Plan d’action pour la cybersécurité

Publié sous l’autorité du Secrétaire général

Deuxième édition, janvier 2022

Organisation de l’aviation civile internationale

Terminologie[1]

Cybersécurité

Ensemble des technologies, des contrôles et des mesures, ainsi que des processus et des pratiques, conçus pour garantir la confidentialité, l'intégrité, la disponibilité et la protection globale des systèmes, réseaux, programmes, dispositifs, informations et données contre les attaques, les dommages et l'accès, l'utilisation et/ou l'exploitation non autorisés.

Entité (ou auteur) de menace

Entité partiellement ou entièrement responsable d'un incident ayant — ou susceptible d'avoir — un impact sur une organisation ou un système.

Évènement

Occurrence identifiée dans l'état d'un système, d'un service ou d'un réseau indiquant une violation possible de la politique de sécurité de l'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité de l'information [ISO/IEC 27035]. Il convient de noter que le terme « occurrence » doit être considéré au sens large et ne doit pas être compris dans son acception d'occurrence (de sécurité), qui désigne uniquement les événements qui revêtent ou sont susceptibles de revêtir une importance dans le contexte de la sécurité aérienne.

Incident

Un ou plusieurs événements indésirables relatifs à la sécurité de l'information et risquant fortement de compromettre les activités opérationnelles ou de menacer la sécurité des informations [ISO/IEC 27035-1].

Matrice de risque

Outil destiné à hiérarchiser et à mettre en évidence les composantes des risques (menace, probabilité, impact/conséquence et vulnérabilité), les mesures d'atténuation des risques mises en œuvre et, en dernière analyse, les risques résiduels.

Partage d'information

Processus par lequel des informations sont fournies par une entité à une ou à plusieurs autres entités pour faciliter la prise de décision fondée sur le risque et promouvoir les pratiques optimales.

Politique de cybersécurité

Document qui énonce les intentions et l'orientation d'une organisation en ce qui concerne la gestion des cybermenaces, formalisées par sa direction. L'organisation y décrit les moyens de se protéger contre les cybermenaces et de gérer les incidents et les événements lorsqu'ils se produisent.

Sécurité de l'information

Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. En outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées [BS ISO/CEI 27000:2018].

---

[1] Terminologie en cours d'examen.

Système de management de la sécurité de l'information (SMSI) de l'aviation civile

Modèle d'approche visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, maintenir et améliorer la protection des ressources informationnelles d'une organisation afin de réaliser les objectifs de l'aviation civile en se fondant sur une appréciation du risque et sur les niveaux d'acceptation du risque définis par l'organisation pour traiter et gérer les risques. Source : ISO27000:2009.

Vulnérabilité

Insuffisance d'un système d'information, des procédures de sûreté du système, des contrôles internes ou de la mise en œuvre, qui pourrait être exploitée ou déclenchée par une entité de menace. Il peut s'agir d'un système qui soutient directement ou indirectement une fonction du système de l'aviation.

RÉSUMÉ ANALYTIQUE

À sa 39e session, l'Assemblée de l'Organisation de l'aviation civile internationale 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, de ses 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 dans l'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 complet en matière de cybersécurité.

Pour répondre aux attentes de l'Assemblée, le Groupe d'étude du Secrétariat sur la cybersécurité (SSGC) a élaboré une stratégie de cybersécurité pour l'aviation civile.

À sa 40e session, l'Assemblée de l'OACI a adopté la résolution amendée A40-10 — *Cybersécurité dans l'aviation civile* —, qui appelle les États à mettre en œuvre la Stratégie de cybersécurité et souligne l'importance d'élaborer un plan de mise en œuvre durable de cette stratégie, et de poursuivre les travaux visant à élaborer un cadre de cybersécurité solide.

Le Plan d'action pour la cybersécurité (CyAP) établit les bases d'une collaboration entre les États, l'industrie, les autres parties prenantes et l'OACI en vue de renforcer la capacité d'identifier, de prévenir et de détecter les cyberattaques contre l'aviation civile, d'intervenir et d'assurer la reprise, ainsi que de définir un cadre de coopération solide. Le Plan d'action propose une série de principes, mesures et actions destinés à réaliser les objectifs des sept piliers de la stratégie.

Chapitre 1

INTRODUCTION

1.1 CONTEXTE

1.1.1 Le contexte actuel de l'aviation civile devrait se caractériser par une progression du trafic aérien à long terme, une évolution rapide de la technologie, une complexité croissante des modalités d'exploitation et un environnement opérationnel qui devient par conséquent plus exigeant. L'évolution rapide de la technologie transforme la manière dont l'aviation civile fonctionne, rendant le système plus vulnérable aux cybermenaces. La cybermalveillance peut viser l'aviation civile de diverses façons, allant d'une légère perturbation de l'exploitation jusqu'à des suites catastrophiques. Les risques augmentent rapidement, d'où l'impérieuse nécessité d'un cadre de cybersécurité durable aux niveaux international, régional et national.

1.1.2 La mise en place d'une solide infrastructure de cybersécurité, fondée sur une étroite coopération entre les États, l'industrie et l'OACI, permet une sensibilisation commune à la cybersécurité et contribuera à améliorer la sûreté et la résilience du système de l'aviation civile.

1.1.3 L'OACI s'adapte continuellement pour faire face à l'évolution constante de la situation mondiale en matière de menaces, conformément aux résolutions du Conseil de sécurité des Nations Unies, qui affirment la responsabilité incombant aux États de veiller à la sécurité des services aériens assurés sur leur territoire et appellent tous les États à collaborer avec l'OACI pour veiller à ce que les normes de sûreté internationales soient réexaminées, actualisées et mises en place, en fonction des risques actuels, conformément à la Convention de Chicago. Compte tenu de l'évolution et de la multiplication probable des cybermenaces pour l'aviation civile, l'OACI, conformément aux dispositions de la résolution 2341 (2017) du Conseil de sécurité, s'emploie résolument à établir des mécanismes appropriés pour atténuer et réduire les risques d'intervention illicite visant les infrastructures essentielles de l'aviation liés à des vecteurs de cybermenaces et à tout événement susceptible d'avoir une incidence sur la sécurité des opérations.

1.1.4 À cet égard, le présent Plan d'action a été conçu pour réaliser pleinement les objectifs des sept piliers de la Stratégie pour la cybersécurité de l'aviation et donner forme à un cadre de cybersécurité.

1.2 OBJET

1.2.1 Le présent plan est un document évolutif qui s'adaptera aux faits nouveaux concernant la cybersécurité et sera régulièrement actualisé en fonction des changements nécessaires découlant notamment de l'analyse des écarts et des activités décrites dans les Chapitres 3 et 4. Le Plan d'action pour la cybersécurité (CyAP) décrit les objectifs à atteindre et les actions à mener pour mettre en œuvre la Stratégie de cybersécurité de l'OACI pour l'aviation. Les éléments qui y sont présentés reflètent les travaux accomplis ou en cours dans différents États/régions, ou dans l'industrie. Le Plan prend en compte les résultats de l'analyse de la situation actuelle, « en l'état », du système de l'aviation en matière de cybersécurité, par rapport à la situation « future », proposée dans la Stratégie, et précise les actions à mener pour porter cette évolution vers la vision stratégique.

1.2.2 Compte tenu du travail considérable que nécessitent la réalisation des objectifs et la mise en œuvre des mesures définies dans le présent document, une approche graduelle, fixant des cibles à court, moyen et long terme, est proposée à l'Appendice A.

1.3 CONTEXTE DE RISQUE

1.3.1 Le concept de cybersécurité n'est pas nouveau dans l'aviation civile. Toutefois, les cybermenaces devenant un phénomène de plus en plus courant, la cybersécurité est aujourd'hui l'une des principales préoccupations dans l'examen et l'analyse des risques pour le système de l'aviation civile et des vulnérabilités du système. L'aviation civile est un secteur particulièrement exposé au risque, car les cyberattaques y ont plus de chance d'atteindre leur but, du fait de l'interdépendance fonctionnelle et numérique croissante de ses composantes, et aussi parce que les mécanismes de cyberdéfense actuellement en usage dans le secteur de l'aviation civile ne sont pas encore adaptés pour faire face à cette menace persistante et évolutive.

1.3.2 Le Groupe d'experts de la sûreté de l'aviation de l'OACI a récemment jugé moyen le niveau de risque découlant de l'exploitation d'une vulnérabilité dans un contexte terroriste. Cette évaluation est basée sur la vulnérabilité résiduelle dans le domaine de la cybersécurité, en supposant que les États ont effectivement mis en œuvre les dispositions de l'Annexe 17 — *Sûreté*. Cependant, les cyberrisques évoluent rapidement et doivent être évalués pour tous les profils de cyberattaquants susceptibles de porter atteinte non seulement à la sécurité, mais également à la sûreté de l'exploitation de l'aviation civile. De plus, l'origine des cyberattaques est souvent difficile à localiser, de sorte qu'il est souvent compliqué et difficile d'attribuer et de poursuivre les cyberattaques, alors que la victime d'une attaque ou ses assureurs doivent supporter les coûts de rétablissement. Pour ces raisons, il est de la plus haute importance que l'OACI, les États et l'industrie travaillent en collaboration à mettre en œuvre la Stratégie de cybersécurité de façon systématique.

1.4 AVANTAGES DU PLAN D'ACTION

1.4.1 Le CyAP a pour objectif d'obtenir l'engagement de l'OACI, des États membres et de l'industrie à mettre en œuvre la Stratégie pour la cybersécurité de l'aviation et à réaliser les objectifs définis par ses sept piliers. Un solide cadre de cybersécurité renforcera le système de l'aviation civile et sera bénéfique pour l'ensemble de la communauté de l'aviation mondiale.

Chapitre 2

OBJECTIF

2.1 OBJECTIF DU PLAN D'ACTION POUR LA CYBERSÉCURITÉ

2.1.1 Le Plan d'action pour la cybersécurité vise à réaliser les objectifs définis dans chacun des sept piliers de la Stratégie de cybersécurité, ainsi que de développer un solide cadre de cybersécurité pour l'aviation civile.

