Orientations en matière de politique de cybersécurité

Publié sous l'autorité du Secrétaire général

Janvier 2022

Organisation de l'aviation civile internationale

1. Introduction

Les présentes orientations cadrent avec la Stratégie[1] pour la cybersécurité de l'aviation de l'OACI et le Plan d'action[2] pour la cybersécurité, dont la mesure CyAP0.1 recommande que l'Organisation de l'aviation civile internationale (OACI) élabore un modèle de politique de cybersécurité auquel les États membres et l'industrie pourront se référer pour élaborer leurs propres politiques nationales/internes.

Le modèle de politique de cybersécurité figure en appendice A des présentes orientations.

2. Portée

Le modèle de politique de cybersécurité décrit à l'appendice A du présent document traite de la protection et de la résilience des infrastructures essentielles de l'aviation civile internationale contre les cybermenaces, et de l'exigence de collaboration multilatérale tant à l'intérieur du secteur de l'aviation civile qu'avec les autorités extérieures comme celles de l'armée, de la cybersécurité et de la sûreté nationale.

3. Objectifs

Le modèle de politique de cybersécurité est destiné à servir de guide qui aidera les États et l'industrie à concentrer les ressources et les actions sur l'adoption d'une approche systémique de la cybersécurité dans l'aviation civile, y compris les systèmes actuels et anciens. L'objectif ultime est que les États et les parties prenantes soient en mesure de mettre au point une approche systémique qui permette à l'aviation civile d'être protégée contre les cybermenaces, de répondre aux cyberincidents et de s'en remettre en temps voulu, et donc de résister à de nouvelles menaces sans subir de perturbations notables.

Les principaux résultats attendus de la mise en œuvre d'une politique de cybersécurité sont les suivants :

3.1 Veiller à la protection de l'aviation civile contre les cybermenaces

La protection de l'aviation civile contre les cyberattaques est assurée par la mise en œuvre des normes et pratiques recommandées, des procédures et des éléments indicatifs en matière de cybersécurité de l'OACI. Elle comprend la mise en œuvre de solides pratiques de gestion des risques, la détermination des infrastructures essentielles et la mise en œuvre d'une approche globale à plusieurs niveaux de la cybersécurité. Cette approche devrait garantir qu'une attaque réussie contre un niveau ne compromet pas les autres niveaux du système et/ou ne conduit pas à une perte de sûreté, de sécurité ou de continuité des fonctions cruciales. Le système devrait aussi adopter une approche d'amélioration continue pour faire en sorte que les améliorations nécessaires aux évolutions techniques ou procédurales prévues soient coordonnées, mises en œuvre et maintenues à jour.

3.2 Assurer la cyberrésilience de l'aviation civile

Le système de l'aviation civile, pour être cyberrésilient, doit pouvoir, en cas d'attaque, maintenir ses fonctionnalités critiques, c'est-à-dire assurer la sécurité et la sûreté des vols avec un minimum de perturbations, voire sans aucune. Le système devrait aussi comprendre des mécanismes appropriés de coopération et d'échange d'informations nécessaires entre les parties prenantes de l'aviation, tels que les autorités publiques, l'industrie et, le cas échéant, les services répressifs civils et les autorités militaires.

---

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx
[2] Lettre 2020/114 de l'OACI.

3.3 **Assurer l'autorenforcement de l'aviation en adoptant une approche de « sûreté intégrée »**

L'adoption d'une approche de sûreté intégrée dans l'aviation civile nécessite, dès la conception d'un système, la prise en compte des objectifs de sûreté à atteindre lors du processus de conception du système, ainsi que des objectifs classiques d'exploitation et de sécurité. Le fait d'assurer la sûreté des éléments cruciaux et des processus « intégrés » change le paradigme de la sûreté, qui cesse d'être réactif pour devenir proactif, et favorise le développement d'un système d'aviation civile autoprotégé, lui permettant ainsi d'évoluer et de renforcer la sûreté et la résilience.

