OACI

Doc 10213 – Diffusion non restreinte

Considérations relatives aux cyberrisques dans le monde

Première édition, 2025

Approuvé par le Secrétaire général et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

OACI

Doc 10213 – Diffusion non restreinte

Considérations relatives aux cyberrisques dans le monde

Première édition, 2025

Approuvé par le Secrétaire général 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).

Première édition, 2025

Doc 10213, *Considérations relatives aux cyberrisques dans le monde*

Commande n° : 10213-U
ISBN 978-92-9275-950-6

AMENDEMENTS

La parution des amendements est annoncée dans les suppléments au *Catalogue des produits et services*. Le catalogue et ses suppléments sont disponibles sur le site web de l'Organisation : www.icao.int. Le tableau ci-dessous est destiné à rappeler les divers amendements.

RELEVÉ DES AMENDEMENTS ET DES RECTIFICATIFS

AMENDEMENTS		
Nº	Date	Inséré par

RECTIFICATIFS			
Nº	Date	Langue	Inséré par

Les *Considérations relatives aux cyberrisques dans le monde* (Doc 10213 – Diffusion restreinte) sont soumises à restriction, car elles sont destinées à l'utilisation limitée des administrations, du secteur et d'autres parties prenantes de l'aviation concernées par la cybersécurité aux fins d'évaluation des risques. La présente version du Doc 10213 consiste en un résumé non soumis à restriction, qui peut donc être publié.

AVANT-PROPOS

Les vingt dernières années ont vu rapidement évoluer l'utilisation de l'information et des nouvelles technologies dans le secteur de l'aviation civile à l'appui des objectifs d'automatisation, d'interconnectivité et d'interopérabilité. Cette tendance s'est accélérée ces derniers temps, en particulier dans les domaines opérationnels, afin de tirer avantage des dernières évolutions technologiques, comme l'apprentissage automatique et l'analyse de mégadonnées. Cette numérisation permettra d'hâter la mise en place de nouveaux concepts opérationnels au sol et dans les airs et à l'intégration de nouveaux acteurs, tels que les systèmes d'aéronef non habité (UAS), dans le système de transport aérien. L'objectif ultime de ces changements est de soutenir la croissance du secteur de l'aviation civile tout en garantissant sa sécurité, sa sûreté, son efficacité, sa capacité et sa durabilité.

Cela étant, cette tendance a étendu le panorama des cybermenaces aux systèmes opérationnels et à l'information, ce qui peut avoir des conséquences négatives sur la sécurité, la sûreté, la capacité et/ou l'efficacité de l'aviation civile. Le secteur aérien s'est ainsi trouvé obligé de faire face aux cybermenaces et aux cyberrisques qui pèsent sur l'aviation civile au-delà du traditionnel cadre de sécurité des technologies de l'information et des technologies opérationnelles (TI/TO), de façon à concilier la gestion des cyberrisques dans l'aviation avec les processus de gestion des risques touchant l'aviation civile dans toutes ses disciplines. Il s'agit ainsi d'étayer la protection et la résilience du système de transport aérien par des cadres de gestion des risques efficaces et solides.

Le document *Considérations relatives aux cyberrisques dans le monde* a été élaboré par l'Organisation de l'aviation civile internationale (OACI) pour aider les États membres et les parties prenantes à intégrer la gestion des cyberrisques dans leurs processus de gestion des risques touchant l'aviation. Il présente aussi un panorama de haut niveau des cybermenaces dans le monde pour souligner combien la lutte contre les cybermenaces et les cyberrisques est fondamentale pour l'aviation civile, à l'appui d'un secteur résilient et protégé.

Ce document apporte une aide aux États et aux parties prenantes pour remplir leurs obligations en matière d'évaluation des risques, qui sont définies dans les Annexes à la Convention relative à l'aviation civile internationale (Convention de Chicago), en particulier leurs obligations en vertu de la norme 4.9.1 de l'Annexe 17 – *Sûreté de l'aviation*. Il soutient aussi la mise en œuvre de la Stratégie de l'OACI pour la cybersécurité de l'aviation[1] et son plan d'action connexe[2].

Les informations qui figurent dans le présent document sont conformes aux principes généraux des orientations de l'OACI sur les processus de gestion et d'évaluation des risques pour la sûreté et la sécurité de l'aviation, tels qu'énoncés dans l'*État du contexte de risque mondial de sûreté de l'aviation civile* (Doc 10108 – Diffusion restreinte), le *Manuel de sûreté de l'aviation* (Doc 8973 – Diffusion restreinte) et le *Manuel de gestion de la sécurité* (Doc 9859).

Le présent document se compose également d'appendices, qui recensent des exemples d'application de la méthode de gestion des cyberrisques dans les évaluations des risques pour la sécurité et la sûreté de l'aviation. Les appendices comprennent aussi des orientations sur la catégorisation des cybermenaces, conçues pour aider les États et les parties prenantes à repérer les interdépendances et les liens entre les différentes disciplines de l'aviation. L'objectif est ici de soutenir la mise au point et la tenue à jour d'un cadre solide de gestion des risques dans l'aviation civile.

Nous tenons à remercier les experts du Groupe d'experts de la cybersécurité et de son groupe de travail sur la menace et les risques en matière de cybersécurité pour le temps précieux et les connaissances qu'ils ont consacrés à l'élaboration du présent document.

