat sur la cybersécurité.

Suite à donner : L'Assemblée est invitée :

a) à adopter la proposition de résolution de l'Assemblée, remplaçant la Résolution A39-19, qui figure en Appendice A ;
b) à entériner la stratégie de sécurité qui figure en Appendice B ;
c) à prier instamment les États de ratifier la *Convention pour la répression d'actes illicites dirigés contre l'aviation civile* et le *Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs*.

Objectifs stratégiques :	La présente note de travail se rapporte aux Objectifs stratégiques : *Capacité et efficacité*, *Sécurité* et *Sûreté et facilitation.*
Incidences financières :	Les activités auxquelles fait référence la présente note de travail seront entreprises sous réserve des ressources disponibles dans le budget du programme ordinaire 2020-2022 ou de fonds extrabudgétaires.
Références :	Doc 10075, *Résolutions de l'Assemblée en vigueur* (au 6 octobre 2016)

1. INTRODUCTION

1.1 À sa 39e session, l'Assemblée a réaffirmé l'importance et l'urgence de protéger les systèmes et les données des infrastructures critiques de l'aviation civile contre les cybermenaces et d'obtenir de l'OACI, des États membres et des parties prenantes de l'industrie qu'ils s'engagent ensemble à agir en collaboration et de façon systématique pour résoudre les questions de cybersécurité aviation civile et atténuer les menaces et les risques connexes. La Résolution A39-19, *Cybersécurité dans l'aviation civile*, a recensé les mesures à prendre par les États et d'autres parties prenantes à cet égard. À sa 39e session, l'Assemblée a en outre chargé l'OACI d'élaborer un plan de travail et une structure de gouvernance complets en matière de cybersécurité.

1.2 Pour atteindre ces objectifs, l'OACI a établi le Groupe d'étude du Secrétariat sur la cybersécurité (SSGC), sous la responsabilité du Directeur adjoint, Sûreté de l'aviation et facilitation (DD/ASF). Constitué de 20 États, de 13 organisations internationales et du Secrétariat de l'OACI, le SSGC est supervisé par le Groupe de suivi de haut niveau du Secrétariat sur les questions communes de sécurité et de sûreté, présidé par la Secrétaire générale de l'OACI.

1.3 Depuis sa création en août 2017, le SSGC s'est réuni six fois et a élaboré un ensemble de recommandations pour faire face au problème émergent de la cybersécurité de l'aviation. Ces travaux ont abouti principalement à l'élaboration d'une stratégie complète de cybersécurité, qui vise à axer les travaux des États et de l'OACI sur l'objectif visant à garantir la sécurité, la sûreté et la continuité de l'aviation civile par l'application d'un cadre de cybersécurité solide. À sa 217e session, le Conseil a approuvé en principe la stratégie de cybersécurité de l'aviation et est convenu, de présenter à la 40e session de l'Assemblée de l'OACI un amendement de la Résolution A39-19, *Cybersécurité dans l'aviation civile*.

2. ANALYSE

2.1 La stratégie de cybersécurité de l'aviation prend en compte et complète d'autres initiatives de l'OACI dans ce domaine. Elle s'harmonise avec les normes et pratiques recommandées (SARP) existantes en matière de sûreté et de sécurité qui sont liées à la cybersécurité et à la protection des renseignements critiques en aviation, en particulier l'Annexe 17 — *Sûreté*.

2.2 La stratégie fait ressortir l'importance de reconnaître la cybersécurité comme étant une question transversale qui englobe tous les domaines du secteur de l'aviation. Elle synthétise dans un seul cadre les dispositions existantes liées aux questions de cybersécurité qui sont abordées dans les différentes Annexes, en mettant l'accent sur la gestion des risques de cybersécurité et en améliorant globalement la cybersécurité. Elle donne aux États une vision du secteur de l'aviation civile en tant que secteur résilient face aux cyberattaques, et qui poursuit par ailleurs son innovation et son expansion.