2.1.2 Le présent Plan d'action est fondé sur les principes suivants :

a) compréhension, par les États membres, des obligations qui leur incombent en matière de cybersécurité en vertu de la *Convention relative à l'aviation civile internationale* (Convention de Chicago), à savoir d'assurer la sécurité, la sûreté et la continuité des opérations de l'aviation civile ;

b) coordination des mesures de cybersécurité dans l'aviation civile entre les autorités des États membres en vue d'assurer la gestion efficace et efficiente de la cybersécurité de l'aviation au niveau mondial

c) engagement de toutes les parties prenantes de l'aviation civile à continuer de développer la cyberrésilience et à protéger l'aviation civile contre les cyberattaques susceptibles d'avoir une incidence sur la sécurité, la sûreté et la continuité du système de transport aérien, quel que soit le profil de l'auteur de la menace.

2.2 APPLICATION

2.2.1 Le présent plan, qui s'adresse principalement aux États membres de l'OACI et à l'industrie, se veut un outil destiné à les aider à gérer les risques de cybersécurité dans le secteur de l'aviation civile, selon une approche exhaustive, globale et coordonnée.

2.2.2 Les États, l'industrie et les autres parties prenantes concernées sont invités à mettre en œuvre les mesures décrites dans le présent plan.

Chapitre 3

PLAN D'ACTION STRATÉGIQUE

3.1 LES SEPT PILIERS DE LA STRATÉGIE POUR LA CYBERSÉCURITÉ DE L'AVIATION

3.1.1 Le présent chapitre propose une série de principes, mesures et actions axés sur la réalisation des objectifs des sept piliers de la Stratégie pour la cybersécurité de l'aviation, à savoir :

1. La coopération internationale
2. La gouvernance
3. Une législation et une réglementation efficaces
4. Une politique de cybersécurité
5. Le partage de l'information
6. La gestion des incidents et la planification d'urgence
7. Le renforcement des capacités, la formation et une culture de la cybersécurité

PREMIER PILIER — LA COOPÉRATION INTERNATIONALE
• Développer la coopération aux niveaux national et international entre toutes les parties prenantes. • Reconnaître mutuellement les efforts (développer, maintenir et améliorer la cybersécurité) pour protéger l'aviation civile. • Poursuivre l'harmonisation réglementaire aux niveaux mondial, régional et national afin de promouvoir la cohérence à l'échelon au niveau mondial et d'assurer l'interopérabilité des mesures de protection. • Engager les États à se pencher sur le thème de la cybersécurité dans l'aviation civile internationale. • Faciliter et promouvoir des manifestations internationales consacrées à la cybersécurité. • Reconnaître que la cybersécurité constitue une responsabilité partagée par tous les segments du système mondial de l'aviation civile.

DEUXIÈME PILIER — LA GOUVERNANCE
• Encourager, soutenir et consolider la Stratégie de cybersécurité de l'OACI. • Élaborer des dispositions claires pour la gouvernance et la transparence au plan national en ce qui concerne la cybersécurité dans l'aviation civile. • Assurer la coordination au niveau de l'État entre les autorités de l'aviation civile et les autorités nationales compétentes en matière de cybersécurité. • Établir des mécanismes de coordination appropriés entre les diverses autorités des États et l'industrie. • Inclure la cybersécurité dans les programmes nationaux de sécurité et de sûreté de l'aviation civile. • Inclure la cybersécurité dans les plans mondiaux et régionaux. • Travailler à l'élaboration d'une base commune pour des Normes et pratiques recommandées sur la cybersécurité.

TROISIÈME PILIER — UNE LÉGISLATION ET UNE RÉGLEMENTATION EFFICACES
• S’assurer que les instruments juridiques internationaux prévoient un cadre approprié pour dissuader les cyberincidents et pour engager des poursuites à l’encontre de leurs auteurs. • Analyser les lois nationales en vigueur et les actualiser ou les adopter, le cas échéant, pour permettre de dissuader les cyberattaques ayant un impact sur la sécurité, la sûreté, l’efficacité ou la continuité de l’aviation civile, de mener des enquêtes à leur sujet et d’engager des poursuites. • Veiller à la mise en place d’une réglementation et d’une législation nationales appropriées pour la cybersécurité de l’aviation civile. • Élaborer, à l’intention des États et de l’industrie, des lignes directrices relatives à la mise en œuvre des dispositions concernant la cybersécurité.

QUATRIÈME PILIER — UNE POLITIQUE DE CYBERSÉCURITÉ
• Veiller à ce que la cybersécurité ait sa place dans les systèmes de sécurité et de sûreté de l’aviation civile ainsi que dans des cadres complets de gestion des risques. • S’assurer que les diverses méthodes d’évaluation des risques de cybersécurité dans l’aviation civile demeurent comparables. • Élaborer des politiques de cybersécurité prenant en compte l’ensemble du cycle de vie des systèmes de l’aviation.

CINQUIÈME PILIER — LE PARTAGE DE L’INFORMATION
• Mettre en place ou exploiter des plates-formes et des mécanismes d’échange d’informations existants qui sont reconnus, en cohérence avec les dispositions actuelles de l’OACI, pour permettre de prévenir, de détecter précocement et d’atténuer les événements pertinents touchant la cybersécurité. • Veiller à ce que tout cyberincident ou toute vulnérabilité pouvant représenter un risque important pour la sécurité ou la sûreté de l’aviation soit signalé à l’autorité compétente.

SIXIÈME PILIER — LA GESTION DES INCIDENTS ET LA PLANIFICATION D’URGENCE
• S’assurer que des plans appropriés et évolutifs prévoient la continuité des opérations sûres et sécurisées de l’aviation civile en cas de cyberincidents. • Veiller à exploiter les plans d’urgence en place pour y inclure des dispositions permettant d’intervenir face aux incidents de cybersécurité et d’assurer la reprise , et effectuer régulièrement/périodiquement des exercices pour vérifier les capacités à détecter les cyberincidents, à intervenir et à assurer la reprise.

SEPTIÈME PILIER — LE RENFORCEMENT DES CAPACITÉS, LA FORMATION ET UNE CULTURE DE LA CYBERSÉCURITÉ
• Veiller à la qualification adéquate du personnel en fonction de son rôle dans le domaine tant de l'aviation que de la cybersécurité. • Accroître la sensibilisation à la cybersécurité, notamment les activités visant à instaurer une cyberhygiène appropriée. • Veiller à ce que le cadre éducatif national comprenne des programmes d'enseignement en bonne et due forme consacrés à la cybersécurité en aviation, afin d'assurer le développement d'un ensemble de connaissances sur la sécurité et la sûreté de l'aviation dans toute l'organisation, y compris au niveau de la haute direction. • Encourager l'innovation ainsi que les activités de recherche et développement dans le domaine de la cybersécurité. • Inclure la cybersécurité dans la stratégie de l'OACI pour la « Prochaine génération de professionnels de l'aviation ».

Chapitre 4

MISE EN ŒUVRE, SURVEILLANCE ET RÉEXAMEN

4.1 MISE EN ŒUVRE

Le CyAP s'adresse à l'OACI, à ses États membres, à l'industrie et aux autres parties prenantes. Chaque entité est encouragée à adopter les cibles retenues selon la feuille de route (voir l'Appendice A), qui définit les résultats attendus et les Mesures prioritaires, ainsi que les tâches qui s'y rapportent. Cela aidera l'OACI, les États et les autres parties prenantes à concentrer leurs travaux sur la mise en œuvre de mesures et d'actions efficaces visant à atteindre l'objectif consistant à mettre en place un solide cadre mondial de cybersécurité dans l'aviation.

4.2 SURVEILLANCE ET RÉEXAMEN

L'OACI procédera à un réexamen du CyAP en tant que de besoin. Elle actualisera également les cibles et les échéanciers prévus dans le CyAP. Seront concernés notamment des domaines dans lesquels les États ont besoin d'être épaulés dans la mise en œuvre du CyAP et/ou le renforcement de leurs capacités, ainsi que d'autres initiatives utiles.

4.3 PARTENARIAT

Toutes les parties prenantes de l'aviation doivent prendre part à l'effort nécessaire pour améliorer en permanence la cybersécurité dans l'aviation civile. Le CyAP offre un cadre de référence commun pour toutes les parties prenantes et définit les actions que l'OACI, les États membres et l'industrie doivent mener pour mettre en place un cadre de cybersécurité commun.

4.4 RÔLES DE L'OACI, DES ÉTATS ET DES PARTIES PRENANTES

4.4.1 L'OACI sera appelée à jouer un rôle moteur et de surveillance au niveau mondial dans la mise en œuvre et la coordination du CyAP, en prenant en charge notamment :

- l'actualisation du CyAP en tant que de besoin ;
- l'élaboration et l'actualisation de normes et pratiques recommandées (SARP) et de Procédures pour les services de navigation aérienne (PANS), complétées par des manuels et d'autres éléments utiles ;
- la surveillance et le réexamen de la situation en matière de cybermenaces et de cyberrisques ;
- la fourniture d'une assistance ciblée pour remédier aux insuffisances en matière de cybersécurité dans l'aviation civile.

4.4.2 Les États et l'industrie ont également un rôle important à jouer dans la mise en œuvre et l'efficacité du CyAP. Les États et les autres parties prenantes sont encouragés à faire la démonstration, d'une année sur l'autre, des progrès qu'ils auront accomplis dans la mise en œuvre du plan.

Chapitre 5

COOPÉRATION INTERNATIONALE

5.1 ÉTABLISSEMENT D'UN INVENTAIRE DES INITIATIVES DE CYBERSÉCURITÉ EN AVIATION

5.1.1 Un inventaire des initiatives de cybersécurité sera établi, tenu à jour et mis à la disposition du public approprié sur le portail de l'OACI. Cet inventaire comprendra les initiatives déjà engagées, ainsi que les initiatives existantes du secteur de l'aviation en matière de cybersécurité aux niveaux mondial, régional ou national. L'inventaire ne se limitera pas à ces initiatives, mais englobera également celles dont les résultats présentent un intérêt pour l'aviation civile (p. ex., la cybersécurité dans d'autres domaines des transports ou dans des secteurs comme l'énergie ou la finance).