1. Voir https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx
2. Voir https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

TABLE DES MATIÈRES

ABRÉVIATIONS ET SIGLES

ANSP	Fournisseur de services de navigation aérienne
APT	Menace persistante avancée
ATC	Contrôle de la circulation aérienne
AVSEC	Sûreté de l'aviation
CPDLC	Communications contrôleur-pilote par liaison de données
CRC	Contrôle de redondance cyclique
DDoS	Déni de service distribué
DPI	Droit de propriété intellectuelle
EATM-CERT	Équipe d'intervention informatique d'urgence pour la gestion du trafic aérien européen
EFB	Sacoche de vol électronique
FTA	Analyse de l'arborescence des pannes
GNSS	Système mondial de navigation par satellite
HVAC	Chauffage, ventilation et climatisation
IP	Protocole Internet
MET	Météorologique
NEASCOG	Groupe de coordination OTAN-EUROCONTROL pour la sûreté de la gestion du trafic aérien (ATM)
PBIED	Engin explosif improvisé porté par une personne
PII	Information permettant l'identification personnelle
TI/TO	Technologie de l'information/Technologie opérationnelle
UAS	Système d'aéronef non habité

Chapitre 1

DÉFINITIONS

Confidentialité. Propriété d'un actif qui n'est pas mis à disposition ni divulgué à une personne, un utilisateur, un programme, un processus, un système ou un appareil non autorisé.

Contrôle d'accès. Mesures visant à garantir que seul un accès autorisé est donné aux biens physiques et aux cyberactifs.

Cyberactifs. Éléments numériques et physiques qui ont une valeur en termes d'activité, d'exploitation, de sécurité et de sûreté de l'aviation, d'efficacité et/ou de capacité, tels que les systèmes, les informations, les données, les réseaux, les appareils, les logiciels, le matériel informatique, les processus, les microprogrammes, le personnel pertinent/certifié et d'autres ressources électroniques.

Cyberattaque. Utilisation délibérée de moyens électroniques pour interrompre, modifier, détruire ou obtenir un accès non autorisé à des cyberactifs.

Cyberatténuation. Contrôles de sûreté qui visent à réduire le cyberrisque associé à une cybermenace ou à une vulnérabilité spécifique, en tenant compte de son incidence sur la sécurité et la sûreté de l'aviation, l'efficacité et/ou la capacité.

Cyberévénement. Toute occurrence observable dans un réseau ou un système.

Cyberincident. Un ou plusieurs cyberévénements qui ont une incidence négative sur la sécurité et la sûreté de l'aviation, l'efficacité et/ou la capacité.

Cybermenace. Tout cyberévénement potentiel qui pourrait avoir une incidence négative sur la sécurité et la sûreté de l'aviation, l'efficacité et/ou la capacité.

Cyberrésilience. Capacité d'un cyberactif à maintenir des fonctions essentielles dans des conditions défavorables ou sous la pression, et à s'en remettre.

Cyberrisque. Possibilité qu'un cyberévénement débouche sur un résultat indésirable.

Cybersécurité de l'aviation. Ensemble de technologies, de contrôles et de mesures, de processus, de procédures et de pratiques conçus pour assurer la confidentialité, l'intégrité, la disponibilité et la protection et la résilience globales des cyberactifs contre les attaques, les dommages, la destruction, les perturbations, les accès non autorisés et/ou l'exploitation.

Disponibilité. Propriété de ce qui est accessible et utilisable à la demande par une personne, un utilisateur, un programme, un processus, un système ou un appareil autorisé.

Entité (ou acteur) à l'origine de la menace. Entité partiellement ou entièrement responsable d'un incident, qui a une incidence – ou est susceptible d'en avoir – sur une organisation ou un système.

Évaluation des cyberrisques. Processus continu de repérage, d'analyse et d'évaluation des cyberrisques.

Fiabilité. Propriété selon laquelle un actif remplira, au niveau attendu, une fonction requise dans des conditions données, sans défaillance, pendant une période déterminée.

Gestion des cyberrisques. Processus continu de repérage, d'atténuation, de traitement et de surveillance des cybermenaces et des cyberrisques, sur la base d'une évaluation des risques.

Gravité. Indication qualitative de l'ampleur de l'effet négatif d'une condition de menace.

Infrastructure critique de l'aviation. Actifs si essentiels que toute défaillance, corruption ou destruction de ces derniers aurait une incidence handicapante sur la sécurité, la sûreté, l'efficacité et/ou la capacité de l'aviation.

Intégrité. Propriété de l'exactitude et de l'exhaustivité d'un actif, qui confirme ce que l'actif prétend être.

Matrice des cyberrisques. Outil destiné à hiérarchiser et mettre en évidence les composants des risques (probabilité, menace, incidences/conséquences et vulnérabilité), les atténuations des risques et, en dernière analyse, les risques résiduels.

Perturbation. Un cyberévénement, anticipé ou non, qui amène à faire entorse aux opérations normales, sans planification.

Vecteur d'attaque. Moyen d'accès utilisé par un pirate informatique pour lancer une attaque.

Chapitre 2

MÉTHODE VISANT À INTÉGRER LA GESTION DES CYBERRISQUES AUX CADRES DE GESTION DES RISQUES EN AVIATION

Note 1.— Dans le présent chapitre, les fonctions aéronautiques désignent les fonctions que l'on retrouve dans la ou les disciplines de l'aviation pour lesquelles la gestion des cyberrisques est intégrée aux processus de gestion des risques. Il s'agit notamment de la sécurité de l'aviation, de la sûreté de l'aviation et de l'efficacité et/ou de la capacité de la navigation aérienne. Dans le même contexte, les fonctions critiques de l'aviation sont des fonctions jugées essentielles pour la ou les disciplines de l'aviation concernées.

Note 2.— Dans le présent chapitre, les professionnels de la gestion des risques pour l'aviation sont des professionnels de la sécurité de l'aviation, de la sûreté de l'aviation, de l'efficacité et/ou de la capacité de la navigation aérienne. Par ailleurs, les processus de gestion des risques pour l'aviation désignent les processus de gestion des risques de la ou des disciplines de l'aviation concernées.