2.3 La stratégie vise :

a) à protéger l'aviation civile et les voyageurs contre les cybermenaces pouvant compromettre la sécurité et la sûreté du système du transport aérien ainsi que la confiance à son endroit ;

b) à maintenir ou améliorer la sécurité et la sûreté du système de l'aviation en préservant la continuité des services de transport aérien ;

c) à ce que les États reconnaissent les obligations que leur impose la *Convention relative à l'aviation civile internationale* (Convention de Chicago) afin de veiller à la sécurité, à la sûreté et à la continuité de l'aviation civile, en tenant compte des cybermenaces ;

d) à coordonner les mesures de cybersécurité entre les autorités nationales pour garantir une gestion efficace et efficiente des risques de cybersécurité.

2.4 Les objectifs de la stratégie seront atteints grâce à une série de principes, de mesures et d'actions dont le cadre repose sur sept piliers, à savoir : coopération internationale ; gouvernance ; mesures législatives et règlements efficaces ; politique de cybersécurité ; partage de l'information ; gestion des incidents et planification d'urgence ; et renforcement des capacités, formation et culture de cybersécurité.

2.5 Comme condition préalable à la mise en œuvre de la stratégie, les États membres doivent veiller à ce que leur législation et leurs règlements nationaux soient formulés et appliqués conformément aux dispositions de l'OACI. Ils devraient notamment déterminer s'il est nécessaire d'actualiser la législation nationale ou d'en adopter une nouvelle pour autoriser les poursuites en cas de cybermenaces liées au terrorisme et de cyberattaques ayant des incidences négatives sur l'aviation civile. Le processus d'évaluation et l'éventuelle actualisation de la législation des États peuvent retarder la mise en œuvre effective de la stratégie et hypothéquer l'harmonisation de la cybersécurité à l'échelle mondiale.

2.6 La stratégie répond au besoin de renforcement des capacités et de promotion d'une culture de cybersécurité. Les États auront donc besoin de personnel adéquatement formé et doté d'une expertise transversale dans les domaines de l'aviation et de la cybersécurité. Pour cela, il faudra peut-être réviser les des programmes universitaires en concevoir de nouveaux, et envisager la question du temps et des ressources qui devront y être consacrés.

2.7 Un plan d'action multidisciplinaire exhaustif sera nécessaire pour assurer l'adoption et la mise en œuvre ordonnées de mesures qui appuient les objectifs de la stratégie. L'OACI, de concert avec les États et l'industrie, devrait commencer sans tarder à élaborer un tel plan au moyen des mécanismes appropriés, portant sur les questions de cybersécurité.

2.8 La cybersécurité est une question qui évolue vite et dont il est important et urgent de s'occuper. Par conséquent, et pour faire ressortir les responsabilités et les obligations qu'il incombe aux États et à l'OACI de s'occuper ensemble de la cybersécurité, une résolution amendée de l'Assemblée soulignera les réalisations des États et de l'OACI en matière de cybersécurité et la nécessité d'adopter et de mettre en œuvre une stratégie de sécurité en étoffant la Résolution A39-19, qui était le point de départ des travaux de l'OACI sur la cybersécurité.

2.9 Le projet de résolution amendée de l'Assemblée joint en Appendice à la présente note de travail ajoute un élément à la résolution existante sur la cybersécurité en faisant ressortir le besoin d'adopter et de mettre en œuvre à l'échelle mondiale et d'une manière universelle la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* (Convention de Beijing) et le *Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing) pour faire face aux cyberattaques contre l'aviation civile.

2.10 Elle reconnaît en outre le besoin de poursuivre d'une manière plus officielle les travaux du SSGC, ce qui assurera une coordination structurée avec d'autres groupes d'experts de l'OACI.

