Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A41-WP/22
EX/10
7/7/22

ASSEMBLÉE — 41e SESSION

COMITÉ EXÉCUTIF

Point 14 : Sûreté de l'aviation — Politique

CYBERSÉCURITÉ DE L'AVIATION CIVILE

(Note présentée par le Conseil de l'OACI)

RÉSUMÉ ANALYTIQUE

Le secteur de l'aviation civile a une conscience toujours plus aigüe qu'il importe de combattre les cybermenaces visant l'aviation civile, bien qu'il ait rencontré des difficultés découlant pour la plupart, directement ou indirectement, de la crise de la pandémie de COVID-19. Malgré les nombreux progrès réalisés aux niveaux national, régional et mondial, il reste des actions à lancer, en particulier au niveau national, pour que la cybersécurité de l'aviation soit assurée de manière globale, harmonisée et cohérente dans le secteur de l'aviation civile.

On trouvera, dans la présente note, une description des activités liées à la cybersécurité de l'aviation, y compris celles dont l'Assemblée avait demandé la réalisation, et un projet de mise à jour de la résolution A40-10 de l'Assemblée, *Cybersécurité de l'aviation civile*, établi pour souligner l'importance du renforcement de la cybersécurité et de la cyberrésilience du secteur de l'aviation civile.

Suite à donner : L'Assemblée est invitée à :
a) prendre acte des faits nouveaux survenus dans les activités en matière de cybersécurité de l'aviation ;
b) adopter la version révisée de la résolution de l'Assemblée intitulée *Cybersécurité de l'aviation civile*, présentée en appendice pour remplacer la résolution A40-10 de l'Assemblée.

Objectifs stratégiques :	La présente note de travail se rapporte aux Objectifs stratégiques suivants : *Capacité et efficacité de la navigation aérienne*, *Sécurité* et *Sûreté et facilitation*.
Incidences financières :	Les activités visées dans la présente note devraient être entreprises dans le cadre des ressources disponibles dans le budget ordinaire 2023-2025 et/ou au moyen de contributions extrabudgétaires, selon les indications contenues dans le plan d'activités 2023-2025.
Références :	Doc 10140, *Résolutions de l'Assemblée en vigueur* (au 4 octobre 2019) Doc 10118, *Plan pour la sécurité de l'aviation dans le monde* Doc 9750, *Plan mondial de navigation aérienne* *Stratégie de cybersécurité de l'aviation civile* *Plan d'action pour la cybersécurité*

1. INTRODUCTION

1.1 À sa 39e session, l'Assemblée de l'Organisation de l'aviation civile internationale (OACI) a chargé l'OACI de veiller à ce que les cybermenaces auxquelles est confrontée l'aviation civile soient dûment examinées et d'aider les États et l'industrie à prendre les mesures nécessaires. Le Groupe d'étude du Secrétariat sur la cybersécurité (SSGC) a été créé en 2017 pour promouvoir ces activités.

1.2 À sa 40e session, l'Assemblée de l'OACI a réaffirmé l'importance et l'urgence d'un engagement mondial pour que toutes les parties prenantes s'emploient ensemble à examiner la question de la cybersécurité de l'aviation civile et adopté la Stratégie de cybersécurité de l'aviation. Elle a aussi chargé l'OACI d'élaborer un plan d'action pour appuyer la mise en œuvre de la Stratégie de cybersécurité de l'aviation et de continuer de veiller à ce que les questions de cybersécurité soient dûment examinées et coordonnées dans toutes les disciplines pertinentes. En outre, elle a constaté l'existence de carences dans la structure d'examen de la cybersécurité à l'OACI et étudié une série de critères qui pourraient constituer le fondement d'une structure révisée de cybersécurité.