2.1 OBJECTIFS

2.1.1 Le présent chapitre vient à l'appui de l'éventail de processus de gestion des risques mis en place par des États et des parties prenantes, allant du recensement des risques à leur traitement et analyse, en recommandant une méthode générique d'intégration de l'évaluation et de la gestion des cyberrisques dans les cadres existants de gestion des risques pour la sécurité et la sûreté de l'aviation, et pour l'efficacité et la capacité de la navigation aérienne.

Note 1.— Bien que la méthode concerne l'intégration de la gestion des cyberrisques dans les évaluations de la sécurité, de la sûreté, et de l'efficacité et de la capacité de la navigation aérienne, elle peut être personnalisée en vue de s'appliquer à toute autre discipline de l'aviation civile (comme la gestion des risques commerciaux).

Note 2.— Avant d'appliquer la méthode décrite dans le présent chapitre, les États et les parties prenantes souhaiteront peut-être examiner les domaines dans lesquels les méthodes d'évaluation des risques existantes sont généralement reconnues par les autorités compétentes comme des moyens acceptables de se conformer à leurs exigences réglementaires spécifiques en matière d'aviation, telles que les évaluations des risques liés à la certification des aéronefs.

2.1.2 Le présent chapitre s'adresse aux professionnels de la sécurité et de la sûreté de l'aviation, de la navigation aérienne et de la gestion des cyberrisques qui devraient travailler en collaboration pour intégrer la gestion des cyberrisques à leurs cadres respectifs de gestion des risques pour l'aviation, et ce, dans l'ensemble des disciplines de l'aviation civile.

2.2 APERÇU

2.2.1 La méthode exposée dans le présent document se fonde sur les concepts généraux d'un cycle de gestion des risques efficace qui sont illustrés dans la figure 1.

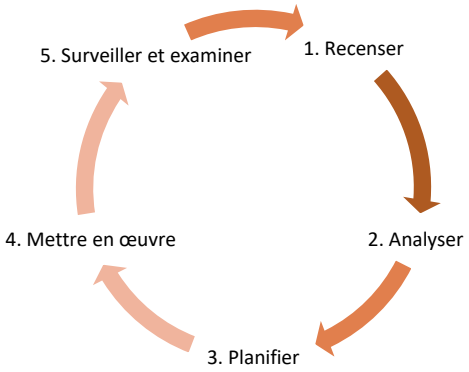


Figure 1. Cycle de gestion des risques

2.2.2 La méthode se fonde sur des éléments indicatifs existants de l'OACI en matière d'évaluation des risques, à savoir le *Manuel de gestion de la sécurité* (Doc 9859) et l'*État du contexte de risque mondial de sûreté de l'aviation civile* (Doc 10108 – Diffusion restreinte). Elle tient compte des travaux de différents groupes d'experts de l'OACI, ainsi que de contributions du Groupe de coordination OTAN-EUROCONTROL pour la sûreté de la gestion du trafic aérien (ATM) (NEASCOG), et s'aligne également sur les normes internationales en matière de gestion des cyberrisques (ISO/IEC 27001:2022[3], ISO 31000:2018[4], EUROCAE/RTCA ED201A/DO-391[5] et NIST SP 800-30 Rev.1[6]).

2.2.3 L'application de la méthode aux évaluations existantes des risques pour des fonctions critiques de l'aviation permet d'obtenir les résultats suivants :

- une évaluation actualisée des risques pour la sécurité de l'aviation qui prenne en compte l'évaluation pertinente des cyberrisques ;
- une évaluation actualisée des risques pour la sûreté de l'aviation qui prenne en compte l'évaluation pertinente des cyberrisques ;
- une évaluation actualisée des risques pour l'efficacité de la navigation aérienne qui prenne en compte l'évaluation pertinente des cyberrisques ; et/ou
- une évaluation actualisée des risques pour la capacité de la navigation aérienne qui prenne en compte l'évaluation pertinente des cyberrisques ;

2.2.4 Avant d'appliquer la méthode, il est essentiel que les professionnels de l'aviation déterminent les fonctions critiques de l'aviation dans la discipline évaluée. Cela peut se faire au moyen notamment de consultations ou d'enquêtes, en tenant compte des exigences réglementaires et juridiques applicables à l'aviation ainsi qu'à l'infrastructure critique nationale.

Note.— La détermination des fonctions critiques de l'aviation et des données, des informations et des systèmes qui les sous-tendent, combinée à l'application de la méthode, contribue aux efforts menés par les États pour s'acquitter de leurs obligations en vertu de la norme 4.9.1 de l'Annexe 17 – Sûreté de l'aviation[7].

3. Voir https://www.iso.org/fr/standard/27001
4. Voir https://www.iso.org/fr/standard/65694.html
5. Voir https://www.eurocae.net/product/ed-201a-aeronautical-information-system-security-aiss-framework-guidance/ ou https://www.rtca.org/security/
6. Voir https://csrc.nist.gov/pubs/sp/800/30/r1/final
7. Les Annexes à la Convention de Chicago, y compris l'Annexe 17 et sa norme 4.9.1, sont applicables aux États et non à des disciplines de l'aviation particulières, sauf indication contraire. La norme 4.9.1 s'adresse aux « exploitants ou [...] entités définis dans le programme national de sûreté de l'aviation civile ou d'autres documents nationaux applicables ». Par ce libellé, la disposition est rendue applicable à toutes les disciplines de l'aviation telles que définies au niveau national par chaque État.