5.2 ÉTABLISSEMENT D'UNE BASE COMMUNE POUR L'INTEROPÉRABILITÉ DES MESURES DE CYBERSÉCURITÉ ET DES SYSTÈMES DE GESTION [2]

5.2.1 Les États et l'industrie sont invités à mettre en œuvre des principes et outils/systèmes adaptés en vue d'assurer l'uniformité, la sûreté et l'interopérabilité de la gestion des systèmes de technologies de l'information et de communication.

5.2.2 La confiance constituant le fondement de l'efficacité, de l'uniformité et de l'interopérabilité de la gestion des échanges d'informations, il conviendrait d'appuyer l'élaboration du cadre de confiance pour l'aviation internationale qui facilite la gestion des informations et l'interopérabilité ; de plus, les politiques et les procédures devraient être exploitées dans la mesure du possible par toutes les parties prenantes concernées.

5.2.3 L'interopérabilité des mesures de cybersécurité et de la gestion peut également reposer sur la participation à diverses formes d'accord de coopération internationale. Un modèle pour de tels accords devrait être élaboré afin de permettre la coopération tout en respectant les politiques applicables en matière de vie privée, de sécurité de l'information et de sûreté nationale. À cet égard, cette base commune pour la conclusion de ces accords devrait comprendre les éléments suivants :

- le sujet et l'objectif de l'accord ;
- les entités qui pourraient conclure ce type d'accord ;
- les rôles et les responsabilités de ces entités ;
- les mesures qui pourraient servir à améliorer la cybersécurité dans l'aviation civile et qui devraient faire l'objet d'une coordination.

5.2.4 Les accords internationaux devraient porter sur :

- l'établissement d'un dialogue entre les parties prenantes pour débattre des moyens visant à réduire le risque collectif et à protéger les infrastructures nationales et internationales de l'aviation civile ;

[2] Les systèmes de gestion, dans ce contexte, comprennent les systèmes de gestion du risque, mais pas uniquement.

- des mesures de réduction et d'atténuation des risques pour parer aux cybermenaces visant l'aviation civile ;
- l'échange d'informations sur les lois nationales relatives à l'aviation civile, et sur les stratégies, politiques et meilleures pratiques nationales en matière de cybersécurité ;
- des mesures visant à appuyer le renforcement des capacités dans le domaine de la cybersécurité, le cas échéant.

5.2.5 Étant donné les nombreux principes et modèles, avec leur terminologie, qui peuvent être en usage chez les parties prenantes de l'aviation, il est primordial d'élaborer un lexique et un cadre de compréhension communs, particulièrement en ce qui concerne la cybersécurité de l'aviation civile. À cet égard, une série de principes généraux pour la gestion coordonnée de la cybersécurité au niveau mondial doit être développée à l'échelon de l'OACI, en étroite coopération avec les États membres et l'industrie. Une analyse du cadre actuel sera effectuée afin de déterminer la meilleure façon de parvenir à un alignement efficace et sans faille de ces principes et modèles.

5.3 ÉTABLISSEMENT D'UNE TERMINOLOGIE COMMUNE

5.3.1 Une terminologie commune de la cybersécurité relative à l'aviation civile sera élaborée sous l'égide de l'OACI, compte tenu de la terminologie existante de la cybersécurité en général et de la terminologie et des cadres de l'aviation, afin que les parties prenantes de l'aviation, quels que soient leur expérience et leur niveau d'activité, soient en mesure de se comprendre.

5.3.2 L'objectif consiste à faciliter les activités se rapportant à la cybersécurité. Cela ne veut pas dire qu'une définition unique sera arrêtée et/ou adoptée pour tous les termes. Il est en effet concevable qu'un même terme ait plusieurs définitions (p. ex., probabilité, gravité, occurrence), si celles-ci renvoient à un certain contexte et que leur répétition n'engendre pas de confusion susceptible d'entraîner une gestion inefficace des risques de cybersécurité de l'aviation civile. Plus précisément, dès lors qu'une place plus importante est faite à la gestion intégrée des risques de sécurité et de sûreté, l'OACI doit veiller tout particulièrement à ce que la terminologie soit correctement alignée. Si l'on se reporte à la description initiale du contexte (voir plus haut), et à la clarification entre la sûreté, qui consiste à gérer les actes illicites intentionnels, et la sécurité, qui porte sur les événements intentionnels, non intentionnels et aléatoires, il importe de préciser davantage les choses en ce qui concerne les questions de gestion intégrée des risques, qui peut couvrir les préoccupations à la fois de sûreté et de sécurité (les définitions des Annexes 17 et 19 de l'OACI peuvent servir de références). Plus précisément, compte tenu de l'orientation différente des disciplines de la sûreté et de la sécurité (la sûreté s'intéressant aux risques intentionnels, non intentionnels ou aléatoires et la sécurité se concentrant sur les actes illicites et intentionnels), l'introduction d'une gestion intégrée des risques couvrant les deux disciplines exige une clarté quant à la portée et à l'objectif des termes utilisés.

5.4 CARTOGRAPHIE GÉNÉRALE DES ÉCHANGES D'INFORMATION/INTERACTIONS DANS L'AVIATION

5.4.1 Un cadre commun pour l'établissement de cartes fonctionnelles de haut niveau décrivant les échanges d'informations entre tous les acteurs de l'aviation est une condition préalable nécessaire pour garantir la compréhension du paysage des cyberrisques. Un cadre commun pour l'établissement d'une cartographie de haut niveau pour les échanges d'informations entre toutes les parties prenantes de l'aviation est nécessaire pour parvenir à une compréhension du paysage des cyberrisques.

5.4.2 Cette cartographie des échanges d'information/interactions devrait être suffisamment générale pour englober tous les types d'opérations liées à l'aviation et devrait, dans la mesure du possible,

être indépendante des architectures physiques et/ou techniques en place (approche par fonction/service). Elle devrait, par exemple, recenser les flux de données numériques utilisées pour la gestion du trafic aérien, les activités aéroportuaires, et les flux de données numériques relatives aux opérations en vol et de maintenance des aéronefs. Elle devrait tirer parti de toutes les initiatives déjà engagées par d'autres groupes. Il s'agirait de permettre à chaque acteur de compléter, d'adapter et de personnaliser sa propre cartographie en fonction des modalités de son interaction avec les autres parties prenantes. En fin de compte, chaque partie prenante devrait être en mesure de développer cette cartographie ou de l'adapter à sa propre situation. En conséquence, les résultats des évaluations des risques de sûreté conduites par chaque acteur selon sa méthodologie et ses critères propres (qui seront comparables, car fondés sur un cadre d'évaluation commun — voir la section 5.6) pourraient être échangés/partagés avec d'autres parties prenantes, dans la mesure du possible. En œuvrant de concert, à l'aide de cadres d'évaluation comparables des risques de sûreté et de la cartographie des échanges d'informations/interactions, les parties prenantes seront à même de comprendre comment les risques peuvent se propager à d'autres partenaires ou être maîtrisés par ceux-ci, et ainsi de contribuer au partage d'information sur les risques auxquels est exposée, ou qu'engendre, chacune d'elles.

5.5 DÉVELOPPEMENT DU PARTAGE DE L'INFORMATION SUR LES RISQUES ENTRE ORGANISATIONS

5.5.1 De nombreux documents d'orientation et normes sont consacrés à la responsabilité qui incombe à chaque organisation à l'égard de sa propre gestion de la cybersécurité, et qui concerne les systèmes, processus, produits et données internes. Cependant, étant donné que les risques de cybersécurité pour l'aviation civile sont communs à de multiples parties prenantes, il importe de dépasser le niveau de chaque organisation. Pour parvenir à une gestion efficace et efficiente des risques communs, il importe de mettre en évidence le partage de l'information sur les risques, qui est caractéristique des situations où des systèmes, processus, produits ou données sont mis en commun ou transmis d'une organisation à une autre.

5.5.2 Il conviendrait d'envisager la conclusion d'accords externes avec des fournisseurs tiers pour permettre l'échange d'informations sensibles en matière de cybersécurité entre une organisation et les autorités/organes de réglementation compétents, afin de faciliter la gestion des risques et des menaces liés à la chaîne logistique.

5.6 DÉFINITION DES CRITÈRES DE COMPARABILITÉ DES ATTITUDES À L'ÉGARD DE L'ÉVALUATION DU RISQUE

5.6.1 Dans un environnement où les risques s'étendent à de multiples organisations, il est essentiel que les parties prenantes puissent comprendre les risques dans leur intégralité, de bout en bout, ainsi que l'attitude des autres parties prenantes à l'égard de la gestion de ces risques. Dans ce contexte, il conviendrait d'établir des critères qui permettent la compréhension aisée et la comparabilité des évaluations des risques de cybersécurité.

5.7 ÉTABLISSEMENT D'UNE COORDINATION CIVILO-MILITAIRE APPROPRIÉE

5.7.1 Lorsque cela est possible et cohérent avec la loi nationale, y compris, mais sans s'y limiter, avec les impératifs de la sécurité et de la défense nationales, les autorités compétentes de l'aviation civile et de l'armée devraient mettre en place les capacités et les processus nécessaires pour coopérer sur les questions liées à la cybersécurité de l'aviation.

5.7.2 La mutualisation et la coordination appropriées, à un stade précoce, des informations relatives à la cybersécurité entre les parties prenantes de l'aviation civile et celles de l'aviation militaire

peuvent se révéler extrêmement utiles pour détecter des cybermenaces et cyberrisques potentiels et ainsi contribuer à la réduction efficace des cyberrisques auxquels le système de l'aviation pourrait être exposé

5.7.3 La mise en commun de l'information entre les parties prenantes civiles et militaires de l'aviation est également importante dans la gestion des cybercrises. Les États peuvent offrir leur concours à leurs parties prenantes nationales de l'aviation civile et militaire pour définir des modalités destinées à faciliter autant que possible le partage de l'information par des mécanismes appropriés.

5.8 PROMOTION DES MANIFESTATIONS MONDIALES ET RÉGIONALES POUR LA CYBERSÉCURITÉ DANS L'AVIATION CIVILE

5.8.1 L'OACI appuiera et planifiera l'organisation de manifestations mondiales et régionales destinées à promouvoir la cybersécurité dans l'aviation civile, en tant que de besoin.