3.4 **Assurer la coordination de la cybersécurité de l'aviation dans le secteur de l'aviation civile et avec les parties prenantes non aéronautiques concernées**

Afin de garantir une approche cohérente et complémentaire de la cybersécurité de l'aviation dans toutes les disciplines de l'aviation, le système de l'aviation civile doit assurer la gestion globale des cyberrisques pour l'aviation civile en coordonnant les aspects relatifs à la sécurité et à la sûreté de la cybersécurité de l'aviation. De plus, la coordination de la cybersécurité de l'aviation devrait s'étendre au-delà de l'aviation civile à d'autres entités concernées comme les autorités nationales/régionales/internationales chargées de la cybersécurité, les services répressifs, l'armée, etc.

4. **Éléments de la politique de cybersécurité**

La présente section fournit des orientations sur les éléments inclus dans le modèle de politique de cybersécurité qui figure en appendice A. Il est donc recommandé de la lire conjointement avec le modèle de politique de cybersécurité.

4.1 **Gouvernance et organisation**

4.1.1 Les États devraient désigner une autorité compétente chargée de la cybersécurité de l'aviation (AA/Cyber), qui est investie d'un mandat et d'une responsabilité globaux en matière de cybersécurité et de cyberrésilience de l'aviation.

4.1.2 Il n'existe pas de formule universelle pour déterminer la place de l'AA/Cyber dans les structures organisationnelles de l'aviation civile de chaque État. La décision sera influencée par plusieurs considérations liées à la structure nationale de l'aviation et aux structures non aéronautiques pertinentes en termes de composantes et de mandats. Il importe toutefois que l'AA/Cyber dispose de ressources et de pouvoirs lui permettant de s'acquitter de son mandat, en ce qui concerne notamment les négociations et la coordination avec les parties prenantes non aéronautiques concernées.

4.1.3 Globalement, l'AA/Cyber désignée devrait :

- déterminer, en coordination avec l'autorité nationale compétente chargée de la cybersécurité, les rôles et les responsabilités incombant à chaque autorité ;
- piloter l'élaboration des règlements régissant la cybersécurité de l'aviation ;
- définir clairement les rôles et les responsabilités des différents domaines de l'aviation civile au sein de l'autorité nationale compétente chargée de l'aviation civile ;
- coordonner la définition des rôles et des responsabilités des entités de l'aviation civile placées sous la supervision de l'autorité nationale compétente en matière d'aviation civile dans le cadre des programmes nationaux de sécurité et de sûreté ;
- définir les éléments de la culture de la cybersécurité de l'aviation civile et suivre sa mise en œuvre ;
- définir les règlements, les processus, les exigences et les rôles en matière de gestion des crises de cybersécurité, y compris les exigences et la fréquence des tests ;

- coordonner les questions transversales de cybersécurité de l'aviation avec les parties prenantes non aéronautiques concernées qui interviennent dans la cybersécurité de l'aviation, comme l'échange des informations et les enquêtes sur les incidents.

4.2 Gestion des risques

4.2.1 Pour assurer la gestion des risques de cybersécurité, il conviendrait de s'appuyer sur les cadres de gestion des risques de sécurité et de sûreté de l'aviation en vue de procéder à une évaluation intégrée et précise des menaces et des risques de cybersécurité, et de garantir l'élaboration et la mise en œuvre de mesures d'atténuation efficaces qui tiennent compte des exigences de sécurité et des conséquences des mesures d'atténuation sur la sécurité et la continuité de l'aviation civile.

4.2.2 La propriété de toutes les données et de tous les systèmes devrait être indiquée à tout moment. L'indication et la tenue à jour de la propriété permettent d'établir les responsabilités et d'appuyer la gestion des données et des systèmes, de leur adoption à leur suppression. À ce titre, les propriétaires devraient établir des règles et des processus concernant notamment l'emplacement physique des données et des systèmes, les droits d'accès, les droits de gestion et les exigences de sécurité en fonction de la classification des données et des systèmes. À terme, cette démarche favorisera l'utilisation adéquate des données et des systèmes par les bonnes personnes, appuiera la définition et la mise en œuvre de normes de contrôle de la qualité, et permettra de résoudre les problèmes et les conflits.