2.2.5 La méthode, illustrée à la figure 2 ci-dessous, devrait comprendre les étapes suivantes :

- **Étape 1** – *Cette étape doit être réalisée par des professionnels des risques de l'aviation compétents en collaboration avec des professionnels de la cybersécurité.*
  - ⇨ Commencez par une évaluation existante des risques liés à une fonction critique de l'aviation.
  - ⇨ L'évaluation des risques pour l'aviation déterminera :
    - un niveau de sécurité minimal acceptable, appelé niveau de sécurité cible ;
    - un risque résiduel pour la sûreté de l'aviation ;
    - un niveau minimal cible de capacité ; et/ou
    - un niveau minimal cible d'efficacité.
  - ⇨ Recensez les données, l'information et les systèmes qui soutiennent le fonctionnement essentiel de l'aviation et dont l'altération pourrait avoir une incidence sur la sécurité, la sûreté, l'efficacité et/ou la capacité de l'aviation civile.

Note.— Lorsqu'une fonction critique de l'aviation est recensée, mais ne fait actuellement pas l'objet d'une évaluation des risques, il convient de réaliser une évaluation pertinente des risques pour l'aviation et de l'utiliser à l'étape 1. Entre-temps, l'étape 2 ci-dessous peut être réalisée pour évaluer le risque que présentent les données, l'information et les systèmes sur lesquels repose cette fonction.

- **Étape 2** – *Cette étape doit être réalisée par des professionnels de la cybersécurité en collaboration avec des professionnels compétents en matière de risques pour l'aviation.*
  - ⇨ Déterminez les scénarios de cybermenaces qui pourraient avoir une incidence sur les données, l'information et les systèmes cités ci-dessus, et menez une évaluation des cyberrisques dans ces scénarios.
    - Décrivez le scénario de menace, ainsi que les moyens et méthodes de la cyberattaque et le type d'acteur malveillant.
    - Il conviendrait d'évaluer la probabilité en premier lieu, sans tenir compte des mesures actuelles d'atténuation des risques. Cela permet de déterminer l'intention et la capacité de l'acteur malveillant à mettre à exécution un scénario de menace. Cette étape pourrait inclure une description, dans la mesure du possible, du profil de l'acteur malveillant, des outils, etc.

Note.— Les cybermenaces recensées devraient faire l'objet d'une surveillance continue afin de tenir compte de l'évolution des intentions et/ou des capacités des acteurs malveillants.

- L'incidence, les conséquences ou les effets[8] sont évalués en fonction de la nature et de l'ampleur de l'attaque en question, du point de vue de la sécurité et de la sûreté de l'aviation, et de la capacité et/ou de l'efficacité de la navigation aérienne, dans le cadre du scénario le plus défavorable ou du pire scénario crédible.
- Les autres vulnérabilités du système sont évaluées en fonction des mesures d'atténuation actuellement mises en œuvre.
- Ce qui découle de l'évaluation à laquelle il est fait référence ci-dessus constitue le cyberrisque résiduel. Il s'agit du risque global qui subsiste après que les mesures d'atténuation existantes ainsi que la probabilité et les conséquences de la menace ont été prises en compte.

Note 1.— Les tableaux de classement de la probabilité, de l'incidence et des vulnérabilités restantes sont décrits dans la section suivante.

Note 2.— Chaque organisation devrait définir ses propres objectifs en matière de cybersécurité et critères d'acceptation des cyberrisques sur la base des cadres réglementaires et juridiques applicables au secteur de l'aviation et à d'autres entités (telles que les autorités nationales de cybersécurité), ainsi que de ses propres niveaux de tolérance au risque.

8. Dans le présent document, les termes incidence, conséquence et effet sont utilisés de manière interchangeable.

➢ **Étape 3** – *Cette étape doit être réalisée par des professionnels des risques pour l'aviation*.

⇨ Mettez à jour l'évaluation des risques pour l'aviation définie à l'étape 1. Cette étape produira les résultats suivants :

- un niveau de sécurité actualisé ;
- un risque résiduel pour la sûreté de l'aviation actualisé ;
- un niveau de capacité actualisé ; et/ou
- un niveau d'efficacité actualisé ;

➢ **Étape 4** – *Cette étape doit être réalisée conjointement par des professionnels des risques pour l'aviation et des professionnels de la cybersécurité*.

⇨ Analysez les résultats de l'évaluation des risques pour l'aviation actualisés en fonction des niveaux de risque initiaux obtenus à l'étape 1.

⇨ Les critères d'acceptation des risques devraient être prédéfinis par l'organisation et devraient être exhaustifs, couvrant au minimum les disciplines de l'aviation pertinentes (sécurité, sûreté et capacité et/ou efficacité de l'aviation) et les objectifs et cibles en matière de cybersécurité.

Note.— Chaque organisation devrait définir ses propres critères d'acceptation des cyberrisques sur la base des cadres réglementaires et juridiques applicables au secteur de l'aviation (et parfois à d'autres secteurs), ainsi que de ses propres niveaux de tolérance au risque.

⇨ Au moment d'évaluer les résultats actualisés par rapport aux résultats originaux obtenus à l'étape 1, le risque mis à jour de l'évaluation des risques pour l'aviation devrait être jugé inacceptable si :

- l'évaluation actualisée des risques pour l'aviation n'atteint pas les cibles acceptées (niveaux de risque initiaux) obtenues à l'étape 1 ; ou
- le cyberrisque résiduel ne répond pas aux objectifs de l'organisation en matière de cybersécurité.

⇨ Si le risque mis à jour n'est pas acceptable, l'organisation devrait l'atténuer en ajoutant des mesures d'atténuation spécifiques des risques de cybersécurité, dans la mesure du possible, et réévaluer l'acceptation du risque.

⇨ Si, même après la mise en œuvre de mesures d'atténuation des risques de cybersécurité, le risque n'est toujours pas acceptable, l'organisation devrait définir de nouvelles mesures d'atténuation pertinentes et efficaces pour ramener le risque à des niveaux acceptables.

Note.— En cas de désaccord entre les professionnels de l'aviation et ceux de la cybersécurité concernant le caractère acceptable des risques, la décision devrait être portée à la charge des instances dirigeantes de l'organisation.