Chapitre 6

GOUVERNANCE

6.1 ÉTABLISSEMENT D'UNE STRUCTURE DE GOUVERNANCE

6.1.1 L'OACI devrait établir, pour la cybersécurité de l'aviation, une structure de gouvernance interne qui assure une approche globale, transversale et fondée sur les risques de la cybersécurité et de la cyberrésilience dans tous les domaines et champs d'expertise pertinents de l'aviation.

6.1.2 De plus, les États devraient définir et mettre en place des structures nationales de gouvernance et de responsabilité pour la cybersécurité de l'aviation civile, en veillant à l'élaboration et à la mise en œuvre des exigences nationales et internationales en matière de cybersécurité et de cyberrésilience, ainsi qu'en définissant le rôle et les responsabilités de chaque partie prenante au niveau national. Cette évolution devrait aussi tenir compte de la nécessité d'assurer la coordination entre les autorités nationales compétentes en matière d'aviation civile et de cybersécurité.

6.2 ÉLABORATION DE PLANS PLURIANNUELS POUR LA CYBERSÉCURITÉ

6.2.1 Il est recommandé d'aligner correctement le Plan d'action pour la cybersécurité (CyAP) sur le Plan pour la sûreté de l'aviation dans le monde (GASeP), le Plan mondial de navigation aérienne (GANP) et le Plan pour la sécurité de l'aviation dans le monde (GASP), et d'inclure et de promouvoir les aspects liés à la cybersécurité dans ces plans s'il y a lieu.

6.2.2 Afin d'assurer la bonne mise en œuvre et application des plans mondiaux au niveau national, les États sont instamment invités à inclure des mesures correspondantes et coordonnées à l'échelon national en matière de cybersécurité dans leurs programmes nationaux de sécurité et de sûreté, et dans leurs plans de navigation aérienne.

6.3 DÉVELOPPEMENT DE LA GOUVERNANCE ET DE LA RESPONSABILITÉ

6.3.1 L'OACI devrait élaborer des orientations pratiques sur la cybersécurité afin de faciliter l'harmonisation et la cohérence entre les politiques de cybersécurité mondiales, régionales et nationales.

6.3.2 La gouvernance de la cybersécurité devrait être axée sur les politiques et mise en application, et il convient de déterminer les responsabilités en matière de conformité.

6.3.3 Les États devraient prendre des mesures concrètes pour améliorer en permanence l'efficience, la qualité et la cohérence des processus de gestion de la cybersécurité au niveau national.

6.3.4 Au besoin, les systèmes de management de la sécurité de l'information (SMSI) peuvent se révéler des outils efficaces pour gérer la cybersécurité et ils sont susceptibles d'être mis en œuvre au niveau de l'État ou de l'organisation[3].

[3] Pour développer la gouvernance de la cybersécurité au niveau national, les États peuvent s'inspirer de la norme ISO 27001 en vue de définir les principes de direction, par exemple : veiller à ce que les exigences du système de gestion de la sûreté de l'information soient intégrées aux processus des organisations ; veiller à ce que les ressources nécessaires soient disponibles ; et veiller à ce que le système de management de la sécurité de l'information produise les résultats attendus.

Chapitre 7

EFFICACITÉ DE LA LÉGISLATION ET DU CADRE RÉGLEMENTAIRE

7.1 EXAMEN DES INSTRUMENTS DE DROIT AÉRIEN INTERNATIONAL EN VIGUEUR DANS LE DOMAINE DE LA CYBERSÉCURITÉ

7.1.1 L'OACI procédera à une analyse des instruments internationaux actuels de droit aérien afin de mettre en évidence les lacunes existantes et potentielles concernant les cyberrisques et proposera des solutions possibles pour les combler, s'il y a lieu, en vue d'améliorer la protection de l'aviation civile.

7.2 MAINTIEN DE L'ALIGNEMENT DES DISPOSITIONS DE L'OACI SUR LES BESOINS EN MATIÈRE DE CYBERSÉCURITÉ

7.2.1 Au fur et à mesure que la cybersécurité dans l'aviation se développe, il peut être nécessaire d'élaborer des dispositions pour compléter les SARP et les PANS en vigueur. Cela devrait être fait au cas par cas, en notant que l'ajout de nouvelles dispositions de SARP et de PANS devrait être évité dans toute la mesure du possible et, si nécessaire, coordonné entre toutes les parties prenantes concernées.

7.3 RATIFICATION DE LA CONVENTION ET DU PROTOCOLE DE BEIJING

7.3.1 Les États sont encouragés à ratifier la *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale* (Convention de Beijing, 2010) et le *Protocole additionnel à la Convention pour la répression de la capture illicite d'aéronefs* (Protocole de Beijing, 2010).

7.4 ÉLABORATION ET APPLICATION PAR LES ÉTATS D'UNE LÉGISLATION ET D'UNE RÉGLEMENTATION APPROPRIÉES AU NIVEAU NATIONAL

7.4.1 Les États sont encouragés à évaluer leurs cadres juridiques actuels à l'égard de la cybersécurité et de l'aviation civile afin de détecter d'éventuelles lacunes et de s'assurer que les lois et les règlements appropriés sont en place pour les éléments spécifiques de la cybersécurité dans l'aviation civile. Un autre élément clé est le mécanisme d'application que les États sont encouragés à mettre en œuvre, s'il n'existe pas déjà dans leurs cadres juridiques nationaux, pour criminaliser les actes illicites contre l'aviation civile commis à l'aide de cybermoyens et pour engager les poursuites nécessaires.

Chapitre 8

POLITIQUE DE CYBERSÉCURITÉ

8.1 ÉLABORATION ET MISE EN ŒUVRE DES POLITIQUES DE CYBERSÉCURITÉ

8.1.1 Une politique de cybersécurité doit être définie aux niveaux national et organisationnel. Les États devraient mettre en place une politique de cybersécurité claire et réalisable qui comprenne :

- des objectifs découlant des résultats d'évaluations des cyberrisques dans l'aviation civile ;
- un engagement à satisfaire aux exigences applicables et les moyens d'évaluer la conformité à ces exigences ;
- des considérations relatives à la gestion et à la coordination avec des parties dépendantes extérieures (voir le chapitre sur la collaboration internationale) ;
- un engagement à améliorer en permanence le cadre de cybersécurité ;
- des dispositions visant à garantir que la politique est entièrement documentée et disponible en tant qu'information officielle ;
- des dispositions visant à assurer une diffusion appropriée de la politique.

8.2 IDENTIFICATION ET ÉVALUATION DES CYBERRISQUES QUI MENACENT L'AVIATION CIVILE

8.2.1 L'une des difficultés que posent l'identification et l'évaluation des risques est de pouvoir anticiper l'évolution rapide des origines et des caractéristiques des menaces. L'anticipation de l'évolution des menaces est essentielle pour aider le système de transport aérien à adapter de manière proactive sa stratégie de protection non seulement en fonction des menaces actuelles, mais aussi à la lumière des menaces potentielles futures. Le secteur de l'aviation civile devrait ainsi être mieux en mesure d'être proactif dans un contexte caractérisé par une asymétrie entre les agresseurs, qui sont très agiles et ne cessent de s'adapter, et les défenseurs qui, en raison de la complexité du système à protéger, réagissent avec lenteur. Dans ce scénario, cette approche proactive devient d'autant plus cruciale. Il est donc nécessaire de définir un cadre d'identification et d'évaluation des cyberrisques permettant de répondre à ce besoin d'anticipation, afin de contribuer à atténuer ces risques.

8.2.2 Il est recommandé d'identifier et d'évaluer les cyberrisques en tenant compte de toutes les conséquences possibles d'une attaque dirigée contre le système de l'aviation civile (sûreté, sécurité, efficacité, résilience, continuité du service, etc.), ainsi que de toutes les sources de menace potentielles et des vulnérabilités qui découlent de ces menaces. Cette activité devrait s'inspirer des matrices de cyberrisques élaborées sous l'égide du Groupe de travail sur la menace et les risques (WGTR) du Groupe d'experts de la sûreté de l'aviation.

8.2.3 Étant donné qu'une forte proportion des cyberrisques qui menacent l'aviation civile concerne de nombreuses parties prenantes, il est recommandé d'envisager une cartographie des échanges d'information/interactions dans le secteur de l'aviation (voir le Chapitre 5.1). Cette cartographie devrait être utilisée comme un moyen de garantir l'exhaustivité des scénarios pris en compte et de permettre aux parties prenantes de comprendre les modalités de leur interaction ainsi que leur dépendance à l'égard des risques.

8.2.4 Étant donné que le niveau de gravité des risques liés à la cybersécurité variera dans le temps et que ces risques peuvent évoluer rapidement par rapport à d'autres, il est recommandé d'envisager un moyen d'adapter à ces risques toute réponse de l'aviation mondiale qui peut être déployée rapidement et de manière cohérente (p. ex. concilier la nécessité de se conformer à des normes aéronautiques, éléments indicatifs, pratiques exemplaires extérieures à l'aviation, et recourir/se fier à des mesures provenant d'autres domaines).

8.2.5 Il est recommandé que l'identification et l'évaluation des cyberrisques soient intégralement assurées par un groupe composé d'experts de la cybersécurité dans l'aviation civile ou, à défaut, par une équipe d'experts mixte, de la cybersécurité et de l'aviation civile, de préférence avec une expérience approfondie en matière de cybersécurité.

8.2.6 Ce groupe d'experts serait responsable de l'élaboration d'un état du contexte de risque mondial de cybersécurité.

Chapitre 9

PARTAGE D'INFORMATIONS

L'échange des informations relatives à la cybersécurité est essentiel à la gestion des risques de cybersécurité qui menacent les systèmes de l'aviation civile. Reconnaissant que la promotion du partage des informations est un élément clé de l'instauration d'une culture de la cybersécurité, les parties prenantes de l'aviation civile devraient, dans la mesure du possible, élaborer ou exploiter les programmes actuels et mettre en œuvre des programmes permettant le partage des informations dans leurs organisations et avec des parties extérieures. Grâce à ces programmes, elles devraient nouer des partenariats et partager des informations de fond avec d'autres parties prenantes qui possèdent et exploitent des infrastructures d'aviation civile, et mettre au point des systèmes et des pratiques de partage d'informations au sein de leurs organisations.

