



ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 13 : Sûreté de l'aviation — Politique

CYBERSÉCURITÉ DANS L'AVIATION CIVILE

(Note présentée par le Conseil de l'OACI)

RÉSUMÉ ANALYTIQUE

Le secteur de l'aviation civile est de plus en plus conscient des cybermenaces et des cyberrisques qui pèsent sur lui et prend des mesures pour y faire face. De nombreuses initiatives ont été prises au cours du dernier triennat à l'OACI ainsi que dans les États aux niveaux national, régional et mondial. Des travaux supplémentaires doivent toutefois être entrepris, en particulier au niveau national, pour garantir une approche globale, harmonisée et cohérente de la cybersécurité de l'aviation dans l'ensemble du secteur de l'aviation civile.

La présente note donne une vue d'ensemble des activités liées à la cybersécurité de l'aviation, y compris celles prescrites par l'Assemblée, et propose une mise à jour de la résolution A41-19 sur la *Cybersécurité dans l'aviation civile* afin de souligner qu'il importe de renforcer la protection et la résilience du secteur de l'aviation civile face aux cybermenaces et aux cyberrisques, tout en tenant compte de l'évolution des travaux de l'OACI sur ce sujet.

Suite à donner : L'Assemblée est invitée à :

- a) prendre note de l'évolution des activités de cybersécurité dans l'aviation ;
- b) adopter la résolution de l'Assemblée sur la *Cybersécurité dans l'aviation civile* figurant en appendice.

<i>Objectifs stratégiques :</i>	La présente note de travail se rapporte aux objectifs stratégiques <i>Chaque vol est sûr et sécurisé et L'aviation assure une mobilité fluide, accessible et fiable pour tous.</i>
<i>Incidences financières :</i>	Les activités décrites dans la présente note seront entreprises sous réserve des ressources prévues par le budget ordinaire pour 2026-2028 et/ou provenant de contributions extrabudgétaires, selon les indications contenues dans le Plan d'activités 2026-2028 de l'OACI.
<i>Références :</i>	Doc 10184, <i>Résolutions de l'Assemblée en vigueur (au 7 octobre 2022)</i> <i>Stratégie pour la cybersécurité de l'aviation</i> <i>Plan d'action pour la cybersécurité</i>

1. INTRODUCTION

1.1 Le secteur de l'aviation civile évolue rapidement en ce qui concerne l'utilisation de l'information et des nouvelles technologies pour répondre à ses besoins d'automatisation, d'interconnectivité et d'interopérabilité, ainsi que la mise en place de nouveaux concepts opérationnels au sol et dans les airs pour intégrer de nouveaux acteurs, tels que les systèmes d'aéronef non habité (UAS), dans le système de transport aérien. L'objectif ultime des changements est de soutenir la croissance du secteur de l'aviation civile tout en garantissant sa sécurité, sa sûreté, son efficacité, sa capacité et sa durabilité.

1.2 Toutefois, cette tendance a conduit à une augmentation des cybermenaces qui pèsent sur les systèmes opérationnels, les données et les informations. Cette augmentation est encore exacerbée par les tensions géopolitiques qui se font sentir dans le monde. Bien qu'il n'y ait eu aucun cas signalé de cyberattaque ayant eu des répercussions importantes sur la sécurité ou la sûreté aériennes, le secteur observe une tendance à la hausse du signalement des cyberincidents, qui, à ce jour, semblent être principalement motivés par le gain financier, le vol d'informations ou le cyberactivisme¹.

1.3 La complexité croissante des cybermenaces et leurs répercussions potentielles sur l'aviation civile soulignent la nécessité d'établir une approche mondiale, robuste et harmonisée pour renforcer la protection et la résilience du secteur face à ces menaces. À cet égard, l'OACI continue de travailler avec les États membres, les organisations internationales et le secteur pour les aider à atténuer les cyberrisques dans l'aviation civile.