⇨ Si des mesures d'atténuation des risques de cybersécurité sont prévues, retournez à l'étape 3.

⇨ Veillez à ce que les nouvelles mesures d'atténuation des risques de cybersécurité n'aient pas d'incidence négative sur l'évaluation des risques pour l'aviation. Le cas échéant, prenez des mesures propres à l'aviation[9] ou réexaminez les mesures de cybersécurité pour remédier à toute incidence négative.

Note.— Il est important de tenir compte de l'effet potentiel des mesures d'atténuation des risques de cybersécurité sur les données, les informations et/ou les systèmes critiques d'autres fonctions essentielles de l'aviation, car ces mesures peuvent avoir une incidence sur ces fonctions. Si de telles incidences sont recensées, il conviendrait d'effectuer une évaluation conjointe des risques pour l'aviation et des cyberrisques associés à ces fonctions critiques.

⇨ L'évaluation devrait être effectuée une nouvelle fois dans les cas suivants :

- les cybermenaces évoluent, notamment lorsque des scénarios de cybermenaces existants ou nouveaux sont susceptibles de devenir plausibles au fil du temps, ou lorsque des changements surviennent dans les renseignements ou les connaissances utilisés pour l'identification, l'analyse et la classification des risques ;

9. Les mesures propres à l'aviation désignent les mesures opérationnelles concernant la sécurité et la sûreté de l'aviation, ainsi que l'efficacité et/ou la capacité de la navigation aérienne.

- des modifications sont apportées aux exigences relatives à l'évaluation des risques dans la ou les disciplines dans lesquelles les cyberrisques sont intégrés ;
- des changements fonctionnels surviennent dans les fonctions de l'aviation qui sont évaluées ; et/ou
- des changements surviennent dans la propension à prendre des risques de l'organisation et dans sa politique de surveillance et d'évaluation continues et/ou la périodicité de l'évaluation des risques.

2.2.6 Les appendices A et B illustrent la manière dont la méthode peut être appliquée. Le premier exemple, figurant dans l'**appendice A,** démontre comment intégrer une cybermenace dans une évaluation des risques pour la sécurité. Le deuxième exemple, figurant dans l'**appendice B,** démontre comment une cybermenace peut être intégrée à une évaluation des risques pour la sûreté de l'aviation.

2.2.7 L'objectif de ces exemples est de démontrer que les évaluations des risques pour l'aviation et les évaluations des cyberrisques ne peuvent pas être menées de manière isolée lorsqu'il s'agit d'examiner des cybermenaces pour les processus d'aviation. **Il est essentiel qu'il y ait des liens, une coordination et une collaboration entre elles afin d'assurer une protection et une résilience complètes de l'aviation civile face aux cybermenaces et aux cyberrisques.**