Ces programmes d'échange d'informations devraient permettre la mise en place, le fonctionnement et l'adaptation des cyberdéfenses de l'aviation civile contre les cybermenaces connues et nouvelles. Ils devraient contribuer au développement :

- de la connaissance de la situation, tant dans le cadre des opérations normales et quotidiennes que pendant une crise, un incident ou un événement ;
- de la gestion des risques opérationnels et tactiques en prévision et en réponse à une menace ;
- de la planification stratégique pour développer des capacités qui renforcent la cybersécurité et la résilience à l'avenir.

9.1 DÉVELOPPEMENT DU PARTAGE D'INFORMATIONS SUR LES RISQUES

9.1.1 L'échange d'informations de cybersécurité comprend des aspects bilatéraux et multilatéraux — et peut faire intervenir, selon diverses combinaisons (au plan national, régional ou mondial), les parties suivantes :

- autorités nationales chargées de la cybersécurité ;
- autorités nationales de l'aviation civile ;
- autorités nationales de l'aviation militaire ;
- autres parties prenantes de l'aviation (exploitants, fournisseurs de services et constructeurs) ;
- parties prenantes non liées à l'aviation (fournisseurs de technologies de l'information et des communications et chaîne logistique).

9.1.2 Il est reconnu qu'il existe de nombreuses catégories d'informations relatives à la cybersécurité, par exemple :

- Le *cyberrenseignement*, concernant notamment la situation en matière de menaces, les renseignements sur les capacités et les intentions des acteurs de la cybermenace.
- Les *indicateurs de compromis (IoC).*
- Les *tactiques, techniques et procédures (TTP),* comme les scénarios d'attaques et les méthodes privilégiées par les pirates informatiques.
- Les *vulnérabilités,* notamment au niveau du matériel, du logiciel, du service, du protocole, de la norme, etc., y compris les scénarios d'exploitation potentiels.
- Les *rapports d'incident*.

9.1.3 Selon la législation nationale et la nature de l'information de cybersécurité, le partage d'information peut faire l'objet de diverses méthodes ou contraintes avec divers destinataires (p. ex., autorité nationale chargée de la cybersécurité, autorité nationale de l'aviation civile, autorité nationale de l'aviation militaire et autres parties prenantes de l'aviation).

9.1.4 Les besoins et les politiques relatifs au partage d'information et à la collaboration devraient être définis (notamment en période de crise, mais pas seulement) aux niveaux mondial, régional et national.

9.1.5 Il est recommandé d'utiliser le *Traffic Light Protocol* (TLP)[4] pour indiquer le niveau de distribution/restrictions lorsque l'on diffuse et partage plus largement de l'information de cybersécurité.

9.1.6 Dans la mesure du possible, l'information de cybersécurité, qui peut contenir certains éléments sensibles, devrait être anonymisée et aseptisée avant d'être partagée, plutôt que non partagée du tout.

9.2 ÉLABORATION DE PRINCIPES ET D'ORIENTATIONS POUR LA DIVULGATION RESPONSABLE DES RÉSULTATS DE RECHERCHE DANS LE DOMAINE DE LA SÉCURITÉ

9.2.1 Étant donné l'intérêt croissant que les chercheurs en sécurité portent à la cybersécurité dans l'aviation civile, et afin d'éviter la divulgation irresponsable de résultats de recherche susceptibles d'être préjudiciables à la sécurité, à la sûreté, à l'efficacité ou à la continuité de l'aviation civile, il importe de définir des principes pour guider la divulgation responsable des vulnérabilités constatées par les chercheurs en matière de sûreté ou d'autres parties, afin de s'assurer que les divulgations ne sont pas préjudiciables à la cybersécurité de l'aviation civile. La définition de ces principes devrait prendre en compte la recommandation 4.4 de la Stratégie de cybersécurité.

9.2.2 Les orientations associées à ces principes (portant notamment sur la constatation, la notification du fabricant, l'investigation, la résolution, la notification de l'industrie et, enfin, la diffusion auprès du public) devraient être établies entre, d'une part, les chercheurs et tiers, et d'autre part, les autorités de l'aviation et les parties prenantes de l'aviation, afin de s'assurer autant que possible que la recherche et la constatation des vulnérabilités, et les activités relatives à leur révélation n'aient pas d'incidence sur la sécurité et la prestation de services. Idéalement, les orientations ne porteraient pas uniquement sur les processus de divulgation responsable, mais comprendraient aussi des éléments axés sur la sensibilisation et l'éducation.

9.3 CRÉATION D'UN RÉSEAU MONDIAL D'AUTORITÉS RÉGIONALES/NATIONALES DE LA CYBERSÉCURITÉ POUR L'AVIATION CIVILE

9.3.1 L'attribution de la responsabilité en matière de cybersécurité au sein des États et dans l'industrie n'est pas uniforme, et les compétences nécessaires couvrent un large éventail de parties prenantes de l'aviation et du secteur non aéronautique, et de domaines fonctionnels. La préoccupation que soulève par définition cette variété rend difficile l'identification du correspondant approprié au sein d'une entité, ainsi que l'établissement et le maintien de voies de communication formalisée entre les parties prenantes. Des orientations relatives aux modalités d'établissement et de maintien d'un correspondant unique pour les questions de cybersécurité dans l'aviation civile au sein des États et des organisations

[4] Se reporter aux Orientations relatives au *Traffic Light Protocol*.

peuvent faciliter la création de voies de communication aux niveaux mondial, régional et national, la constitution de communautés de cybersécurité efficaces et l'impulsion d'une culture de la cybersécurité.

9.4 CAPACITÉ MONDIALE DE PARTAGE DE L'INFORMATION DE CYBERSÉCURITÉ POUR L'AVIATION

9.4.1 Les capacités de partage d'information peuvent être développées transversalement aux niveaux mondial, régional et/ou national pour favoriser l'échange d'information de cybersécurité.

9.4.2 Les forums de partage d'informations peuvent inclure des structures publiques-publiques, publiques-privées et privées-privées. Les parties prenantes devraient collaborer avec des communautés de confiance pour faciliter l'échange de bonnes pratiques et de renseignements sur les menaces.

Chapitre 10

GESTION DES INCIDENTS ET PLANIFICATION D'URGENCE

10.1 RENFORCEMENT DES CAPACITÉS DE RÉPONSE AUX INCIDENTS ET PLANIFICATION DES INTERVENTIONS D'URGENCE

10.1.1 Toutes les parties prenantes sont vivement encouragées à élaborer et à tester des plans de réponse aux incidents et des plans d'urgence de manière coordonnée avec leurs partenaires opérationnels, notamment :

- utilisation des plans d'urgence actuels et/ou modification de ces plans pour y inclure des dispositions relatives à la cybersécurité ;
- élaboration et mise à jour par les parties prenantes de l'aviation civile de plans évolutifs adéquats assurant la sécurité, la sûreté et la continuité du transport aérien dans l'éventualité de cyberincidents ;
- élaboration de dispositions relatives aux capacités d'intervention et de reprise en cas d'incident de cybersécurité, y compris des plans d'intervention en cas d'urgence ;
- association des parties prenantes de l'aviation militaire au processus de planification, afin d'établir proactivement des voies de communication ;
- réalisation de niveaux de performance acceptables et le respect des exigences de maintien des niveaux de service minimum pour les services essentiels ;
- mise au point d'une catégorisation harmonisée pour le compte rendu des cyberincidents, et coordination des systèmes de notification des incidents de cybersécurité dans l'aviation civile aux niveaux national, régional et, le cas échéant, international ;
- conduite régulière, par les parties prenantes de l'aviation, d'exercices réels pour tester la validité des hypothèses formulées lors de la planification et des exercices sur table.

10.2 MOYENS DE DÉTECTION DES INCIDENTS, D'ANALYSE ET D'INTERVENTION AU NIVEAU DES PARTIES PRENANTES

10.2.1 Dans la mesure du possible, des plans de réponse aux incidents devraient être mis en œuvre, et les parties prenantes devraient développer les capacités de détection, d'analyse et de réponse aux incidents de cybersécurité à tous les niveaux. Il est important de suivre la situation, au regard de la cybersécurité, des systèmes/services jugés critiques pour le soutien de l'aviation civile, afin de détecter d'éventuels problèmes et de surveiller l'efficacité continue des mesures de sécurité protectrices. Une fois que des incidents de cybersécurité sont détectés, il convient de les analyser et de déclencher les plans d'intervention appropriés, qui doivent comprendre des mesures visant à limiter l'impact de l'incident de cybersécurité.

10.3 CRÉATION D'UNE CELLULE DE COORDINATION DE CRISE POUR LA CYBERSÉCURITÉ DANS L'AVIATION CIVILE

10.3.1 Il convient de créer, dans la mesure du possible (à partir des mécanismes déjà en place), une cellule de coordination de crise pour l'aviation civile comprenant des spécialistes de la cybersécurité et à laquelle devraient être associées, le cas échéant, les parties prenantes de l'aviation militaire.

10.3.2 Il conviendrait aussi de procéder régulièrement à des exercices périodiques, en particulier des exercices sur table (XT), avec la participation de toutes les parties prenantes concernées de l'industrie le cas échéant.

Chapitre 11

RENFORCEMENT DES CAPACITÉS, FORMATION ET CULTURE DE LA CYBERSÉCURITÉ, ET SENSIBILISATION

11.1 RENFORCEMENT DES CAPACITÉS TECHNIQUES, DÉVELOPPEMENT DE LA FORMATION ET DE LA CULTURE DE LA CYBERSÉCURITÉ, ET ÉLABORATION DE MATÉRIEL ÉDUCATIF

11.1.1 Il conviendrait de définir et de promouvoir l'éducation, la formation et la sensibilisation à la cybersécurité dans l'aviation civile aux niveaux mondial, régional et national.