1.4 La 41^e session de l'Assemblée de l'OACI a noté avec satisfaction l'évolution des travaux de l'Organisation sur la cybersécurité de l'aviation au cours du triennat (2019-2022) et a félicité l'Organisation et ses groupes d'experts pour leur travail. L'Assemblée s'est en particulier félicitée de l'adoption et de la mise en œuvre d'une structure de gouvernance interne renforcée pour la cybersécurité de l'aviation à l'OACI, ainsi que de l'élaboration continue de politiques, de dispositions, d'orientations, d'initiatives de renforcement des capacités et de sensibilisation en matière de cybersécurité de l'aviation. La 41^e session de l'Assemblée de l'OACI a également adopté la résolution A41-19 sur la *Cybersécurité dans l'aviation civile*, qui a remplacé la résolution A40-10.

2. ANALYSE

2.1 Normes et pratiques recommandées relatives à la cybersécurité de l'aviation

2.1.1 En réponse au point CyAP3.4 du plan d'action pour la cybersécurité (CyAP), qui demande à l'OACI de « réexaminer les normes et pratiques recommandées (SARP) actuelles de l'OACI en vue de déterminer la nécessité de les actualiser en fonction de la cybersécurité », l'OACI a réalisé en 2022 une analyse approfondie de chacune des seize Annexes à la *Convention relative à l'aviation civile internationale* (Convention de Chicago), dans le but de recenser les domaines susceptibles de faire l'objet des SARP de l'OACI relatives à la cybersécurité de l'aviation, en faveur d'une approche globale et transversale de la cybersécurité de l'aviation dans les dispositions de l'OACI.

2.1.2 L'analyse a été remise au Groupe d'experts de la cybersécurité, qui a créé une Équipe spéciale sur les normes et pratiques recommandées relatives à la cybersécurité (TF-CYSARPS), pour qu'il poursuive son travail en procédant au recoupement des champs d'intérêt possibles des différentes disciplines aéronautiques couvertes par les Annexes concernées. L'Équipe spéciale est chargée de déterminer si les SARP existantes couvrent adéquatement (de manière explicite ou implicite) la question

¹ Pour en savoir plus sur les cybermenaces et les cyberrisques qui pèsent sur le secteur de l'aviation civile, voir le document *Global Cyber Risk Considerations* (Considérations relatives aux cyberrisques dans le monde) (en anglais seulement) (Doc 10213 – Diffusion restreinte).

de la cybersécurité de l'aviation, de recenser les lacunes potentielles dans le cadre des SARP de l'OACI et de coordonner, avec les groupes d'experts compétents, les travaux nécessaires pour combler ces lacunes, le cas échéant. Les travaux sur ce sujet sont en cours et devraient se poursuivre tout au long du prochain triennat.

2.2 Instruments juridiques internationaux

2.2.1 L'étude consacrée à l'applicabilité des instruments de droit aérien international aux cybermenaces dirigées contre l'aviation civile, soumise à la 38^e session du Comité juridique, a conclu que la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale*² (Beijing, 2010 – « Convention de Beijing 2010 ») et le *Protocole additionnel à la Convention pour la répression de la capture illicite d'aéronefs*³ (Beijing, 2010 – « Protocole de Beijing 2010 ») contiennent des améliorations importantes par rapport aux instruments plus anciens, fournissant ainsi une base suffisante pour que les États érigent en infractions pénales les cyberattaques contre l'aviation civile.

2.2.2 Au 1^{er} avril 2024, 53 États membres avaient ratifié la Convention de Beijing de 2010 et 54 États membres avaient ratifié le Protocole de Beijing de 2010. Étant donné que ces instruments contiennent des dispositions pertinentes pour lutter contre les cyberattaques contre l'aviation civile, il est vivement recommandé aux États membres de les adopter et de les ratifier à grande échelle, comme le soulignent les résolutions de l'Assemblée sur la cybersécurité dans l'aviation civile, afin de favoriser la dissuasion des cybermenaces contre l'aviation civile et d'intensifier les poursuites pénales des cyberattaques contre le secteur.