1.3 Il convient de noter que la pandémie de COVID-19 a compromis les travaux de l'OACI sur la cybersécurité de l'aviation en raison de la réaffectation des ressources au financement de tâches essentielles dans le cadre de la gestion de la crise et du redémarrage et de la reprise de l'aviation civile, ainsi que des restrictions financières subies par cette organisation au cours des huit premiers mois de 2020, qui ont entraîné la perte des ressources consacrées à la cybersécurité.

2. DÉLIBÉRATIONS

2.1 Plan d'action pour la cybersécurité

2.1.1 Conformément à la résolution A40-10 de l'Assemblée, l'OACI a élaboré et publié en novembre 2020 le Plan d'action pour la cybersécurité (CyAP) afin d'appuyer la mise en œuvre de la Stratégie de cybersécurité de l'aviation par les États et les parties prenantes. Le CyAP établit les bases d'une collaboration entre les États et les parties prenantes et propose une série de principes, mesures et actions destinés à réaliser les objectifs des sept piliers de la Stratégie (coopération internationale, gouvernance, législation et règlementation efficaces, politique de cybersécurité, partage d'information, gestion des incidents et planification d'urgence, renforcement des capacités, formation et culture de la cybersécurité).

2.1.2 Au vu de l'évolution des priorités des États membres liée à la pandémie de COVID-19 et de l'expérience acquise par les États et les parties prenantes dans la mise en œuvre d'initiatives pour la cybersécurité de l'aviation dans leurs États et organisations, l'OACI a actualisé le CyAP et en a publié une deuxième édition en janvier 2022. Les modifications apportées visaient notamment à simplifier ce document afin de le rendre plus court et plus clair, et à décrire plus précisément les actions générales à mener en indiquant les mesures, les indicateurs et la date de début de la mise en œuvre.

2.2 Renforcement du mécanisme d'examen des questions de cybersécurité à l'OACI

2.2.1 À sa 40e session, l'Assemblée de l'OACI a constaté que de nombreux organes étaient engagés dans l'examen de la cybersécurité de l'Organisation et la possibilité préoccupante de doublons, de carences et d'incohérences, ainsi qu'un manque de transparence. Afin de remédier à cette situation, elle a chargé l'Assemblée de placer les activités de ces groupes sous la supervision d'une structure générale et examiné les critères qui pourraient régir une nouvelle structure de la gouvernance en matière de cybersécurité.

2.2.2 À sa 218e session, le Conseil a approuvé la méthode d'élaboration de l'étude de faisabilité et l'étude des carences relatives au projet de mécanisme d'examen des questions de cybersécurité. Les deux premières phases de l'étude ont été présentées à la 219e session. Le Conseil a prié le Secrétariat de poursuivre l'examen et la mise à jour de cette étude et habilité le Président du Conseil à examiner la possibilité de créer un groupe de travail restreint composé de Représentants au Conseil et de membres de la Commission de navigation aérienne (ANC) et chargé de mener à bien la phase 3 de l'étude avec l'aide du Secrétariat. De novembre 2020 à janvier 2021, le groupe de travail restreint a tenu de nombreuses réunions, examiné différents modes de gouvernance et recommandé une solution, qui a été approuvée par le Conseil à la 222e session. Les mesures nécessaires à la création de la nouvelle structure de gouvernance en matière de cybersécurité à l'OACI sont les suivantes :

a) faire du Groupe d'étude du Secrétariat sur la cybersécurité un groupe d'experts de la cybersécurité relevant du Comité de la sûreté de l'aviation au niveau du Conseil de l'OACI ;

b) modifier le Groupe d'étude sur le cadre de confiance en vue de l'intégrer à la structure du groupe d'experts de la Commission de navigation aérienne ;

c) créer un comité ad hoc de coordination de la cybersécurité (AHCCC) relevant du Conseil. Ce comité sera composé d'un membre du Comité du transport aérien, du Comité de la sûreté de l'aviation, de la Commission de navigation aérienne, et de chacun des groupes d'experts de l'OACI dont le programme de travail porte sur la cybersécurité. Le comité devrait représenter l'interlocuteur unique du Conseil et de toutes les parties de l'OACI participant aux activités de cybersécurité, ce qui améliorera la définition des responsabilités, la transparence, l'efficacité et la coordination des travaux de l'OACI sur la cybersécurité et la cyberrésilience de l'aviation. À sa 224e session, le Conseil a approuvé le projet de mandat du AHCCC.

