OACI

Objectif stratégique de sûreté et facilitation

Stratégie de cybersécurité de l'aviation

Octobre 2019

Approuvé par la Secrétaire générale et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

OACI

Objectif stratégique de sûreté et facilitation

Stratégie de cybersécurité de l'aviation

Octobre 2019

Approuvé par la Secrétaire générale et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

Publié séparément en français, en anglais, en arabe, en chinois, en espagnol et en russe par l'ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE
999, boul. Robert-Bourassa, Montréal (Québec) H3C 5H7 Canada

Les formalités de commande et la liste complète des distributeurs officiels et des librairies dépositaires sont affichées sur le site web de l'OACI (www.icao.int).

Stratégie de cybersécurité de l'aviation
https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

STRATÉGIE DE CYBERSÉCURITÉ DE L'AVIATION

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

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

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

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

Cette vision peut être réalisée comme suit :

- reconnaissance par les États membres des obligations que leur impose la *Convention relative à l'aviation civile internationale* (Convention de Chicago) d'assurer la sécurité, la sûreté et la continuité de l'aviation civile, en tenant compte de cybersécurité ;

- coordination de la cybersécurité de l'aviation entre les autorités des États afin d'assurer l'efficacité et l'efficience de la gestion mondiale des risques de cybersécurité ;

- engagement de toutes les parties prenantes de l'aviation civile à développer plus avant la cyberrésilience, en assurant la protection contre les cyberattaques qui peuvent influer sur la sécurité, la sûreté et la continuité du système de transport aérien.

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

1. Coopération internationale

2. Gouvernance

3. Législation et règlements efficaces

4. Politique de cybersécurité

5. Partage de l'information

6. Gestion des incidents et planification d'urgence

7. Renforcement des capacités, formation et culture de cybersécurité

1. COOPÉRATION INTERNATIONALE

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

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

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

2. GOUVERNANCE

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

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

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

3. LÉGISLATION ET RÈGLEMENTS EFFICACES

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

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

3.3 Il faudrait analyser les instruments juridiques internationaux pertinents pour y chercher les dispositions clés de droit aérien qu'elles contiennent ou qui y font défaut sur la prévention des cyberincidents, les poursuites et les réactions opportunes en la matière, pour établir la base d'une mise en œuvre systématique et cohérente de la législation et des règlements de cybersécurité dans tout le secteur de l'aviation mondiale. Entre-temps, les États

sont encouragés à ratifier les instruments de l'OACI, dont 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).

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

4. POLITIQUE DE CYBERSÉCURITÉ

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

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

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

5. PARTAGE DE L'INFORMATION

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

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

6. GESTION DES INCIDENTS ET PLANIFICATION D'URGENCE

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

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

7. RENFORCEMENT DES CAPACITÉS, FORMATION ET CULTURE DE CYBERSÉCURITÉ

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

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

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

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

— FIN —