2.3 Deuxième édition du Plan mondial pour la sûreté de l'aviation (GASeP)

2.3.1 Conformément au point CyAP2.5 du plan d'action pour la cybersécurité, qui demande à l'OACI d'inclure la cybersécurité dans les plans régionaux et mondiaux visant à assurer la sécurité, la sûreté et la résilience de l'aviation, et mettant à profit la mise à jour du GASeP dont la deuxième édition a été publiée en juin 2024 (<https://www.icao.int/Security/Pages/Global-Aviation-Security-Plan.aspx>), l'OACI a inclus la cybersécurité de l'aviation dans les dispositions du plan au titre des priorités globales 1, 2 et 4.

2.4 Éléments indicatifs

2.4.1 Conformément au plan d'action pour la cybersécurité, l'OACI a élaboré des éléments indicatifs⁴ pour aider les États et les parties prenantes à aborder la cybersécurité dans l'aviation civile, notamment des orientations sur la gouvernance et la politique de cybersécurité dans l'aviation au niveau des États, la culture de cybersécurité dans l'aviation civile, ainsi que la planification et la mise en œuvre du partage de renseignements sur la cybersécurité. L'OACI a également publié le *Global Cyber Risk Considerations* (Doc 10213 – Diffusion restreinte), un document d'orientation qui fournit une méthode pour intégrer la gestion des cyberrisques dans les processus de gestion des risques liés à la sécurité et à la sûreté de l'aviation, ainsi qu'à l'efficacité et à la capacité de la navigation aérienne, et qui présente une vue d'ensemble des cybermenaces et des cyberrisques à l'échelle mondiale :

2.4.2 Conformément à la recommandation 4.2/1 issue de la 14^e Conférence de navigation aérienne au sujet de la cybersécurité de l'aviation, les travaux en cours sur les éléments indicatifs comprennent l'élaboration d'un ensemble complet de documents d'orientation portant sur différents aspects de la cybersécurité de l'aviation. Il est également prévu de rassembler tous les éléments indicatifs dans un *Manuel de cybersécurité de l'aviation* qui couvre tous les aspects liés à la protection et à la résilience des infrastructures et services critiques de l'aviation face aux cybermenaces et aux cyberrisques.

² [Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale](#)

³ [Protocole additionnel à la Convention pour la répression de la capture illicite d'aéronefs](#)

⁴ <https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx>

2.5 Cadres de confiance

2.5.1 Lors de sa 220^e session en juin 2022, la Commission de navigation aérienne a approuvé la création du Groupe d'experts du cadre de confiance (TFP). Depuis lors, le TFP contribue à l'élaboration d'éléments indicatifs pour l'établissement de cadres de confiance interopérables :

- a) des orientations techniques pour la confiance interopérable et l'assurance de l'identité dans des contextes opérationnels ont été élaborées, y compris des orientations sur la sécurité de l'information (Doc 10204 – *Manuel sur la sécurité de l'information en aviation*) ;
- b) une politique commune de certification dans le domaine de l'aviation visant à favoriser l'interopérabilité des identités numériques, ainsi que l'authenticité et l'assurance de l'information dans l'aviation civile, y compris l'authentification des systèmes de renforcement satellitaire (SBAS) pour les systèmes mondiaux de navigation par satellite (GNSS) ;
- c) une liste de cas d'utilisation opérationnelle pour lesquels des cadres de confiance seraient utiles a été élaborée et est tenue à jour ; des travaux ont récemment commencé sur des orientations visant à aider les parties prenantes de l'aviation à établir des exemples de cadre de confiance ;
- d) des éléments indicatifs sur les communications air/sol sécurisées par le réseau de télécommunications aéronautiques utilisant les normes et protocoles de la suite de protocoles Internet (IPS) sont en cours d'achèvement, en étroite coordination avec les groupes d'experts concernés. Ces éléments viendront appuyer directement l'Amendement n° 93 de l'Annexe 10 – *Télécommunications aéronautiques*, volume III – *Systèmes de télécommunication*.