2.3 SCHÉMA DES PROCESSUS MÉTHODOLOGIQUES ET TABLEAUX DE NOTATION DES CYBERRISQUES

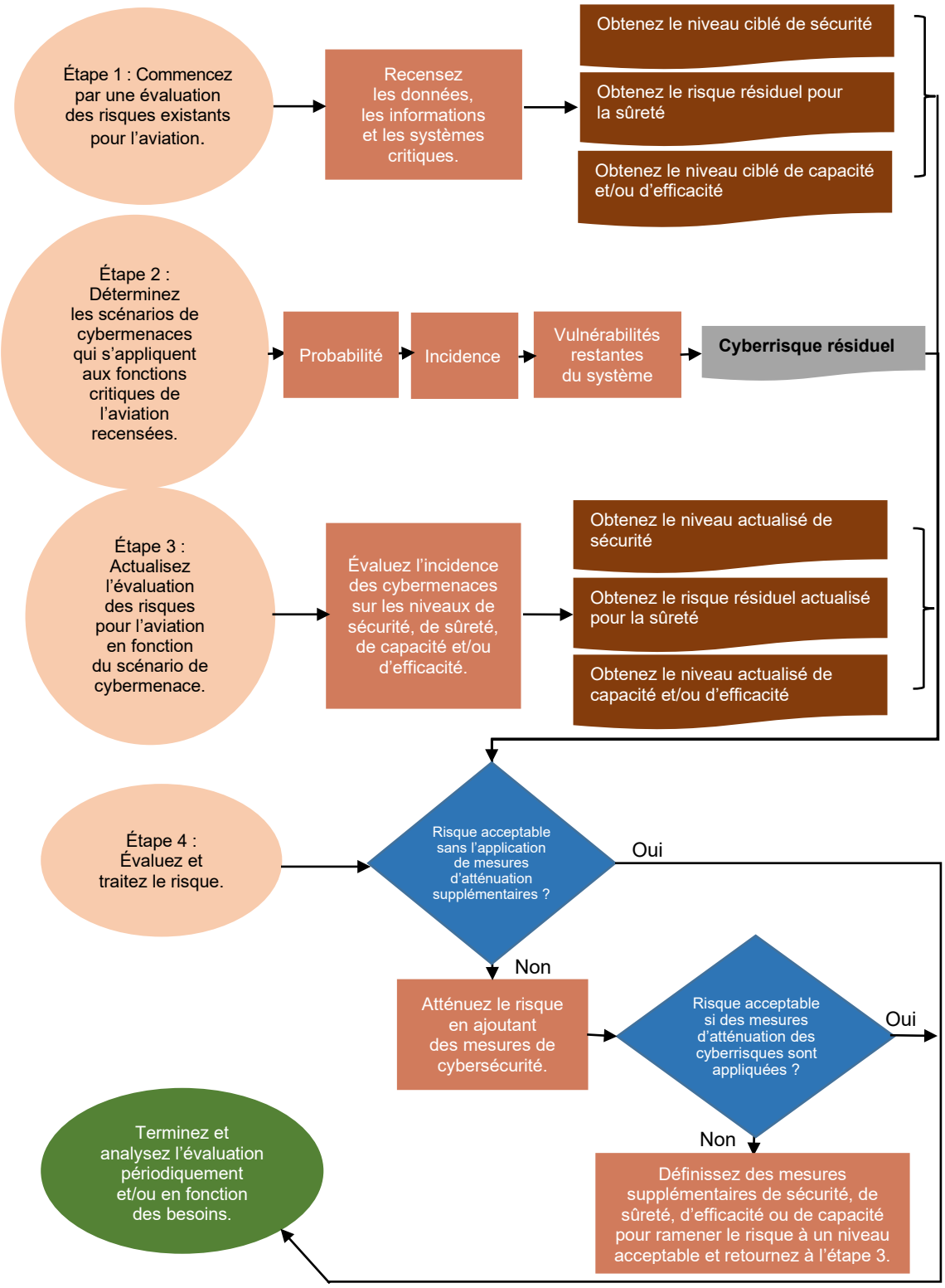


Figure 2. Schéma du processus de la méthode de gestion des risques

Tableaux de notation des cyberrisques

2.3.1 Les différents tableaux de notation figurant dans la présente section donnent des exemples de meilleures pratiques et des conseils sur la procédure visant à élaborer des matrices d'évaluation des cyberrisques. Bien qu'il soit recommandé de les consulter en vue d'assurer une compréhension commune des cybermenaces et des cyberrisques dans le contexte du partage d'informations[10], ces tableaux de notation peuvent être adaptés en fonction des stratégies de gestion des risques mises en place par les organisations.

2.3.2 Les évaluations figurant dans le chapitre 3 de la version en diffusion restreinte du présent document ont été réalisées au moyen des scores figurant dans la présente section.

2.3.3 Dans le cadre de cette méthode, la probabilité, l'incidence et la vulnérabilité sont classées sur cinq niveaux (ÉLEVÉ, MOYEN-ÉLEVÉ, MOYEN, MOYEN-FAIBLE ou FAIBLE). Chaque niveau est accompagné d'un score et d'une définition.

Probabilité

2.3.4 Il s'agit de la probabilité qu'une cybermenace se concrétise, compte tenu de la capacité et de l'intention d'un auteur de menace de mener à bien une cyberattaque.

2.3.5 L'évaluation de la probabilité devrait être effectuée par des experts en cybersécurité ou, à tout le moins, par des experts en risques pour l'aviation compétents qui ont accès aux rapports de renseignements sur les cybermenaces.

Tableau 1. Classement de la probabilité des cybermenaces

NOTE DE PROBABILITÉ		
ÉLEVÉ	5	Scénario très plausible, une attaque réelle de ce genre étant survenue il y a quelques années ou parce qu'il y a des éléments tangibles qui indiquent la présence de moyens et d'une intention.
MOYEN-ÉLEVÉ	4	Scénario clairement plausible, avec des preuves ou des exemples relativement récents de planification en amont d'un attentat ou d'une action de reconnaissance hostile.
MOYEN	3	Scénario globalement plausible, avec quelques preuves d'intention et de capacité, et éventuellement quelques exemples.
MOYEN-FAIBLE	2	Scénario pour lequel il n'y a pas d'exemple, ou pas d'exemple récent, à part quelques preuves d'intention, mais la méthode de réalisation ne semble pas être suffisamment élaborée pour réussir un scénario d'attaque, ou elle va probablement être remplacée par d'autres formes d'attaque.
FAIBLE	1	Scénario théoriquement plausible, mais sans exemple, avec une intention théorique, mais sans moyens apparents.

10. Pour de plus amples renseignements sur l'échange d'informations sur la cybersécurité, voir les éléments indicatifs y relatifs à l'adresse suivante : https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx

Incidence/Conséquence/Effet

2.3.6 L'incidence est le résultat de la mesure qualitative des conséquences d'un cyberincident sur les actifs mentionnés dans la description du scénario de menace.

2.3.7 L'évaluation des incidences devrait être réalisée par des experts de l'aviation dans la fonction analysée.

2.3.8 Les incidences sur la sécurité et la sûreté de l'aviation sont extraites des éléments indicatifs de l'OACI sur l'évaluation des risques pour la sécurité et la sûreté de l'aviation, respectivement, dans le *Manuel de gestion de la sécurité* (Doc 9859) et dans l'*Énoncé du contexte de risque mondial de sûreté de l'aviation civile* (Doc 10108 – Diffusion restreinte). L'incidence sur la capacité et l'efficacité de la navigation aérienne a été mise au point pour le présent document.

Tableau 2. Classement de l'incidence des cybermenaces

NOTE D'INCIDENCE/DE CONSÉQUENCE/D'EFFET[11]			
	Sécurité de l'aviation[12]	**Sûreté de l'aviation[13]**	**Capacité et/ou efficacité de la navigation aérienne**
ÉLEVÉ **Score = 5**	**Catastrophique :** - Aéronef détruit	- Centaines de morts - Milliards USD - Lourdes perturbations des services aériens et une très grande perte de confiance envers l'aviation civile	- Perturbation grave de la capacité et/ou de l'efficacité de la navigation aérienne. - Pannes généralisées ou défaillance complète de systèmes opérationnels essentiels, ayant une incidence grave sur la gestion de la circulation aérienne, les opérations aéroportuaires[14] ou les opérations des entreprises de transport aérien.[15] - Retards ou annulations de vols importants, ce qui pose des risques opérationnels importants pour le système de l'aviation et la capacité d'exploiter des aéronefs.
MOYEN-ÉLEVÉ **Score = 4**	**Danger :** - Blessures graves - Dommages majeurs - Une réduction importante de la marge de sécurité, au point qu'on ne peut plus être sûr que le personnel opérationnel fournira un travail précis ou complet.	- Certaines, mais pas toutes les incidences du niveau ÉLEVÉ	- Perturbations importantes de la capacité et/ou de l'efficacité de la navigation aérienne. - Pannes ou défaillances prolongées des principaux systèmes opérationnels, ayant une incidence sur les services essentiels et la capacité d'exploiter des aéronefs. - Retards importants dans le flux de la circulation aérienne ou les opérations aéroportuaires ou aériennes, entraînant une congestion.