3. CONCLUSION

3.1 Dans l'esprit de la Convention de Chicago, la stratégie mondiale de cybersécurité de l'OACI fournira dorénavant une base mutuellement acceptable pour tous les États. Elle servira à harmoniser les cadres de cybersécurité internationaux, nationaux et régionaux, et à promouvoir des mécanismes d'échange d'information appropriés qui procureront des avantages supplémentaires en matière de gestion des risques de cybersécurité.

3.2 La stratégie fournira un cadre souple pour préparer l'aviation civile à gérer efficacement la cybersécurité au cours des prochaines décennies. Elle est structurée en modules de manière à pouvoir être adaptée aux cybermenaces émergentes, pour tenir compte de l'évolution future de l'aviation civile. Elle veillera à ce que tous les domaines du secteur de l'aviation soient inclus et examinera les diverses questions d'une manière transversale et multidisciplinaire.

3.3 La stratégie de cybersécurité devra être appuyée par un plan d'action, comprenant des mesures concrètes pour bâtir un cadre de cybersécurité qui fait ses preuves. Le plan d'action s'inspirera d'orientations sur la manière de mettre en œuvre les SARP existantes liées à la cybersécurité, mais il les étoffera et les synthétisera pour proposer des orientations complètes sur la manière d'atteindre le plus haut niveau de cybersécurité.

3.4 La stratégie tient compte des plans mondiaux existants, et reconnaît en outre la nécessité d'avoir du personnel formé et compétent ayant de l'expérience à la fois en aviation et en cybersécurité.

– – – – – – – – – – – –

APPENDICE A

PROJET DE RÉSOLUTION DE L'ASSEMBLÉE SUR LA STRATÉGIE DE CYBERSÉCURITÉ DE L'AVIATION

Résolution A~~39-19~~40-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,

Reconnaissant la nature multiforme et multidisciplinaire des défis et solutions en matière de cybersécurité, et notant que les cyberrisques peuvent simultanément toucher une vaste gamme de domaines et s'étendre rapidement,

Réaffirmant les obligations qu'impose la *Convention relative à l'aviation civile internationale* (Convention de Chicago) de garantir la sécurité, la sûreté et la continuité de l'aviation civile,

Considérant que la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* (Convention de Beijing) et le *Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing) renforceraient le cadre juridique mondial visant à considérer les cyberattaques contre l'aviation civile internationale comme des crimes, et qu'en conséquence la ratification à grande échelle de ces instruments par les États découragerait et punirait de telles attaques où qu'elles se produisent,

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 le travail accompli par le Groupe d'étude du Secrétariat sur la cybersécurité, qui a grandement contribué au format de la stratégie de sécurité et aux caractéristiques de sûreté de la cybersécurité,

Reconnaissant qu'il est nécessaire d'harmoniser la cybersécurité dans l'aviation à l'échelle mondiale, régionale et nationale et d'assurer la pleine interopérabilité des mesures de protection et les systèmes de gestion du risque,

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. *Prie* instamment les États membres et l'OACI de promouvoir l'adoption et la mise en œuvre universelles de la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* (Convention de Beijing) et du *Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing) comme moyen de viser les cyberattaques dirigées contre l'aviation civile ;

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

   a) Mettre en œuvre la stratégie de sécurité figurant en Appendice ;

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

   ~~c)~~d) 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)~~e) 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)~~f) 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)~~g) 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)~~h) 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~~3. *Charge* le Secrétaire général :

a) d'élaborer un plan d'action pour appuyer les États et l'industrie dans l'adoption de la stratégie de cybersécurité ~~d'aider les États et l'industrie à prendre ces mesures et de leur faciliter la tâche en ce sens~~ ;

b) de continuer à veiller à ce que les questions de cybersécurité soient examinées et coordonnées de façon transversale au moyen des mécanismes appropriés dans l'esprit de la stratégie ~~de veiller à ce que les questions de cybersécurité soient dûment examinées et coordonnées dans toutes les disciplines pertinentes de l'OACI~~.