2.6 Programme des travaux de cybersécurité de l'OACI

2.6.1 À sa 228^e session, tenue en 2023, le Conseil a approuvé la création, la composition et le mandat du Comité ad hoc de coordination de la cybersécurité (AHCCC), une fois qu'il avait été déterminé que le Secrétariat disposait des ressources adéquates pour assurer son fonctionnement. L'AHCCC est composé d'un membre du Comité du transport aérien (ATC), du Comité de sûreté de l'aviation (ASC) et de la Commission de navigation aérienne (ANC), et de onze membres de chaque groupe d'experts traitant régulièrement de la cybersécurité dans le cadre de son programme de travail.

2.6.2 Les principales fonctions du comité consistent à coordonner les travaux liés à la cybersécurité de l'aviation au sein de l'OACI en élaborant et en tenant à jour un programme complet des travaux de l'OACI sur la cybersécurité de l'aviation. Il est également le principal organe consultatif du Conseil pour la hiérarchisation des éléments de travail conformément au programme des travaux.

2.6.3 L'AHCCC s'est réuni trois fois depuis sa création et continue de parfaire le programme des travaux de cybersécurité de l'aviation de l'OACI à mesure que progressent les travaux sur la cybersécurité. Il constitue un forum de collaboration pour les groupes d'experts qui permet le partage des informations et la promotion d'une approche harmonisée et cohérente de la cybersécurité de l'aviation dans le cadre de leurs domaines de travail respectifs.

2.7 Formation et renforcement des capacités

2.7.1 Le catalogue des formations à la cybersécurité de l'OACI comprend à ce jour deux cours sur la cybersécurité dans l'aviation :

- a) Fondements de la direction et de la gestion technique de la cybersécurité de l'aviation : Ce cours, élaboré par l'OACI en partenariat avec l'Embry-Riddle Aeronautical University, est offert depuis octobre 2021. Il s'agit d'un cours de sensibilisation complet qui couvre tous les aspects de la cybersécurité abordés dans la stratégie pour la cybersécurité de l'aviation. Au cours du précédent triennat, il a été dispensé à 88 participants entre septembre 2022 et avril 2025 ;
- b) Supervision de la cybersécurité dans l'aviation civile : Ce cours, élaboré par l'OACI en partenariat avec l'Autorité de l'aviation civile du Royaume-Uni, est offert depuis mars 2023. Il couvre les aspects essentiels qui aideraient les États à élaborer et à mettre en œuvre un cadre de supervision de la cybersécurité de l'aviation, en prenant l'expérience du Royaume-Uni comme exemple. Au cours du précédent triennat, il a été dispensé à 34 participants entre mars 2023 et avril 2025.

2.8 Activités de sensibilisation et d'information

2.8.1 Conformément aux appels lancés par la 41^e session de l'Assemblée à l'OACI pour que l'Organisation intensifie ses campagnes de sensibilisation et réalise des exercices de simulation de cybersécurité de l'aviation, celle-ci a bénéficié des contributions volontaires du Portugal et de Singapour au programme de cybersécurité de l'aviation, ce qui a permis d'élaborer et d'organiser au cours du triennat une série de cinq séminaires régionaux sur la cybersécurité de l'aviation.

2.8.2 Ces séminaires ont rassemblé des participants de toutes les disciplines aéronautiques et non aéronautiques concernées (sécurité de l'aviation, sûreté de l'aviation, navigation aérienne, cybersécurité, CERT/CSIRT nationaux, autorités nationales chargées de la cybersécurité, forces de l'ordre, militaires, etc.) Au total, les séminaires ont rassemblé plus de 450 participants.