11.1.2 La culture de la cybersécurité et les activités éducatives connexes devraient être encouragées par la haute direction dans l'ensemble des organisations de l'aviation civile, et devraient être présentées de façon à mettre en évidence les rôles essentiels des différents acteurs et ce qui est attendu d'eux. Elle devrait conduire à la constitution d'un socle de connaissances chevauchant la sécurité et la sûreté de l'aviation et devrait inclure :

- des notions de principes de sécurité intégrée à la conception pour atténuer les cybermenaces, en coordination avec les spécialistes de la sécurité. Ces connaissances devraient aider les spécialistes de la sécurité en aviation à prendre des décisions mieux informées face à des cybermenaces ;
- une approche coordonnée entre les parties prenantes de la sécurité et de la sûreté, reconnaissant que les contrôles de sûreté ne doivent pas avoir d'incidence négative sur la sécurité des vols, permettant le transfert de connaissances techniques et garantissant que des décisions éclairées sont prises sur la base d'un environnement de risque mutuellement compris ;
- une connaissance des pratiques relevant de la « cyberhygiène », pour le personnel d'exploitation et de soutien qui devrait contribuer à prévenir les incidences négatives pour le système de l'aviation civile, susceptibles d'être causées par le nombre croissant de produits disponibles sur le marché et de maliciels génériques ;
- une connaissance de la « culture d'équité » dans le monde de la sécurité, qui permet et encourage l'autodéclaration d'occurrences résultant d'un comportement involontaire du personnel (p. ex., mauvais usage involontaire d'une clé USB).

11.1.3 Ces activités devraient mettre l'accent sur l'incidence ou l'incidence potentielle.

11.1.4 Le développement et la promotion de cette culture de la cybersécurité et la promotion de matériel éducatif connexe devraient contribuer à une compréhension mutuelle/commune, au sein des communautés de la sécurité et de la sûreté, de l'environnement de risque pour la cybersécurité, ainsi qu'à une confiance mutuelle concernant les contre-mesures mises en place.

11.1.5 L'OACI devrait encourager les programmes d'échange entre les États et entre les régions sur l'éducation et la formation à la cybersécurité[5].

11.1.6 La culture de la cybersécurité et les activités d'éducation y afférentes ne doivent pas être centrées sur le fonctionnement des systèmes, mais plutôt sur l'ensemble de leur cycle de vie et prendre en compte :

- exigences (la sûreté est intégrée dès la phase des exigences) ;
- conception (adoption d'une stratégie de sécurité intégrée à la conception, sûreté du matériel, des logiciels et des données, gestion du changement et gestion de la vulnérabilité) ;
- développement (environnement sécurisé, tests de sûreté continus et intégrés) ;
- fabrication/acquisition (y compris la chaîne d'approvisionnement en matériel et en logiciels des technologies opérationnelles et de l'information) ;
- exploitation (y compris la gestion de l'accès, l'intégrité des données, la sûreté d'exploitation des systèmes) ;
- maintenance (y compris la stratégie de mise à jour et de correctifs) ;
- suppression (y compris la gestion des justificatifs d'identité et des données résiduelles sur les dispositifs de stockage).

[5] Par exemple, les initiatives concernant les campus multinationaux ou le réseau et les centres de compétence en cybersécurité de l'UE.

Chapitre 12

CONCLUSION

Le Plan d'action pour la cybersécurité associe l'OACI, les États, l'industrie et d'autres parties prenantes dans un effort global et coordonné pour relever les défis de cybersécurité actuels et émergents. Il met en évidence le caractère transversal de la cybersécurité, qui concerne tous les domaines du secteur de l'aviation. Le plan contribue à la mise en œuvre de la Stratégie pour la cybersécurité de l'aviation de l'OACI et à l'évolution vers la création d'un cadre solide de cybersécurité mondiale.

– – – – – – – – – – – –

APPENDICE A

Feuille de route du Plan d'action pour la cybersécurité

STRATÉGIE DE CYBERSÉCURITÉ — ACTIONS GÉNÉRALES À MENER

Résultat prioritaire	**ÉLABORER UNE VISION MONDIALE CONCERTÉE**
Mesures prioritaires	• Reconnaître qu'il est impératif d'élaborer une vision exhaustive et concertée de la cybersécurité, comme base d'une gestion mondiale solide et coordonnée des risques de cybersécurité dans l'aviation. • Reconnaître que le secteur de l'aviation civile doit être résilient aux cyberattaques, et demeurer sûr et fiable dans le monde entier, tout en continuant d'innover et de croître. • Reconnaître que les risques de cybersécurité dans l'aviation civile doivent être traités dans le cadre de la Convention relative à l'aviation civile internationale.

Mesures

Mesure	**Par**	**Mesures/tâches spécifiques**	**Indicateurs**	**Niveau de priorité**	**Date de début de la mise en œuvre**
CyAP 0.1	OACI, États membres, et industrie	L'OACI élaborera un modèle de politique de cybersécurité auquel les États membres et l'industrie pourront se référer pour élaborer leurs propres politiques nationales/organisationnelles.	Mise à disposition du modèle aux États membres et à l'industrie.	Élevé	2021
CyAP 0.2	OACI et États membres	Débuter les travaux de mise en œuvre de la Stratégie pour la cybersécurité de l'aviation de l'OACI au niveau national (conformément à la Résolution A40-10) (afin de vérifier la mise en œuvre par les États, il faudra élaborer une série d'indicateurs pour mesurer la concrétisation de certaines actions).	Preuve nationale du début des travaux de mise en œuvre.	Élevé	2023
CyAP 0.3	OACI	Mener des enquêtes en vue d'établir comment les États ont mis en œuvre la Stratégie pour la cybersécurité de l'aviation de l'OACI (il devra être demandé aux États s'ils ont défini un plan d'action pour mettre en œuvre la Stratégie).	Enquête/questionnaire de l'OACI envoyé aux États membres.	Élevé	2021-2022

PILIERS DE LA STRATÉGIE DE CYBERSÉCURITÉ

Résultat prioritaire	**1. RÉALISER LA COOPÉRATION INTERNATIONALE**
Mesures prioritaires	• Développer la coopération aux niveaux national, régional et international entre toutes les parties prenantes. • Reconnaître mutuellement les efforts (développer, maintenir et améliorer la cybersécurité) visant à protéger l'aviation civile. • Poursuivre l'harmonisation réglementaire aux niveaux international, régional et national, afin de promouvoir la cohérence à l'échelle mondiale et d'assurer l'interopérabilité des mesures de protection. • Engager les États à se pencher sur le thème de la cybersécurité dans l'aviation civile internationale. • Faciliter et promouvoir des manifestations internationales consacrées à la cybersécurité. • Reconnaître que la cybersécurité est une responsabilité partagée par tous les segments du système mondial de l'aviation civile.

Mesures

Mesure	**Par**	**Référence dans la Stratégie pour la cybersécurité de l'aviation**	**Référence dans le Chapitre 5**	**Mesures/tâches spécifiques**	**Indicateurs**	**Niveau de priorité**	**Date de début de la mise en œuvre**
CyAP 1.1	OACI et États membres	1.1	5.2	Inclure la cybersécurité dans les programmes de supervision de la sécurité et de la sûreté de l'OACI – inclure les normes pertinentes dans les programmes d'audit de l'OACI (tels que l'USOAP et l'USAP).	Les programmes d'audit de l'OACI, tant du point de vue de la sécurité que de la sûreté, comprennent les normes pertinentes de cybersécurité.	Élevé	En cours
CyAP 1.2	OACI	1.1	5.1 Voir également CyAP 4.6 (§ 8. du Plan d'action)	Mener des enquêtes pour recenser les initiatives et pratiques en matière de cybersécurité en vue de déterminer comment les États et l'industrie gèrent la cybersécurité dans l'aviation civile.	Résultats des questionnaires, nombre d'initiatives et de régions.	Élevé	En cours
CyAP 1.3	OACI	1.1	5.1	Dresser un inventaire de toutes les initiatives de cybersécurité engagées dans les différents groupes d'experts de l'OACI.	Un programme de travail de l'OACI en matière de cybersécurité dans l'aviation est élaboré et actualisé par le Comité ad hoc de coordination de la cybersécurité.	Élevé	2024

CyAP 1.4	OACI et États membres	1.2	5.2.3 et 5.5 Voir également CyAP 5.1 (§ 9.2 du Plan d'action)	A) Élaborer des modèles de protocoles d'entente/de collaboration, des accords extérieurs B) Fournir des lignes directrices sur la façon d'élaborer ces accords.	Disponibilité du modèle et des lignes directrices.	Faible	2023-2024
CyAP 1.5	OACI, États membres, et industrie	1.2	5.3	Élaborer une terminologie cohérente et acceptée de la cybersécurité dans l'aviation civile, de façon que toutes les parties prenantes de l'aviation, quels que soient leur expérience et leur niveau d'activité, puissent se comprendre quand il est question de cybersécurité.	Publication d'un glossaire sur la cybersécurité.	Moyen	2023
CyAP 1.6	OACI, États membres, et industrie	1.2	5.4	L'OACI élaborera un cadre commun pour la définition d'une cartographie fonctionnelle générale décrivant les échanges d'information entre les parties prenantes de l'aviation (p. ex., ANSP, AOC, A/C, aéroport, MET, MRO, CNS), condition nécessaire pour faciliter la compréhension de la situation en matière de cyberrisques. Les États membres et l'industrie élaboreront des cadres de ce genre aux niveaux national et organisationnel.	Existence d'un cadre commun et d'une cartographie générique des échanges d'informations/ interactions dans l'aviation Sensibilisation et compréhension relativement à la cartographie fonctionnelle.	Élevé	2024
CyAP 1.7	OACI et États membres	1.2	5.7 Voir également CyAP 6.2 et § 10.2 du Plan d'action)	L'OACI établira des modèles de coopération entre l'aviation civile et militaire afin d'élaborer, s'il y a lieu, des modèles/orientations pour les interfaces d'interopérabilité entre l'aviation civile et militaire. Déterminer les critères et le niveau d'interaction appropriés.	Disponibilité de modèles/d'orientations pour la coopération et l'interopérabilité civile/militaire en matière de cybersécurité. Publication de la liste des critères et des interactions minimales requises.	Élevé	2023