– – – – – – – – – – – –

APPENDICE B

STRATÉGIE DE CYBERSÉCURITÉ DE L'AVIATION

1. LA VISION D'UNE STRATÉGIE MONDIALE DE CYBERSÉCURITÉ DE L'AVIATION

1.1 Le secteur de l'aviation de l'aviation civile dépend de plus en plus de la disponibilité de l'information, ainsi que de l'intégrité de la confidentialité des données. La menace posée à l'aviation civile par d'éventuels cyberincidents est en évolution constante, les menaces se centrant principalement sur les intentions malveillantes, la perturbation de la continuité des affaires et le vol d'informations à des fins politiques, financières ou autres.

1.2 Reconnaissant la nature multiforme et multidisciplinaire de la cybersécurité, et notant que les cyberattaques peuvent simultanément toucher une vaste gamme de domaines et s'étendre rapidement, il faut impérativement élaborer une vision commune et définir une stratégie mondiale de cybersécurité.

1.3 La vision OACI de la cybersécurité mondiale est que le secteur de l'aviation civile est résilient aux cyberattaques et qu'il reste sûr et fiable au niveau mondial, tout en continuant à innover et à croître.

1.4 Cette vision peut être réalisée comme suit :

- reconnaissance par les États membres des obligations que leur impose la *Convention relative à l'aviation civile internationale* (Convention de Chicago) d'assurer la sécurité, la sûreté et la continuité de l'aviation civile, en tenant compte de cybersécurité ;
- coordination de la cybersécurité de l'aviation entre les autorités des États afin d'assurer l'efficience et l'efficacité de la gestion mondiale des risques de cybersécurité ;
- engagement de tous les acteurs de l'aviation civile à développer plus avant la cyberrésilience, en assurant la protection contre les cyberattaques qui peuvent influer sur la sécurité, la sûreté et la continuité du système de transport aérien.

1.5 La stratégie s'aligne sur d'autres initiatives de l'OACI liées à la cybernétique et coordonnées avec les dispositions correspondantes en matière de gestion de la sécurité et de la sûreté. Les objectifs de la stratégie seront atteints grâce à une série de principes, de mesures et d'actions dont le cadre repose sur sept piliers, à savoir :

I. Coopération internationale
II. Gouvernance
III. Législation et règlements efficaces
IV. Politique de cybersécurité
V. Partage de l'information
VI. Gestion des incidents et planification d'urgence
VII. Renforcement des capacités, formation et culture de cybersécurité

2. COOPÉRATION INTERNATIONALE

2.1 De par leur nature, la cybersécurité et l'aviation ne connaissent pas de frontières. Elles exigent toutes deux une coopération au niveau national et international et appellent une reconnaissance mutuelle des efforts pour développer, maintenir et améliorer la cybersécurité en vue de protéger le secteur de l'aviation civile contre les cyberattaques à la sécurité et à la sûreté.

2.2 La cybersécurité de l'aviation doit être harmonisée aux niveaux mondial, régional et national afin de promouvoir une cohérence mondiale et de garantir la pleine interopérabilité des mesures de protection et des systèmes de gestion du risque.

2.3 L'OACI est l'instance mondiale compétente pour exhorter les États à s'occuper de la cybersécurité de l'aviation civile internationale. À cette fin, l'OACI organisera, facilitera et promouvra des événements internationaux servant de plate-forme à l'échange des connaissances entre les États, les organisations internationales et l'industrie. Les États sont encouragés à participer à des débats sur la cybersécurité de l'aviation civile.

3. GOUVERNANCE

3.1 Tous les États membres sont encouragés à appuyer la stratégie cybersécurité de l'aviation de l'OACI et à s'en inspirer pour assurer la sécurité, la sûreté et la continuité de l'aviation civile dans un monde plus en plus en proie à des menaces à la cybersécurité.