2.8.3 Outre les exercices de simulation réalisés dans le cadre des séminaires régionaux sur la cybersécurité de l'aviation, l'OACI en a mené un le 5 juin 2025, en marge de la quatrième réunion du Groupe d'experts de la cybersécurité (CYSECP/4), pendant sa Semaine de la sûreté en 2023, ainsi que quatre exercices autonomes, ce qui porte à dix le nombre total d'exercices de simulation menés à l'échelle internationale par l'OACI au cours du triennat.

3. Révision de la résolution A41-19 de l'Assemblée

3.1 À la suite de l'adoption de la Déclaration de Mascate et compte tenu des résultats de la 14^e Conférence de navigation aérienne, les propositions de mise à jour de la résolution A41-19 de l'Assemblée sont présentées ci-après en appendice. La résolution a été mise à jour en coordination avec le Groupe d'experts de la cybersécurité de l'OACI, afin qu'elle soit harmonisée avec le contenu de la Déclaration et les résultats de la Conférence concernant la cybersécurité de l'aviation, ainsi qu'avec les définitions des termes de la cybersécurité de l'aviation approuvées par la troisième réunion du Groupe d'experts de la cybersécurité, et compte tenu de l'évolution des travaux de l'OACI sur le sujet.

— — — — —

APPENDICE

Résolution ~~A41-19~~ A42-XX : Cybersécurité dans l'aviation civile

L'Assemblée,

Considérant que le système mondial de l'aviation est un système éminemment complexe et ~~intégré~~ interconnecté constitué de données, d'informations et de systèmes qui sont essentiels à la sécurité, et à la sûreté, à l'efficacité et à la capacité des vols d'aviation civile,

Notant que le secteur de l'aviation dépend de plus en plus de la disponibilité, et de l'intégrité ~~et de la confidentialité~~ des données, de l'information, ~~des données~~, et des systèmes et, dans certains cas, de leur confidentialité,

Notant que la cybersécurité de l'aviation est essentielle au développement durable et efficace du transport aérien et qu'elle devrait par conséquent être considérée comme une priorité et bénéficier de ressources appropriées,

Consciente que les cybermenaces pesant sur l'aviation civile sont en évolution ~~rapide et constante~~ et qu'elles sont d'une ampleur, d'une complexité et d'une fréquence croissantes, que l'aviation demeure une cible pour des acteurs malveillants ~~ceux qui mettent en œuvre des cybermenaces ou des menaces physiques~~ tant dans l'environnement physique que cybernétique, et que ~~ces~~ les cybermenaces ~~peuvent~~ pourraient présenter des risques importants pour l'infrastructure critique de l'aviation civile, et compromettre ~~évoluer~~ et porter atteinte aux systèmes critiques de l'aviation civile dans le monde entier la sécurité, la sûreté, l'efficacité ou la capacité de l'aviation,

Constatant 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'y propager ~~s'étendre rapidement~~,

Notant que tous les événements de cybersécurité ~~cyberincidents~~ qui compromettent la sécurité, la sûreté, l'efficacité ou la capacité de l'aviation civile ne sont pas illégaux ~~et/ou~~ intentionnels,

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 additionnel à la Convention pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing) renforceraient le cadre juridique mondial pour ériger en infractions pénales ~~visant à considérer~~ les cyberattaques contre l'aviation civile internationale ~~comme des crimes~~, et qu'en conséquence la ratification et la mise en œuvre à grande échelle ~~par les États~~ de ces instruments par les États membres décourageraient et ~~pourrait punir~~ puniraient de telles attaques où qu'elles se produisent,

Réaffirmant l'importance et l'urgence de ~~prendre en compte~~ renforcer la cybersécurité et la cyberrésilience protection et la résilience des données, des informations et des systèmes, ~~des données et des informations critiques de l'aviation civile contre les~~ face aux cybermenaces et ~~les~~ aux cyberrisques, notamment les interfaces communes entre l'aviation civile et ~~l'aviation militaire~~ d'autres secteurs connectés,