2.2.3 Du fait de la décision du Conseil relative au nouveau mécanisme de gouvernance, le Groupe d'experts de la cybersécurité a été créé à la 225e session et a tenu sa première réunion en mai 2022. À sa 219e session, la Commission de navigation aérienne a approuvé la transformation du Groupe d'étude sur le cadre de confiance en un nouveau groupe d'experts de la Commission qui poursuivra le travail sur le cadre de confiance pour l'aviation internationale.

2.3 Élaboration d'un cadre de confiance pour l'aviation internationale

2.3.1 Depuis sa 223e session, le Conseil mène des discussions sur l'élaboration d'un cadre de confiance pour l'aviation internationale. Il poursuivra ces travaux, notamment en ce qui concerne le concept des opérations et la gouvernance du cadre.

2.4 Efficacité des instruments de droit aérien international dans la lutte contre les cyberattaques visant l'aviation civile

2.4.1 Aux termes de la Stratégie de cybersécurité de l'aviation, 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 et les réactions opportunes en la matière. En conséquence, ce travail figure dans le plan d'action pour la cybersécurité parmi les mesures à prendre par l'OACI. Le SSGC a donc créé le Sous-groupe de recherche sur les aspects juridiques (RSGLEG), qui est composé d'experts du droit et de la cybersécurité et dispose donc de toutes les compétences nécessaires pour atteindre les objectifs fixés. Comme convenu par le RSGLEG à sa dernière réunion en janvier 2022, le Secrétariat a fait rapport sur le travail effectué par le Sous-groupe à la 38e session du Comité juridique, tenue en mars 2022.

2.5 Éléments indicatifs

2.5.1 Conformément au plan d'action pour la cybersécurité, pour aider les États et les parties prenantes à traiter la question de la cybersécurité de l'aviation civile, l'OACI a élaboré des éléments indicatifs (publiés sur le portail ICAO-NET sous « Publications », puis « Others ») tels que :

a) Éléments indicatifs sur le Traffic Light Protocol (TLP) fournissant aux États et aux parties prenantes des orientations sur les moyens d'utiliser le TLP pour faciliter le partage d'informations relatives à la cybersécurité ;

b) Éléments indicatifs concernant la politique de cybersécurité, portant sur la protection et à la résilience des infrastructures critiques de l'aviation civile internationale face aux cybermenaces, et sur les exigences en matière de coopération multilatérale à l'intérieur de l'aviation civile et avec les autorités extérieures. Les éléments indicatifs prennent également en compte la nécessité de désigner l'autorité compétente de la cybersécurité de l'aviation et comprennent un modèle conçu pour aider les États et les parties prenantes à élaborer une politique de cybersécurité ;

c) Culture de cybersécurité de l'aviation civile, qui favorise la conception et la mise en œuvre d'une solide culture de cybersécurité en s'appuyant sur les bons résultats obtenus par l'aviation civile dans la mise en place de cultures de la sécurité et de la sûreté.