3.2 Les États sont encouragés à élaborer des principes clairs de gouvernance et de responsabilisation au niveau national en matière de cybersécurité de l'aviation civile. Les autorités de l'aviation civile sont encouragées à assurer la coordination avec leur autorité nationale compétente en matière de cybersécurité, reconnaissant que l'autorité globale en matière de cybersécurité pour tous les secteurs ne relève peut-être pas de la responsabilité de l'autorité de l'aviation civile. Il est également essentiel d'établir des voies appropriées de coordination entre les diverses autorités des États et parties prenantes de l'industrie.

3.3 En outre, les États membres sont encouragés à inclure la cybersécurité dans leurs programmes nationaux de sécurité et de sûreté de l'aviation civile. À cette fin, l'OACI devrait aussi inclure la cybersécurité dans les plans régionaux et mondiaux et travailler à l'établissement d'une base commune pour les normes et pratiques recommandées (SARP) sur la cybersécurité.

4. LÉGISLATION ET RÈGLEMENTS EFFICACES

4.1 L'objectif principal de la législation et de la réglementation internationale, régionale et nationale et sur la cybersécurité de l'aviation civile est d'appuyer la mise en œuvre d'une stratégie exhaustive de cybersécurité afin de protéger l'aviation civile et les voyageurs des effets des cyberattaques.

4.2 Les États membres doivent veiller à ce qu'une législation des règlements appropriés soit formulée et appliquée, conformément aux dispositions de l'OACI, avant de mettre en œuvre une politique nationale de cybersécurité de l'aviation civile. Il faudra élaborer plus avant des orientations appropriées destinées aux États et à l'industrie sur la mise en œuvre des dispositions liées à la cybersécurité. À cette fin, l'OACI est déterminée à veiller à la création, à l'examen et à l'amendement, selon les besoins, des éléments indicatifs nécessaires concernant l'inclusion des aspects cybersécurité dans la sûreté et la sécurité.

4.3 Il faudrait analyser les instruments juridiques internationaux pertinents pour y chercher les dispositions clés de droit aérien qu'elles contiennent ou qui y font défaut sur la prévention des cyberincidents, les poursuites les réactions opportunes en la matière, pour établir la base d'une mise en œuvre systématique et cohérente de la législation et des règlements dans tout le secteur de l'aviation mondiale. Entre-temps, les États sont encouragés à ratifier les instruments de l'OACI, dont la *Convention pour la répression d'actes illicites dirigés contre l'aviation civile* (Convention de Beijing) et le *Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing).

4.4 Les États sont encouragés à examiner s'il convient de mettre à jour leur législation nationale ou d'en adopter une nouvelle pour pouvoir sanctionner les cyber menaces liées au terrorisme ainsi que les cyberattaques qui ont une incidence négative sur l'aviation civile. En parallèle, les États sont encouragés à établir des mécanismes appropriés de coopération avec les activités de recherche « de bonne foi » en sûreté, à savoir les activités de recherche réalisées dans un environnement conçu pour éviter d'influer sur la sécurité, la sûreté et la continuité de l'aviation civile.

5. POLITIQUE DE CYBERSÉCURITÉ

5.1 La cybersécurité doit être incluse dans les systèmes de supervision de la sûreté et de la sécurité de l'aviation des États dans le cadre d'une gestion exhaustive du risque.

5.2 Reconnaissant qu'il y a différentes méthodologies d'évaluation du risque, il faudrait en priorité amender les éléments indicatifs, ou en élaborer éventuellement de nouveaux, sur les évaluations de la menace et du risque pour la cybersécurité, pour que les résultats de ces évaluations puissent être comparables.

5.3 Dans l'ensemble du secteur de l'aviation civile, les politiques de cybersécurité peuvent porter sur le cycle de vie complet du système de l'aviation, et comprendre des éléments comme les suivants : culture de cybersécurité, promotion de la sûreté au niveau de la conception, sécurité de la chaîne logistique pour le logiciel et le matériel, intégrité des données, contrôle d'accès approprié, gestion proactive de la vulnérabilité, amélioration de l'agilité des mises à jour de sûreté sans compromettre la sécurité, et incorporation de systèmes et de processus de surveillance des données pertinentes de cybersécurité.