Considérant la nécessité de travailler de façon collaborative en vue de l'élaboration d'un cadre mondial efficace et coordonné de cybersécurité de l'aviation et de favoriser ~~la cybersécurité et la cyberrésilience du système mondial de l'aviation~~ la protection et la résilience du secteur face aux cybermenaces ~~qui peuvent compromettre la sécurité et/ou la sûreté de l'aviation civile~~ et aux cyberrisques de manière harmonisée et cohérente,

Notant le rôle mobilisateur de l'OACI et le travail qu'elle mène en matière de cybersécurité de l'aviation ~~et de cyberrésilience~~, dans les différentes ~~l'ensemble des~~ disciplines aéronautiques,

Notant qu'il est nécessaire d'harmoniser la cybersécurité de l'aviation aux échelons mondial, régional et national afin ~~d'assurer de renforcer~~ la cohérence et ~~la pleine~~ l'interopérabilité des mesures et processus de protection ~~et des systèmes de gestion du risque~~ et de résilience,

Mesurant l'importance ~~pour les États d'élaborer des principes clairs de gouvernance et de responsabilité au niveau national en matière de~~ et de mettre en œuvre des plans pour la cybersécurité de l'aviation clairs et complets, qui tiennent compte des lois, règlements, politiques, procédures et mesures relatifs à la 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,

Prenant acte de la valeur des ~~dispositions, éléments indicatifs et initiatives, plans d'action, publications et autres médias~~ conçus pour faire face aux problèmes de cybersécurité de manière collaborative et intégrée,

Considérant les résultats de la 14^e Conférence de navigation aérienne, tenue à Montréal du 26 août au 6 septembre 2024, et les dispositions de la Déclaration de Mascate sur la sûreté et la cybersécurité de l'aviation, adoptée à Mascate (Oman) le 11 décembre 2024,

1. *Prie* instamment les États membres ~~d'adopter et de ratifier~~ et de mettre en œuvre la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* (Convention de Beijing) de 2010 ~~et du~~ le *Protocole additionnel à la Convention pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing) de 2010 comme moyen de viser les cyberattaques dirigées contre l'aviation civile ;
2. *Invite* les États et les parties prenantes du secteur à prendre les mesures suivantes pour faire face aux cybermenaces auxquelles est confrontée l'aviation civile :
 - a) mettre en œuvre la Stratégie de l'OACI pour la cybersécurité de l'aviation civile 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) élaborer et mettre en œuvre des plans nationaux de cybersécurité de l'aviation qui répondent aux objectifs stratégiques de cybersécurité de l'aviation et abordent la gouvernance et les responsabilités, les politiques, les communications, la gestion des cyberrisques, l'intervention et la reprise en cas d'incident, le renforcement des capacités et la formation, la conformité réglementaire et les audits, le suivi et l'amélioration continue, la documentation et la tenue de registres, dans le but de faire face aux cybermenaces et aux cyberrisques pour l'aviation civile d'une manière globale dans toutes les disciplines aéronautiques ;