CyAP 1.8	OACI, États membres et industrie	1.3	5.8	Planifier, organiser et soutenir des manifestations internationales et régionales en vue de promouvoir la cybersécurité dans l'aviation civile.	Manifestations, activités de sensibilisation, coopération internationale.	Sans objet	En cours
CyAP 1.9	OACI, États membres, et industrie	1.3	5.4	Veiller à ce que toutes les parties prenantes concernées soient associées aux discussions et aux activités concernant la cybersécurité dans l'aviation civile : Ouverture à la participation permanente des parties prenantes concernées.	Publier les résultats des efforts communs Publier les preuves de participation telles que partenariats, appartenance à un groupe, etc.	Élevé	En cours
CyAP 1.10	OACI, États membres, et industrie	1.2	5.2.2	Élaborer un cadre de confiance pour l'aviation internationale qui permette l'interopérabilité des entités sur la base de la confiance qu'elles ont dans les autres parties prenantes.	Mise en place d'un cadre de confiance utilisé par de nombreuses organisations.	Élevé	2024-2025

Résultat prioritaire	**2. DÉVELOPPER LA GOUVERNANCE ET LA TRANSPARENCE**
Mesures prioritaires	• Encourager et appuyer la Stratégie de cybersécurité de l'OACI et y donner suite. • Élaborer des dispositions claires pour la gouvernance et la transparence sur le plan national en ce qui concerne la cybersécurité dans l'aviation civile. • Assurer la coordination au niveau de l'État entre les autorités de l'aviation civile et les autorités nationales compétentes en matière de cybersécurité. • Établir des mécanismes de coordination appropriés entre les diverses autorités des États et l'industrie. • Inclure la cybersécurité dans les programmes nationaux de sécurité et de sûreté de l'aviation civile. • Inclure la cybersécurité dans les plans mondiaux et régionaux. • Travailler à définir une base commune pour l'élaboration de normes et pratiques recommandées relatives à la cybersécurité.

Mesures

Mesure	**Par**	**Référence dans la Stratégie de cybersécurité**	**Référence dans le Chapitre 6**	**Mesures/tâches spécifiques**	**Indicateurs**	**Niveau de priorité**	**Date de début de la mise en œuvre**
CyAP 2.1	OACI et États membres		6.1	Établissement d'une structure de gouvernance dans le domaine de la cybersécurité de l'aviation civile.	Détermination de la structure de gouvernance la plus adéquate pour la cybersécurité de l'aviation civile.	Sans objet	2021-2023

CyAP 2.2	OACI et États membres	2.2	6.3	L'OACI élaborera un ensemble de principes généraux pour des systèmes de gestion adéquate de la cybersécurité de l'aviation civile. Les États membres élaboreront ces principes au niveau national selon le modèle de l'OACI.	Publication des principes généraux.	Élevé	2023-2024
CyAP 2.3	OACI, États membres, et industrie	2.2	6.3.2 Voir également § 8.1. du Plan d'action	Élaborer des éléments indicatifs pour aider les organisations à mettre en œuvre des cadres coordonnés de gestion de la cybersécurité afin d'appuyer la mise en place d'une approche systématique pour gérer les risques de cybersécurité dans l'aviation et évaluer le degré de maturité et l'efficacité de ces cadres.	Publication de lignes directrices.	Élevé	2023
CyAP 2.4	OACI et États membres	2.2	6.3	Promouvoir les mécanismes de coordination entre les autorités de l'aviation civile et celles chargées de la cybersécurité.	Enquête de l'OACI – nombre de mécanismes de coordination déjà mis en place	Moyen	2022
CyAP 2.5	OACI	2.3	6.2.1 Voir également CyAP 1.9 (§ 5.2 du Plan d'action)	L'OACI intégrera la cybersécurité dans les plans régionaux et mondiaux, pour garantir la sécurité, la sûreté et la résilience de l'aviation.	Publication des plans actualisés.	Sans objet	2022-2023
CyAP 2.6	OACI		6.2	L'OACI préparera une section « registre/lignes directrices sur les meilleures pratiques » dans le répertoire.	Répertoire des meilleures pratiques de l'OACI.	Sans objet	2020-2021
CyAP 2.7	OACI, États membres et industrie	3.2	6.3	L'OACI élaborera des procédures types pour signaler les cyberincidents, notamment des orientations sur la classification des incidents. Les États membres et l'industrie élaboreront des procédures nationales et organisationnelles pour signaler les cyberincidents en temps utile et de	Procédures de signalement des cyberincidents/nombre d'incidents signalés selon les procédures.	Élevé	2022-2023

				manière efficace.			
CyAP 2.8	OACI et États membres	2.2	6.2	L'OACI évaluera dans quelle mesure les États membres incluent la cybersécurité dans leurs programmes nationaux de sécurité et de sûreté de l'aviation civile et dans leurs plans de navigation aérienne.	Enquête de l'OACI — nombre d'États ayant inclus la cybersécurité dans leurs programmes nationaux de sécurité et de sûreté de l'aviation civile.	Élevé	Enquête en 2022, Mesures supplémentaires en cours
Résultat prioritaire	**3. ÉLABORER UNE LÉGISLATION ET UNE RÉGLEMENTATION EFFICACES**						
Mesures prioritaires	• S'assurer que les instruments juridiques internationaux prévoient un cadre approprié pour dissuader les cyberincidents et pour engager des poursuites à l'encontre de leurs auteurs. • Analyser les lois nationales en vigueur et les actualiser ou les adopter, le cas échéant, pour permettre de dissuader les cyberattaques ayant un impact sur la sécurité, la sûreté, l'efficacité ou la continuité de l'aviation civile, de mener des enquêtes à leur sujet et d'engager des poursuites. • Veiller à la mise en place d'une réglementation et d'une législation nationales appropriées pour la cybersécurité de l'aviation civile. • Élaborer, à l'intention des États et de l'industrie, des lignes directrices relatives à la mise en œuvre des dispositions concernant la cybersécurité.						
Mesures							
Mesure	**Par**	**Référence dans la Stratégie de cybersécurité**	**Référence dans le Chapitre 7**	**Mesures/tâches spécifiques**	**Indicateurs**	**Niveau de priorité**	**Date de début de la mise en œuvre**
CyAP 3.1	États membres	3.3	7.4	Les États membres ratifieront les instruments de Beijing.	Nombre d'États ayant ratifié les instruments de Beijing.	Élevé	En cours
CyAP 3.2	OACI	3.3	7.3	Analyser les instruments internationaux de droit aérien.	Examen et analyse des écarts des instruments pertinents du droit aérien international.	Élevé	2022
CyAP 3.3	OACI et États membres	3.3 et 3.4	7.2	Analyser la législation nationale en vigueur dans le domaine de la cybersécurité de l'aviation civile et identifier les lacunes, y compris en droit pénal.	Enquête sur l'état de la législation nationale en ce qui concerne le traitement des actes illicites contre l'aviation civile commis par des cybermoyens.	Moyen	2023-2024
CyAP 3.4	OACI	3.3	7.1	Réexaminer les normes et pratiques recommandées en vue de déterminer la nécessité de les actualiser en fonction de la cybersécurité.	Examen et analyse des écarts des SARP de l'OACI.	Élevé	2022

CyAP 3.5	OACI	3.2		Créer, revoir et modifier les éléments indicatifs relatifs à la mise en œuvre des exigences de cybersécurité de l'aviation civile.	Publication d'éléments indicatifs sur la cybersécurité de l'aviation civile.	Élevé	2021 et en cours
Résultat prioritaire	**4. ÉLABORER UNE POLITIQUE DE CYBERSÉCURITÉ**						
Mesures prioritaires	• Veiller à ce que la cybersécurité ait sa place dans les systèmes de sécurité et de sûreté de l'aviation civile ainsi que dans des cadres complets de gestion des risques. • S'assurer que les diverses méthodes d'évaluation des risques de cybersécurité de l'aviation civile demeurent comparables. • Élaborer des politiques de cybersécurité prenant en compte l'ensemble du cycle de vie des systèmes de l'aviation.						
Mesures							
Mesure	**Par**	**Référence dans la Stratégie de cybersécurité**	**Référence dans le Chapitre 8**	**Mesures/tâches spécifiques**	**Indicateurs**	**Niveau de priorité**	**Date de début de la mise en œuvre**
CyAP 4.1	États membres et industrie	4.1	8.1	Les États membres et l'industrie veilleront à l'engagement de leurs directions à traiter la question de la cybersécurité et de la cyberrésilience de l'aviation civile.	Campagne de sensibilisation / Preuves d'engagement telles que des déclarations d'engagement, définition des responsabilités dans le domaine de la cybersécurité dans les manuels de gestion des autorités et des organisations.	Moyen	2022-2023
CyAP 4.2	OACI, États membres, et industrie	4.3	8.2 Voir également § 5.11 du Plan d'action	Encourager la recherche et le développement dans le domaine de la cybersécurité en aviation civile en collaborant avec des universités, des instituts, des communautés de chercheurs, etc.	Nombre d'interactions et de projets.	Élevé	2022-2023
CyAP 4.3	États membres, et industrie	4.2	5.6 et 8.2	Définir des critères pour une évaluation transorganisationnelle commune des risques, ainsi que l'information à partager et les critères nécessaires pour assurer la comparabilité des méthodes d'évaluation. Les États membres définiront ces critères au niveau national, et l'industrie le fera au niveau organisationnel.	Publication des objectifs et des critères pour une évaluation des risques transorganisationnelle partagée.	Élevé	2023