11. Le tableau des notes d'incidence, de conséquence et d'effet décrit l'incidence pour chaque discipline de l'aviation à laquelle la méthode est appliquée. Les colonnes sont indépendantes les unes des autres et concernent chaque discipline de l'aviation, et la notation de la première colonne doit être lue en même temps que la colonne spécifique à la discipline de l'aviation dans laquelle l'évaluation des cyberrisques est intégrée.
12. Les informations sur l'incidence/la conséquence/l'effet pour la sécurité de l'aviation proviennent de la quatrième édition du *Manuel de gestion de la sécurité* (Doc 9859).
13. Les informations sur l'incidence/la conséquence/l'effet pour la sûreté de l'aviation proviennent de la troisième édition de l'*Énoncé du contexte de risque mondial de sûreté de l'aviation civile* (Doc 10108 – Diffusion restreinte).
14. Dans ce contexte, les opérations aéroportuaires comprennent tous les services aéroportuaires nécessaires aux arrivées, aux départs et à la circulation à la surface des aéronefs, ainsi que la gestion des passagers, y compris, mais sans s'y limiter, l'accès aux portes d'embarquement, la disponibilité des services de sûreté, l'inspection des pistes, la manutention des bagages, le carburant, le dégivrage, la restauration, l'éclairage de l'aéroport et d'autres services connexes.
15. Dans ce contexte, les opérations d'une entreprise de transport aérien comprennent tous les aspects qui ont une incidence sur la capacité d'exploiter les aéronefs de manière efficace, y compris l'information destinée aux équipages de conduite, la maintenance des aéronefs, l'exploitation des aéronefs, la météorologie, la disponibilité du GNSS par rapport à la navigation et à l'approche de non-précision, l'information aéronautique, etc.

NOTE D'INCIDENCE/DE CONSÉQUENCE/D'EFFET[11]			
	Sécurité de l'aviation[12]	**Sûreté de l'aviation[13]**	**Capacité et/ou efficacité de la navigation aérienne**
MOYEN Score = 3	**Majeur :** - Personnes blessées - Incident grave - Une baisse de la capacité du personnel opérationnel à faire face à des conditions de fonctionnement difficiles en raison d'une augmentation de la charge de travail ou des conditions affectant son efficacité	- Dizaines de morts - Centaines de millions USD - De graves perturbations des services aériens et une importante perte de confiance envers l'aviation civile	- Perturbations perceptibles de la capacité et/ou de l'efficacité de la navigation aérienne. - Pannes ou défaillances partielles des principaux systèmes opérationnels, affectant plusieurs services. - Retards modérés dans la fluidité du trafic aérien ou incidence modérée sur les opérations aéroportuaires ou aériennes, nécessitant une coordination et des ressources supplémentaires pour y faire face.
MOYEN-FAIBLE Score = 2	**Mineur :** - Désagréments et exploitation réduite - Recours à des procédures d'urgence - Incident mineur	- Certaines, mais pas toutes les incidences des conséquences du niveau MOYEN	- Perturbation légère de la capacité et/ou de l'efficacité de la navigation aérienne. - Incident limité affectant des systèmes ou des services spécifiques. - De légers retards ou des inefficacités dans la fluidité de la circulation aérienne ou dans les opérations aéroportuaires ou aériennes, gérables dans le cadre des procédures opérationnelles normales.
FAIBLE Score = 1	**Négligeable :** - Potentiellement quelques blessés - Peu de conséquences	- Potentiellement quelques morts et blessés - Quelques incidences économiques - Quelques perturbations des services aériens et une certaine perte de confiance à l'égard de l'aviation civile	- Perturbation minime de la capacité et/ou de l'efficacité de la navigation aérienne. - Incident isolé avec une incidence très limitée sur l'ensemble des opérations. - Retards ou perturbations très faibles de la circulation aérienne, incidence très limitée sur les opérations aéroportuaires ou aériennes.

Vulnérabilité

2.3.9 La vulnérabilité se mesure de manière qualitative et décrit l'efficacité des mesures existantes pour atténuer les conséquences du scénario de cybermenace sur les actifs concernés.

2.3.10 L'évaluation de la vulnérabilité devrait être réalisée conjointement par des experts de l'aviation et des experts en cybersécurité capables d'analyser la fonction critique de l'aviation concernée et d'évaluer comment les acteurs de la menace peuvent exploiter les failles de la cybersécurité.

Tableau 3. Classement de la vulnérabilité aux cybermenaces

NOTE DE VULNÉRABILITÉ		
ÉLEVÉ	1	Il n'y a pas de mesures d'atténuation, soit parce qu'il n'existe pas d'exigences dans ce sens, soit parce qu'on ne dispose pas de mesures réalistes et efficaces.
MOYEN-ÉLEVÉ	0,8	Les mesures d'atténuation sont d'une portée limitée, et des domaines et aspects importants du risque ne correspondent pas aux prescriptions ni à des mesures mises en place.
MOYEN	0,6	Les caractéristiques des niveaux MOYEN-ÉLEVÉ et MOYEN-FAIBLE sont présentes.
MOYEN-FAIBLE	0,4	Des mesures limitant la vulnérabilité sont généralement en place, mais elles peuvent ne pas être au point ou n'être efficaces qu'en partie seulement. Par exemple, les manuels de sécurité de l'information élaborés par l'OACI peuvent être en place pour tous les domaines et tous les aspects, mais dans la pratique, ils pourraient être perfectionnés ou mis en œuvre de manière plus efficace.
FAIBLE	0,2	Des exigences claires sont en place et des mesures d'atténuation généralement considérées comme efficaces sont largement utilisées.