6. PARTAGE DE L'INFORMATION

6.1 Le secteur de l'aviation civile est un système mondial interdépendant composé de nombreux systèmes communs, et les cyberattaques facilement s'étendre et avoir une incidence mondiale. Le partage de l'information a pour objectif de permettre la prévention, la détection rapide et l'atténuation des événements pertinents de cybersécurité avant qu'ils n'aient des effets plus étendus sur la sécurité ou la sûreté de l'aviation. Une culture de partage de l'information réduira fortement le cyberrisque systémique dans tout le secteur de l'aviation, et son utilité a déjà été prouvée dans toute la sécurité et la sûreté de l'aviation.

6.2 Le partage de l'information, au moyen de relations établies et fiables, concernant des aspects comme les vulnérabilités, les menaces, les événements et les meilleures pratiques, peut réduire l'incidence des attaques en cours. Les mécanismes appropriés de partage de l'information doivent être reconnus, conformément aux dispositions existantes de l'OACI.

7. GESTION DES INCIDENTS ET PLANIFICATION D'URGENCE

7.1 Il est nécessaire, conformément aux mécanismes existants de gestion des incidents, de disposer de plans appropriés et adaptables assurent la continuité du transport aérien pendant des cyberincidents. Il est recommandé que les États et le secteur de l'aviation se servent des plans d'urgence déjà élaborés et les modifient pour y inclure des dispositions sur la cybersécurité.

7.2 Les exercices de cybersécurité constituent un outil utile pour tester la cyberrésilience et déterminer les améliorations nécessaires, et sont donc vivement recommandés. Ces exercices peuvent prendre diverses formes (exercices de simulation ou en temps réel) et peuvent varier en étendue (niveau international, national ou organisationnel).

8. RENFORCEMENT DES CAPACITÉS, FORMATION ET CULTURE DE CYBERSÉCURITÉ

8.1 L'élément humain est au cœur de la cybersécurité. Il est d'une importance critique que le secteur de l'aviation civile prenne des mesures concrètes pour augmenter le nombre de professionnels qualifiés et ayant des connaissances à la fois en aviation et en cybersécurité. On peut y arriver grâce à une sensibilisation à la cybersécurité, et grâce à l'éducation, au recrutement et à la formation. Des programmes de cours pertinents pour la cybersécurité et, si possible, pour la cybersécurité propre à l'aviation à tous les niveaux devraient être inclus dans le cadre éducatif national ainsi que dans les programmes internationaux pertinents de formation. Il faudrait rechercher des solutions novatrices permettant de faire en sorte que les cheminements de carrière traditionnels en technologies de l'information et cybernétique soient fusionnés et mis en rapport avec ceux de professionnels pertinents en aviation.

8.2 L'appui et la stimulation du développement des aptitudes de la main-d'œuvre actuelle et future devraient favoriser l'innovation en cybersécurité ainsi que la recherche et la conception dans le secteur de l'aviation. Une formation appropriée axée sur l'emploi devrait être dispensée de façon continue pour appuyer le personnel dans ses tâches journalières.

8.3 La cybersécurité pourrait être incluse dans la stratégie destinée à la prochaine génération de professionnels de l'aviation étant donné que l'OACI est bien placée pour travailler avec les États et l'industrie à l'établissement des compétences requises pour les diverses fonctions des professionnels de l'aviation.

8.4 Le secteur de l'aviation a un bilan enviable en matière de sécurité, basé sur une culture proactive de sécurité qui est considérée comme étant la responsabilité de chacun. Les principes de cette culture de sécurité doivent être appliqués pour élaborer et maintenir une culture de cybersécurité dans l'ensemble du secteur de l'aviation.

— FIN —