CyAP 4.4	OACI, États membres, et industrie	4.3	8.1	Élaborer une politique de sûreté intégrée à la conception comme base d'un cycle de vie sûr des systèmes d'aviation civile.	Formulation d'une politique de sûreté du cycle de vie des systèmes d'aviation civile.	Moyen	2022-2023
CyAP 4.5	OACI, États membres, et industrie	4.2	8.2	L'OACI organisera des forums internationaux pour examiner les objectifs précis de cybersécurité et de cyberrésilience transorganisationnelles/ transfonctionnelles et le niveau minimum de fonctionnalités essentielles au secteur de l'aviation civile. Les États membres organiseront ces forums aux niveaux national et régional, et l'industrie organisera des forums spécifiques et participera activement aux forums établis par l'OACI et les États membres.	Nombre de forums pour examiner les objectifs.	Élevé	2022-2023
CyAP 4.6	OACI, États membres, et industrie	4.3	8.2	Dresser un inventaire des initiatives actuelles en matière de gestion des cyberrisques dans l'aviation civile (profils de risque, scénarios, gestion de la vulnérabilité et évaluations des risques).	Mise à disposition d'un répertoire des initiatives de gestion des cyberrisques.	Moyen	2023-2024
CyAP 4.7	OACI, États membres, et industrie	4.3	8.3	L'OACI établira une liste de scénarios stratégiques pour les cyberrisques au niveau international. Les États membres et l'industrie contribueront à l'établissement de listes semblables aux niveaux national et organisationnel.	Disponibilité de 10 scénarios de cyberrisques.	Élevé	2023-2024
CyAP 4.8	OACI, États membres, et industrie		8.2	L'OACI définira des profils de risque pour chaque domaine opérationnel. Les États membres et l'industrie contribueront en définissant des profils de risque similaires aux niveaux national et organisationnel.	Disponibilité de profils de risque.	Élevé	2023
CyAP 4.9	OACI		8.2	Élaborer un État du contexte de risque mondial de cybersécurité.	Publication de l'État du contexte de risque mondial de cybersécurité.	Élevé	2023

Résultat prioritaire	**5. RENFORCER LES CAPACITÉS DE PARTAGE D'INFORMATIONS**
Mesures prioritaires	• Mettre en place ou exploiter les plates-formes et mécanismes actuels d'échange d'informations qui sont reconnus, en cohérence avec les dispositions en vigueur de l'OACI, pour permettre de connaître la situation cybernétique et, partant, de prévenir, de détecter précocement et d'atténuer les événements pertinents de cybersécurité. • Veiller à ce que tout cyberincident ou toute vulnérabilité pouvant représenter un risque important pour la sécurité et/ou la sûreté de l'aviation soit signalé à l'autorité compétente.

Mesures

Mesure	**Par**	**Référence dans la Stratégie de cybersécurité**	**Référence dans le Chapitre 9**	**Mesures/tâches spécifiques**	**Indicateurs**	**Niveau de priorité**	**Date de début de la mise en œuvre**
CyAP 5.1	OACI	5.1	9.1 & 9.2	L'OACI définira des orientations pour le partage d'information.	Disponibilité d'un document d'orientation sur le partage d'information.	Élevé	2022-2023
CyAP 5.2	OACI	5.1	9.1	OACI, avec le soutien des États membres et de l'industrie, définira les besoins en matière de partage d'information et de collaboration relatifs à la cybersécurité (notamment en périodes de crises, mais pas uniquement) et les politiques y afférentes.	Établissement d'une liste d'informations potentielles à partager.	Moyen	2022-2024
CyAP 5.3	OACI	5.1	9.1	Élaborer des orientations sur l'utilisation du TLP (*Traffic Light Protocol*) pour déterminer le niveau de distribution/restrictions applicable à la diffusion et au partage plus large de cyberinformations.	Publier des orientations de politique pour l'utilisation du TLP lors de la diffusion et du partage de cyberinformations.	Élevé	2021
CyAP 5.4	OACI, États membres, et industrie	5.2	9.2	Envisager la possibilité de définir des critères pour une divulgation responsable des vulnérabilités en matière de cybersécurité.	Disponibilité et publication de principes devant régir la divulgation responsable des vulnérabilités, si cela est jugé possible.	Élevé	2023
CyAP 5.5	OACI et États membres	5.2	9.4	L'OACI établira et tiendra à jour un réseau de correspondants au niveau international pour les questions de cybersécurité de l'aviation civile dans les États membres et	Création d'un réseau de correspondants cybersécurité de l'aviation civile. Publication du réseau de correspondants de chaque État membre.	Moyen	2024-2025

				l'industrie. Les États membres à coopéreront avec l'OACI en créant ce réseau de correspondant au niveau national.			
Résultat prioritaire	**6. DÉVELOPPER LA GESTION DES INCIDENTS ET LA PLANIFICATION D'URGENCE**						
Mesures prioritaires	• Veiller à établir des plans appropriés et évolutifs qui assurent la continuité des opérations de l'aviation civile en toute sûreté et sécurité en cas de cyberincident. • S'assurer de tirer parti des plans d'urgence actuels en y incluant des dispositions qui permettent d'intervenir face aux incidents de cybersécurité et d'assurer la reprise, et effectuer régulièrement/périodiquement des exercices pour vérifier les capacités à détecter les cyberincidents, à intervenir et à assurer la reprise.						
Mesures							
Mesure	**Par**	**Référence dans la Stratégie de cybersécurité**	**Référence dans le Chapitre 10**	**Mesures/tâches spécifiques**	**Indicateurs**	**Niveau de priorité**	**Date de début de la mise en œuvre**
CyAP 6.1	États membres et industrie	6.1	10.1	Les États membres fixeront des cibles et des niveaux minimums de fonctionnalités essentielles au secteur de l'aviation civile. L'industrie appliquera les cibles fixées.	Publication d'une liste de cibles et de niveaux minimums acceptables de fonctionnalités pour la continuité de l'aviation.	Élevé	2022-2023
CyAP 6.2	OACI et États membres	6.1	10.2	L'OACI élaborera des orientations et des processus permettant d'intégrer les parties prenantes militaires à la planification de la réponse aux incidents de cybersécurité dans l'aviation civile. Les États membres élaboreront des procédures et des accords de coopération entre les autorités de l'aviation civile et de l'aviation militaire.	Élaboration et publication d'orientations concernant les processus et procédures de coopération civilo-militaire dans le cadre de la réponse aux incidents de cybersécurité de l'aviation civile.	Élevé	2022-2023
CyAP 6.3	OACI, États membres, et industrie	6.1.	10.1	L'OACI élaborera des orientations pour les capacités d'intervention face aux cyberincidents de l'aviation civile et les capacités de reprise, y compris les plans d'intervention en cas d'urgence. Les États membres et l'industrie, suivant les orientations de l'OACI, élaboreront ces orientations aux niveaux national et	Publication d'orientations pour les capacités d'intervention face aux cyberincidents de l'aviation civile et les capacités de reprise, y compris les plans d'intervention en cas d'urgence.	Élevé	2022-2023

				organisationnel.			
CyAP 6.4	États membres	6.1.	10.2 and 10.3	Les États membres concevront et mettront en place les capacités et les plans nécessaires pour détecter et analyser les incidents de cybersécurité dans l'aviation civile et pour y répondre au niveau opérationnel.	Enquête visant à suivre le niveau de mise en œuvre.	Élevé	2023-2024
CyAP 6.5	OACI et États membres	6.1.	10.1	Élaborer des processus de coordination de crise de cybersécurité dans l'aviation civile, notamment aux niveaux national et international.	Établissement des processus de définition de la coordination en situation de crise de cybersécurité. Publication des éléments indicatifs.	Moyen	2024-2025
CyAP6.6	États membres et industrie	6.1	10.3	Procéder périodiquement à des exercices réels et sur table.	Partage des enseignements tirés, le cas échéant.	Élevé	2022-2023

Résultat prioritaire	**7. DÉVELOPPER LE RENFORCEMENT DES CAPACITÉS, LA FORMATION ET UNE CULTURE DE LA CYBERSÉCURITÉ**
Mesures prioritaires	• Veiller à ce que le personnel soit adéquatement qualifié en fonction de son rôle, dans le domaine tant de l'aviation que de la cybersécurité. • Accroître la sensibilisation à la cybersécurité, notamment les activités visant à instaurer une cyberhygiène appropriée. • Veiller à ce que le cadre éducatif national comprenne des programmes d'enseignement en bonne et due forme consacrés à la cybersécurité en aviation, afin d'assurer le développement d'un ensemble de connaissances sur la sécurité et la sûreté dans tout le secteur de l'aviation à l'échelle de l'organisation, y compris au niveau de la haute direction. • Encourager l'innovation, ainsi que les activités appropriées de recherche et de développement. • Inclure la cybersécurité dans la stratégie de l'OACI pour la « Prochaine génération de professionnels de l'aviation ».

Mesures

Mesure	**Par**	**Référence dans la Stratégie de cybersécurité**	**Référence dans le Chapitre 11**	**Mesures/tâches spécifiques**	**Indicateurs**	**Niveau de priorité**	**Date de début de la mise en œuvre**
CyAP 7.1	OACI, États membres, et industrie	7.1.	11.1	Définir et promouvoir une culture de la cybersécurité dans l'aviation civile et la sensibilisation à la cybersécurité.	Disponibilité de cours et d'éléments indicatifs concernant la culture de la cybersécurité dans l'aviation civile.	Moyen	2022-2023
CyAP 7.2	États membres, et industrie	7.2.	11.1	Les États membres et l'industrie élaboreront des exigences de formation appropriée et axée sur les rôles en matière	Élaboration d'une formation appropriée et axée sur les rôles dans le domaine de l'aviation et de la cybersécurité.	Élevé	2022-2023

				de cybersécurité dans l'aviation à tous les niveaux de leurs organisations.			
CyAP 7.3	OACI et États membres	7.3.	11.1	L'OACI intégrera la cybersécurité dans la stratégie pour la « Prochaine génération de professionnels de l'aviation » (NGAP). Les États membres intégreront la cybersécurité dans leurs stratégies nationales relatives à la stratégie NGAP.	Intégration de la cybersécurité dans les stratégies NGAP.	Moyen	2022-2023
CyAP 7.4	OACI	7.3.	11.1	L'OACI analysera les moyens permettant de satisfaire aux exigences en matière de compétences fondées sur les rôles dans le domaine de la cybersécurité	Intégration de la formation basée sur les rôles en matière de cybersécurité dans les Doc 7192 et 9868 de l'OACI, si cela est jugé possible.	Élevé	2023-2025
CyAP 7.5	OACI, États membres, et industrie	7.3.	11.1	Développement d'activités de renforcement des capacités.	Disponibilité de programmes de formation sur la cybersécurité dans l'aviation.	Élevé	En cours

— FIN —