- c) élaborer et appliquer des processus et des outils qui soutiennent la mise en œuvre et le suivi des plans de cybersécurité de l'aviation ;
- d) ~~b)~~ désigner l'autorité compétente pour les questions liées à la cybersécurité de l'aviation dans le cadre du plan national de cybersécurité de l'aviation et définir les rapports entre cette autorité et les organismes aéronautiques et non aéronautiques nationaux concernés ;
- e) ~~e)~~ définir les responsabilités des organismes nationaux et des parties prenantes du secteur en ce qui concerne la cybersécurité de l'aviation civile ;
- f) obtenir des ressources suffisantes pour garantir la disponibilité et la formation continue de professionnels de l'aviation et de la cybersécurité qualifiés et compétents, capables de réglementer, d'exploiter, de gérer, de maintenir et de superviser la mise en œuvre effective des lois, règlements, politiques, procédures et mesures applicables à la cybersécurité de l'aviation ;
- g) ~~d)~~ élaborer et mettre en œuvre un cadre de gestion des risques pour la cybersécurité cyberrisques solide et fondé sur qui intègre la gestion des cyberrisques dans les pratiques pertinentes en matière de gestion des risques pour la sécurité et, la sûreté, l'efficacité et la capacité, et adopter une approche axée sur le risque pour protéger des cybermenaces les renforcer la protection et la résilience des données, informations et systèmes critiques de l'aviation civile, les informations et les données critiques de l'aviation civile face aux cybermenaces et aux cyberrisques ;
- h) ~~e)~~ établir des lois, règlements, politiques, procédures et mesures et des instruments, selon qu'il convient, et affecter des ressources adéquates 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, l'utilisation ou le transfert ; la surveillance des systèmes et les méthodes de détection et de compte rendu d'incidents des cyberincidents soient mises en œuvre ; des plans d'intervention et de reprise à la suite d'incident soient élaborés et mis en pratique en coordination avec les plans d'intervention d'urgence et de gestion de crise établis ; des analyses techniques des cyberincidents soient réalisées ;
- i) ~~créer et faire respecter une solide~~ élaborer et mettre en œuvre des mesures concrètes pour renforcer la culture de cybersécurité dans toutes les entités de l'aviation civile dans l'ensemble du secteur de l'aviation civile ;
- ~~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 ;~~
- j) ~~h)~~ développer, à l'échelle nationale et internationale, des partenariats et des mécanismes gouvernements-industries entre gouvernements et entre gouvernements et industries, et jouer un rôle dans lesdits partenariats et mécanismes, afin que soient systématiquement partagées les informations sur les cybermenaces, les incidents, les vulnérabilités, les indicateurs de compromission, les tendances dans ce domaine, les mesures d'atténuation et les efforts efforts d'atténuation meilleures pratiques et enseignements tirés de l'expérience ;

- k) ~~g) encourager~~ développer les mécanismes de coopération ~~civilo-militaire~~ avec les autorités nationales compétentes, notamment mais sans s'y limiter, l'armée, les forces de l'ordre et les autorités chargées de la cybersécurité, afin de recenser, protéger et surveiller les vulnérabilités et les flux ~~de données d'information communs aux connexions entre les systèmes d'aviation civils et militaires~~ susceptibles de porter atteinte aux systèmes de l'aviation civile, et coopérer afin d'atténuer les cybermenaces communes et de s'y préparer, et coopérer aussi aux fins d'intervention et ~~la~~ de reprise à la suite de cyberincidents ;
- 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 ;~~
- l) ~~k)~~ continuer de collaborer ~~et de contribuer~~ à l'élaboration du cadre de cybersécurité de l'aviation de l'OACI selon une approche horizontale, transversale et fonctionnelle qui associe ~~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, la navigabilité des aéronefs et d'autres~~ toutes les disciplines aéronautique pertinentes, afin d'aborder de manière globale les cybermenaces et les cyberrisques qui pèsent sur la sécurité, la sûreté, l'efficacité et la capacité de l'aviation.

3. Charge l'OACI :

- a) de continuer d'encourager ~~l'adoption et~~ la ratification ~~universelles~~ universelle de la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* (Convention de Beijing) de 2010 et du *Protocole additionnel pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing) de 2010 ;
- b) de continuer à veiller à ce que les questions de cybersécurité de l'aviation ~~et de cyberrésilience~~ soient examinées et coordonnées dans toutes les disciplines pertinentes et de manière globale grâce à la collaboration entre tous les organes compétents de l'OACI ~~au moyen du nouveau mécanisme d'examen des questions de cybersécurité de l'aviation à l'OACI.~~