2.6 Renforcement des capacités

2.6.1 En 2020, l'OACI a élaboré un plan d'action pour la formation en matière de cybersécurité afin de soutenir les mesures qu'elle prend pour accroître la capacité à fournir des activités de formation adaptées, cohérentes et pertinentes aux États et aux parties prenantes. Ce plan d'action favorise l'application de la Stratégie de cybersécurité de l'aviation et du plan d'action pour la cybersécurité. Elle favorise également l'application de la résolution A40-25 de l'Assemblée, intitulée « Mise en œuvre de stratégies de formation et de renforcement des capacités en aéronautique », qui prévoit que l'OACI aidera les États membres dans le cadre de ses activités de formation, afin qu'ils disposent de ressources humaines et de capacités suffisantes. Après avoir élaboré ce plan d'action, l'OACI a commencé à constituer un portefeuille d'activités de formation dans le domaine de la cybersécurité, dans lequel figurent actuellement les cours ci-après :

2.6.1.1 Fondements du leadership en cybersécurité et de la gestion technique de l'aviation (*Foundations of Aviation Cybersecurity Leadership and Technical Management*) : Ce cours a été élaboré en partenariat avec Embry-Riddle Aeronautical University et proposé à partir d'octobre 2021. Il s'agit d'un cours de sensibilisation complet qui couvre tous les aspects de la cybersécurité examinés dans la Stratégie de cybersécurité de l'aviation.

2.6.1.2 Gérer le risque de sûreté dans la gestion du trafic aérien (*Managing Security Risk in ATM*) : Ce cours a été élaboré en partenariat avec l'Organisation européenne pour la sécurité de la navigation aérienne (EUROCONTROL). Il porte sur les éléments tant matériels que virtuels de la sûreté dans la gestion du trafic aérien. La première session du cours aura lieu en novembre 2022.

2.6.1.3 Surveillance de la cybersécurité de l'aviation civile (*Cybersecurity oversight in civil aviation*) : Ce cours est actuellement élaboré en partenariat avec l'Autorité de l'aviation civile du Royaume-Uni. Il porte sur des points essentiels qui aideront les États à concevoir et respecter leurs obligations en matière de contrôle de la cybersécurité de l'aviation.

2.7 Activités de sensibilisation et d'information

2.7.1 La sensibilisation des États et des parties prenantes à l'importance de la prise en compte de la cybersécurité de l'aviation civile est l'une des principales activités de l'OACI. L'Organisation reste très activement engagée, en tant qu'organisatrice et/ou en tant que participante, dans les conférences, réunions et webinaires nationaux, régionaux et internationaux visant à promouvoir la coopération entre toutes les parties prenantes de la cybersécurité et de la cyberrésilience. Elle favorise en outre la mise en œuvre de la Stratégie de cybersécurité de l'aviation et du plan d'action pour la cybersécurité.

2.8 Audit des obligations en matière de cybersécurité au titre du Programme universel d'audits de sûreté — Méthode de surveillance continue

2.8.1 L'objectif du Programme universel d'audits de sûreté – Méthode de surveillance continue (USAP-CMA) est d'améliorer la sécurité mondiale dans le secteur de l'aviation par l'audit et la surveillance continue des résultats des États membres en matière de sûreté aérienne. Les auditeurs recherchent les documents établissant que les opérateurs ou les entités sont tenus d'identifier leurs systèmes critiques de technologie de l'information et des communications et les données utilisées pour l'aviation civile. Ils veillent aussi à ce que ces prescriptions comprennent l'évaluation, l'élaboration et la mise en œuvre de mesures visant à protéger ces informations et systèmes contre toute ingérence illicite. Une fois qu'ils ont recensé les prescriptions, les vérificateurs s'assurent que les responsabilités relatives à l'adoption de mesures de cybersécurité sont clairement attribuées.

2.8.2 Au 31 décembre 2021, 136 États avaient été contrôlés et les documents portant sur la préparation dans le domaine de la cybersécurité avaient été contrôlés dans 54 États. Selon les résultats de ces contrôles :

a) Quinze pour cent des États n'avaient pas établi d'obligation pour les exploitants ou les entités d'identifier leurs systèmes et données critiques en matière de technologies de l'information et des communications utilisés dans le cadre de l'aviation civile, conformément à une évaluation des risques, d'élaborer et de mettre en œuvre, le cas échéant, des mesures pour les protéger contre les interventions illicites ;

b) Vingt-six pour cent des États n'avaient pas défini les responsabilités des exploitants ou des entités concernant la cybersécurité de l'aviation civile ;

c) Quarante et un pour cent des États n'avaient pas élaboré de critères pour la protection des systèmes et données critiques des technologies de l'information et de la communication utilisés dans le cadre de l'aviation contre les interventions illicites.