4.3 Sécurité des systèmes critiques

4.3.1 Il conviendrait d'appliquer les principes de la défense en profondeur pour protéger les systèmes critiques. La défense en profondeur intègre les capacités humaines, technologiques et opérationnelles afin d'établir des barrières variables à l'échelle de niveaux et de missions multiples de l'organisation[3]. Il s'agit d'une approche de la cybersécurité dans laquelle une série de mécanismes défensifs sont superposés en vue de protéger les systèmes, les données et les informations essentiels. Cette approche comportant plusieurs niveaux et des redondances intentionnelles accroît la sûreté d'un système dans son ensemble et vise un grand nombre de vecteurs d'attaque différents[4].

4.3.2 L'AA/Cyber devrait veiller à ce que les entités de l'aviation civile inventorient et protègent convenablement leurs systèmes critiques, et renforcent leur capacité à détecter les cyberincidents, à y répondre et à s'en remettre.

4.4 Sûreté des données

4.4.1 La sauvegarde périodique autonome et sécurisée des données critiques devrait être considérée comme un moyen d'appuyer la disponibilité et l'intégrité des informations. Il est toutefois primordial d'élaborer une politique de sauvegarde solide, en fonction des évaluations des risques, car une sauvegarde autonome effectuée alors qu'une cyberattaque est en cours serait déjà compromise et ne pourrait donc pas servir à rétablir l'accès aux informations essentielles.

4.4.2 Le chiffrement des données sensibles devrait être considéré comme un moyen d'appuyer la confidentialité des informations. Il importe cependant de définir, en fonction des évaluations des risques, des processus d'utilisation du chiffrement qui permettent d'établir un juste équilibre entre le niveau de

[3] Publication spéciale 800-53 Rev.5 du NIST : https://doi.org/10.6028/NIST.SP.800-53r5

[4] La défense en profondeur est généralement appelée « approche du château », car elle reproduit la structure de défense stratifiée d'un château médiéval dans lequel, pour pénétrer, les assaillants doivent franchir des douves, un pont-levis, un rempart, des tours, etc.

confidentialité et les exigences en matière de performance opérationnelle, notamment dans le cas des données « réelles » nécessaires à la sécurité des vols, tout en tenant compte des ressources requises pour gérer les données.

4.4.3 Il conviendrait d'établir des processus pour assurer la continuité des fonctions essentielles en cas de perte de disponibilité et/ou d'intégrité des données.

4.5 **Sûreté de la chaîne logistique**

4.5.1 Les entités devraient veiller à ce que les logiciels et le matériel utilisés dans les fonctions essentielles de l'aviation soient conformes aux exigences de cybersécurité tout au long du cycle de vie des systèmes aéronautiques, depuis la conception et le développement jusqu'à l'élimination sûre et sécurisée, en passant par l'exploitation et la maintenance.

4.5.2 Les accords de niveau de service peuvent être exploités pour inclure des exigences en matière de cybersécurité applicables au matériel et aux logiciels, ainsi qu'aux actualisations, aux mises à niveau et à l'application de correctifs en cas de découverte de vulnérabilités.

4.6 **Sûreté physique**

4.6.1 Les exemples de contrôles de sûreté physique pertinents pour la cybersécurité de l'aviation comprennent, entre autres, la définition de politiques de gestion et de contrôle de l'accès physique, la vérification des antécédents du personnel disposant de droits administratifs sur les systèmes/les bases de données ou ayant accès à des données sensibles et/ou critiques, des recommandations pour la séparation des tâches et/ou la rotation du personnel ayant accès aux systèmes critiques ou pouvant les modifier, etc.

4.7 **Sécurité des informations, des communications et des technologies (ICT)**

4.7.1 Les exemples de contrôles de sécurité des ICT pertinents pour la cybersécurité de l'aviation comprennent, entre autres, les politiques de contrôle d'accès et l'application des principes du moindre privilège, les pare-feu logiciels/matériels et la sûreté des réseaux, la cryptographie, les politiques organisationnelles en matière de mots de passe, la protection des points terminaux, la surveillance des réseaux et la détection des anomalies, la séparation des réseaux, la gestion des dispositifs, etc.

4.8 **Gestion des incidents et continuité des fonctions critiques**

4.8.1 L'AA/Cyber devrait définir des règlements, des processus, des exigences et des rôles pour la gestion des cyberincidents, la récupération et la continuité des systèmes critiques.

4.8.2 Les plans actuels de gestion de crise et de continuité des activités devraient être mis à profit pour inclure la réponse aux cyberincidents et la récupération après ceux-ci.

4.8.3 Il conviendrait de procéder périodiquement à des tests des plans d'intervention d'urgence et de continuité des activités dans le but d'améliorer ces plans et les capacités des intervenants. Les tests devraient englober toutes les parties prenantes concernées et comprendre une combinaison d'exercices sur table (TTX) et d'essais en situation réelle.

4.9 **Culture de cybersécurité**

4.9.1 Il conviendrait de mettre en œuvre la culture de la cybersécurité dans l'ensemble des entités aéronautiques.

4.9.2 La culture de la cybersécurité devrait être approuvée par les dirigeants de l'organisation et comporter un programme à mettre en œuvre par tout le personnel.

4.9.3 Le programme devrait comprendre une éducation récurrente à la cybersécurité (y compris les principes relatifs aux pratiques de cyberhygiène), une sensibilisation aux dernières menaces, la formation et la réalisation de tests (à la fois dans le cadre de la formation et de la simulation d'attaques en direct) pour évaluer le niveau de cyberconscience/cyberhygiène.

4.9.4 La culture de la cybersécurité devrait comprendre des éléments issus des cultures de la sûreté et de la sécurité, par exemple l'autodéclaration, le signalement de comportements/pratiques suspects, la culture de la justice, etc.

– – – – – – – – – – – –

Appendice A

Modèle de politique de cybersécurité

1. Introduction

1.1 La présente politique de cybersécurité constitue le cadre d'un développement et d'une mise en œuvre plus poussés de la cybersécurité de l'aviation. Elle est publiée, diffusée auprès des parties prenantes concernées et révisée périodiquement.

1.2 D'autres éléments indicatifs sont élaborés pour appuyer la mise en œuvre de la présente politique de cybersécurité.

2. Portée

2.1 La cybersécurité de l'aviation concerne la sûreté et la résilience du système de l'aviation civile, et appuie la collaboration avec les entités et autorités non aéronautiques concernées, notamment l'autorité nationale de cybersécurité, la sûreté nationale, les forces de l'ordre et l'armée, selon le cas.

2.2 La cybersécurité de l'aviation est coordonnée au niveau national avec les autorités chargées de la sécurité de l'aviation, de la sûreté de l'aviation, de la protection des infrastructures critiques et de la cyberdéfense, et avec les autorités militaires.

2.3 La cybersécurité de l'aviation est coordonnée au niveau international avec les autorités étrangères compétentes équivalentes désignées pour la cybersécurité de l'aviation.

3. Objectifs

3.1 Les objectifs généraux de la présente politique de cybersécurité de l'aviation sont de garantir la sureté, la résilience et l'autorenforcement du système de l'aviation civile face aux cybermenaces et aux cyberrisques, et d'assurer la coordination de la cybersécurité de l'aviation avec les autorités et entités nationales concernées.

4. Gouvernance et organisation

4.1 Conformément à [référence du règlement/de la loi concernant la désignation], [nom de l'entité] est l'autorité compétente chargée de la cybersécurité de l'aviation (AA/Cyber) et dispose d'un mandat général couvrant la cybersécurité et la cyberrésilience de l'aviation.