2.8.3 Ces résultats ne sont pas nécessairement représentatifs de la situation globale en matière de protection de l'aviation contre les cybermenaces car, en raison de la pandémie de COVID-19, le contrôle a été mené à distance dans certains États et les résultats les concernant sont incomplets. En outre, la taille globale de l'échantillon n'est pas suffisamment représentative pour être complètement fiable. Néanmoins, les résultats montrent clairement que le secteur de l'aviation civile doit intensifier ses efforts afin qu'à son niveau minimum, la lutte contre les cybermenaces visant l'aviation civile permette d'assurer une protection régulière et harmonisée, d'atténuer les effets et de combattre ces menaces.

– – – – – – – – – – – –

APPENDICE

**PROJET DE RÉSOLUTION DE L'ASSEMBLÉE
SUR LA CYBERSÉCURITÉ DE L'AVIATION CIVILE**

~~A40-10~~ A41-xx : Cybersécurité de l'aviation civile

Considérant que le système mondial de l'aviation est un système éminemment complexe et intégré constitué de ~~technologies de l'information et des communications~~ systèmes qui sont ~~essentielles~~ essentiels 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, de l'intégrité et de la confidentialité ~~des systèmes de technologies~~ de l'information, des données et des ~~communications~~ systèmes~~, ainsi que de l'intégrité et de la confidentialité des données~~,

Consciente que ~~la menace représentée par~~ les ~~cyberincidents~~ cybermenaces pesant sur ~~pour~~ l'aviation civile ~~évolue rapidement et continuellement~~ sont en évolution rapide et constante, 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~~ l'aviation demeure une cible pour ceux qui mettent en œuvre des cybermenaces ou des menaces physiques, et que ~~cette menace peut facilement~~ ces cybermenaces peuvent évoluer et porter atteinte aux systèmes critiques de l'aviation civile dans le monde entier,

~~*Reconnaissant*~~ *Notant*[1] que tous les ~~problèmes~~ événements 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*~~ *Constatant*[2] 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 de l'aviation 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,

[1] Cette modification ne concerne que le français.
[2] Idem.

Réaffirmant l'importance et l'urgence de ~~protéger les~~ prendre en compte la cybersécurité et la cyberrésilience des systèmes, ~~et les~~ des données et des informations ~~des infrastructures~~ critiques de l'aviation civile contre les cybermenaces et les cyberrisques, notamment les interfaces communes entre l'aviation civile et l'aviation militaire,

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 de l'aviation, et de ~~prendre des mesures à court terme pour renforcer~~ favoriser la cybersécurité et la cyberrésilience ~~résistance~~ du système mondial de l'aviation face aux cybermenaces qui peuvent compromettre la sécurité et/ou la sûreté de l'aviation civile,

~~*Reconnaissant*~~ *Notant*[3] le rôle mobilisateur de l'OACI et le travail qu'elle mène en matière de cybersécurité et de cyberrésilience de l'aviation, ~~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~~ dans les différentes disciplines aéronautiques,

~~*Reconnaissant*~~ *Notant*[4] qu'il est nécessaire d'harmoniser la cybersécurité de l'aviation aux échelons mondial, régional et national afin ~~de promouvoir une cohérence mondiale et~~ d'assurer la cohérence et la pleine interopérabilité des mesures de protection et des systèmes de gestion du risque,

Mesurant l'importance d'élaborer des principes clairs de gouvernance et de responsabilité au niveau national en matière de cybersécurité de l'aviation civile, notamment en désignant une autorité nationale compétente responsable de la cybersécurité de l'aviation en coordination avec les autorités et agences nationales concernées,