4.2 L'AA/Cyber doit :

- dialoguer avec l'autorité nationale compétente chargée de la cybersécurité en vue de définir les rôles et les responsabilités en matière de cybersécurité de l'aviation civile qui incombent à chaque autorité ;
- coordonner l'élaboration des règlements de cybersécurité de l'aviation et y contribuer ;
- définir, coordonner et fournir l'appui dont ont besoin les autorités compétentes chargées de la sécurité et de la sûreté de l'aviation pour inclure les exigences de cybersécurité de l'aviation, y compris les éléments de supervision et de contrôle de la qualité, dans le Programme national de sécurité de l'État (PNS) et le Programme national de sûreté de l'aviation civile (PNSAC) ;
- définir, appuyer et suivre la mise en œuvre du programme de culture de la cybersécurité par toutes les parties prenantes de l'aviation civile ;

- définir les règlements, les processus, les exigences et les rôles relatifs à la gestion des crises de cybersécurité ;
- coordonner les questions transversales de cybersécurité de l'aviation avec les parties prenantes non aéronautiques pertinentes qui interviennent dans la cybersécurité de l'aviation.

5. Gestion des risques

5.1 La cybersécurité doit être fondée sur le renseignement, axée sur les menaces et gérée en fonction des risques.

5.2 La gestion des risques doit faire partie intégrante du cycle de vie global des systèmes.

5.3 Toutes les données et tous les systèmes doivent avoir un propriétaire identifié à tout moment.

6. Sûreté des systèmes critiques

6.1 Les fonctions, systèmes et infrastructures critiques doivent être déterminés dans le cadre des processus de gestion des risques.

6.2 L'approche de sûreté intégrée, conjuguée aux principes de défense en profondeur, doit être appliquée pour protéger les systèmes critiques.

6.3 La redondance des systèmes critiques doit être considérée comme un moyen de renforcer la sûreté des systèmes.

7. Sûreté des données

7.1 Les données et les informations doivent être protégées pendant leur stockage et leur transmission, en fonction de leur profil de sensibilité.

8. Sûreté de la chaîne logistique

8.1 La gestion de bout en bout de la chaîne d'approvisionnement en logiciels/matériel doit faire partie de la gestion de la cybersécurité de l'aviation.

8.2 Les logiciels et le matériel utilisés dans les fonctions aéronautiques critiques doivent être conformes aux exigences de cybersécurité tout au long du cycle de vie des systèmes de l'aviation.

9. Sûreté physique

9.1 La sûreté physique (y compris la sûreté du personnel) doit être prise en compte dans la gestion de la cybersécurité de l'aviation.

9.2 La sûreté physique doit permettre de protéger les personnes, les infrastructures, les installations, les équipements, le matériel et les documents contre les actes d'intervention illicite et de protéger les systèmes aéronautiques critiques contre tout accès physique non autorisé.

9.3 La sûreté physique doit contribuer à la gestion des risques en permettant d'identifier les acteurs de la menace et/ou de déterminer la probabilité d'attaques contre les infrastructures critiques de l'aviation civile.

10. **Sécurité des informations, des communications et des technologies (ICT)**

10.1 La sécurité des ICT doit être prise en compte dans la gestion de la cybersécurité de l'aviation.

10.2 La sécurité des ICT doit permettre de définir et de mettre en œuvre des mesures de sûreté logique et de contribuer aux processus de gestion des cyberincidents, de récupération et de continuité des opérations.

10.3 La sécurité des ICT contribue à la gestion des risques en déterminant les vulnérabilités et les vecteurs d'attaque et en suivant l'évolution du paysage des menaces pour la cybersécurité de l'aviation.

11. **Gestion des incidents et continuité des fonctions critiques**

11.1 La sûreté des opérations et la continuité des fonctions critiques doivent être les principaux moteurs des processus de gestion des incidents.

11.2 Les tests des plans de gestion de crise et de reprise font partie intégrante de la gestion des incidents.

12. **Culture de la cybersécurité**

12.1 Un plan d'éducation, de sensibilisation, de formation et d'exercices doit faire partie intégrante de la gestion de la cybersécurité de l'aviation.

12.2 La culture de la cybersécurité doit être entièrement coordonnée avec les cultures de sécurité et de sûreté actuelles.

12.3 La culture de la cybersécurité doit être appuyée par des pratiques solides d'échange d'information internes et, dans la mesure du possible, externes.

— FIN —