~~*Reconnaissant*~~ *Prenant acte* de[5] la valeur des initiatives, plans d'action, publications et autres médias conçus pour faire face aux problèmes de cybersécurité de manière collaborative et ~~approfondie~~ intégrée,

L'Assemblée :

1. *Prie* instamment les États membres d'adopter et de ratifier ~~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~~ faire obstacle aux cybermenaces auxquelles est confrontée l'aviation civile :

a) mettre en œuvre la Stratégie de cybersécurité de l'aviation civile de l'OACI et s'appuyer sur le Plan d'action pour la cybersécurité de l'OACI afin de faciliter la mise en œuvre de la Stratégie ;

b) désigner l'autorité compétente pour les questions liées à la cybersécurité de l'aviation et définir les rapports entre cette autorité et les organismes nationaux concernés ;

[3] Idem.
[4] Idem.
[5] Idem.

~~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 ;~~

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

d) élaborer et mettre en œuvre un cadre de gestion des risques pour la cybersécurité solide et fondé sur les pratiques pertinentes en matière de gestion des risques pour la sécurité et la sûreté, et adopter une approche axée sur le risque pour protéger des cybermenaces les systèmes, les informations et les données critiques de l'aviation civile ;

~~j~~e) établir des politiques et des instruments 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 protégés et résistants ; les données soient sécurisées et disponibles pendant le stockage et le tranfert ~~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 plans de reprise à la suite d'incident soient élaborés et mis en pratique ; des analyses techniques des cyberincidents soient réalisées ;

~~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 ;~~

~~e~~f) encourager la coordination des gouvernements et de l'industrie quant aux stratégies, politiques et plans relatifs à la cybersécurité de l'aviation, ainsi que le partage d'informations pour aider à déceler les vulnérabilités critiques auxquelles il faut remédier ;

g) encourager la coopération civilo-militaire visant à recenser, protéger et surveiller les vulnérabilités et les flux de données communs aux connexions entre les systèmes d'aviation civils et militaires, et coopérer aux fins de la gestion des cybermenaces communes et de la reprise à la suite de cyberincidents ;

~~f~~h) 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 ;

~~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 ;~~

~~h~~i) ~~encourager~~ créer et faire respecter une solide culture ~~générale~~ de cybersécurité ~~dans les organismes nationaux et~~ dans l'ensemble du secteur de l'aviation civile ;

j) encourager les États à continuer d'apporter leur contribution à l'OACI en vue d'élaborer des normes internationales, des stratégies et des bonnes pratiques visant à renforcer la cybersécurité et la cyberrésilience de l'aviation ;

~~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~~ ;

k) continuer de collaborer à l'élaboration du cadre de cybersécurité de l'OACI selon une approche horizontale, transversale et fonctionnelle qui met à contribution la sécurité de l'aviation, la sûreté de l'aviation, la facilitation, la navigation aérienne, la communication, la surveillance, la gestion de la circulation aérienne, l'exploitation technique, ~~et~~ la navigabilité des aéronefs et d'autres disciplines pertinentes.

3. *Charge* ~~le Secrétaire général~~ l'OACI :

a) de continuer d'encourager l'adoption et la ratification universelles de la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* (Convention de Beijing) et du *Protocole complémentaire pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing) ;

~~a) d'élaborer un plan d'action pour appuyer les États et l'industrie dans l'adoption de la stratégie de cybersécurité~~ ;

b) de continuer à veiller à ce que les questions de cybersécurité et de cyberrésilience soient examinées et coordonnées dans toutes les disciplines pertinentes au moyen ~~des mécanismes appropriés dans l'esprit de la stratégie~~ du nouveau mécanisme d'examen des questions de cybersécurité de l'aviation à l'OACI.

— FIN —