Exemple d'une évaluation des cyberrisques

Tableau 4. Matrices de notation et d'évaluation des cyberrisques

MATRICE D'ÉVALUATION DES CYBERRISQUES				
Scénario de cybermenace	**Probabilité** **X**	**Incidence** **X**	**Vulnérabilité**	**= Risque résiduel**
Un acteur malveillant lance une cyberattaque pour affecter un actif de l'aviation géré par un acteur de l'aviation en exploitant une vulnérabilité.	**MOYEN** **3**	**MOYEN-ÉLEVÉ** **4**	**MOYEN-ÉLEVÉ** **0,8**	**9,6**

MATRICE DES SCORES DE CYBERRISQUES	
SCORE DU RISQUE	**NOTATION DU RISQUE**
20–25	ÉLEVÉ
15–20	MOYEN-ÉLEVÉ
10–15	MOYEN
5–10	MOYEN-FAIBLE
0–5	FAIBLE

APPENDICES

Appendice A

EXEMPLE D'APPLICATION DE LA MÉTHODE DE GESTION DES RISQUES POUR LA SÉCURITÉ DE L'AVIATION

HYPOTHÈSES ET APERÇU GÉNÉRAL

Cet exemple illustre l'intégration de l'évaluation des cyberrisques dans l'évaluation des risques pour la sécurité de l'aviation, à l'aide d'un scénario de menace hypothétique évalué par un fournisseur de services de navigation aérienne (ANSP).

Hypothèses :

- L'ANSP a déjà examiné, évalué et atténué les risques de sécurité pertinents au moyen de l'analyse de l'arborescence des pannes (FTA[16]).
- Les experts en sécurité de l'aviation ont déterminé que la communication air-sol était une fonction essentielle de l'aviation.
- À des fins de simplification, on suppose que la cybermenace évaluée n'a d'incidence que sur la sécurité (en d'autres termes, elle n'a pas d'incidence sur l'efficacité ni sur la capacité de la navigation aérienne).
- L'ANSP utilise les mêmes tableaux de notation pour la probabilité, l'incidence et la vulnérabilité que ceux figurant dans le présent document.
- La notation utilisée pour l'évaluation des cyberrisques se base sur des valeurs différentes de celles du paragraphe 3.3.17, car la portée de l'évaluation dans cet exemple est limitée aux systèmes au sol et aux données liées aux CPDLC.
- À des fins de simplification, il est supposé que dans le scénario de cybermenace, illustré dans la figure 3 ci-dessous, l'incidence de la cybermenace ne concerne que les messages CPDLC liés à l'autorisation de niveau de vol.

Scénario de cybermenace :

- Des experts en sécurité de l'aviation ont travaillé avec des experts en cybersécurité pour examiner les évaluations de risques de sécurité existants pour la fonction de communications air-sol et considèrent les CPDLC comme un système et des informations soutenant la fonction critique qui devait faire l'objet d'une évaluation des cyberrisques.
- Des experts en sécurité de l'aviation ont produit une évaluation d'un risque existant pour la sécurité concernant un événement de sécurité couvrant les CPDLC : « Transmission parasite non détectée d'un ou de plusieurs messages utilisés pour accorder des autorisations (niveau de vol autorisé – CFL, direction et vitesse) à un ou plusieurs aéronefs ».
- Des experts en cybersécurité, dans le cadre de discussions avec des experts en sécurité de l'aviation, ont identifié « la falsification des données d'un message CPDLC envoyé par un contrôleur de la circulation aérienne à un pilote » comme scénario de cybermenace à évaluer et à intégrer dans l'évaluation des risques pour la sécurité de l'aviation ci-dessus.

16. La FTA est un outil qui contribue au recensement et à l'analyse des conditions et des facteurs qui sont à l'origine ou qui favorisent l'occurrence d'un événement indésirable donné, généralement un événement qui affecte de manière significative la sécurité, la performance, l'économie ou d'autres caractéristiques requises du système. La FTA est appliquée de manière intensive à l'évaluation de la sécurité des systèmes.
Des orientations sur l'utilisation de la FTA figurent dans la partie IV de l'outil Méthode d'évaluation de la sécurité électronique (eSAM) d'EUROCONTROL, https://www.eurocontrol.int/tool/safety-assessment-methodology, dans l'annexe K : Éléments indicatifs sur l'analyse de l'arborescence des pannes.

- Le scénario évalué dans cet exemple couvre la falsification intentionnelle des données d'un message CPDLC envoyé par le contrôleur au pilote, à savoir qu'un message original (autorisation de niveau de vol) envoyé par un contrôleur de la circulation aérienne à un pilote est falsifié (remplacé par un niveau de vol délibérément faux) par un acteur malveillant avant d'être transmis à l'aéronef.
- Par souci de simplicité, le vecteur d'attaque envisagé se situe uniquement sur le segment sol de l'infrastructure CPDLC, c'est-à-dire dans les installations au sol de l'ANSP (réseau interne ou serveurs), ou à partir du réseau sol-sol du fournisseur de services de communications, ou à partir du réseau local et des serveurs de la station air-sol, ce qui signifie que l'exemple exclut d'autres vecteurs d'attaque tels que la communication air-sol au moyen de messages CPDLC. En se basant sur l'exemple de catégorisation des cybermenaces figurant dans l'appendice C (voir la version en diffusion restreinte du présent document), cette cybermenace peut être classée comme suit :
    - Domaine : fournisseur de services de navigation aérienne.
    - Fonction : communications, navigation et surveillance (CNS).
    - Sous-fonction : communication.
    - Cybermenace : altération (modification du contenu du message).

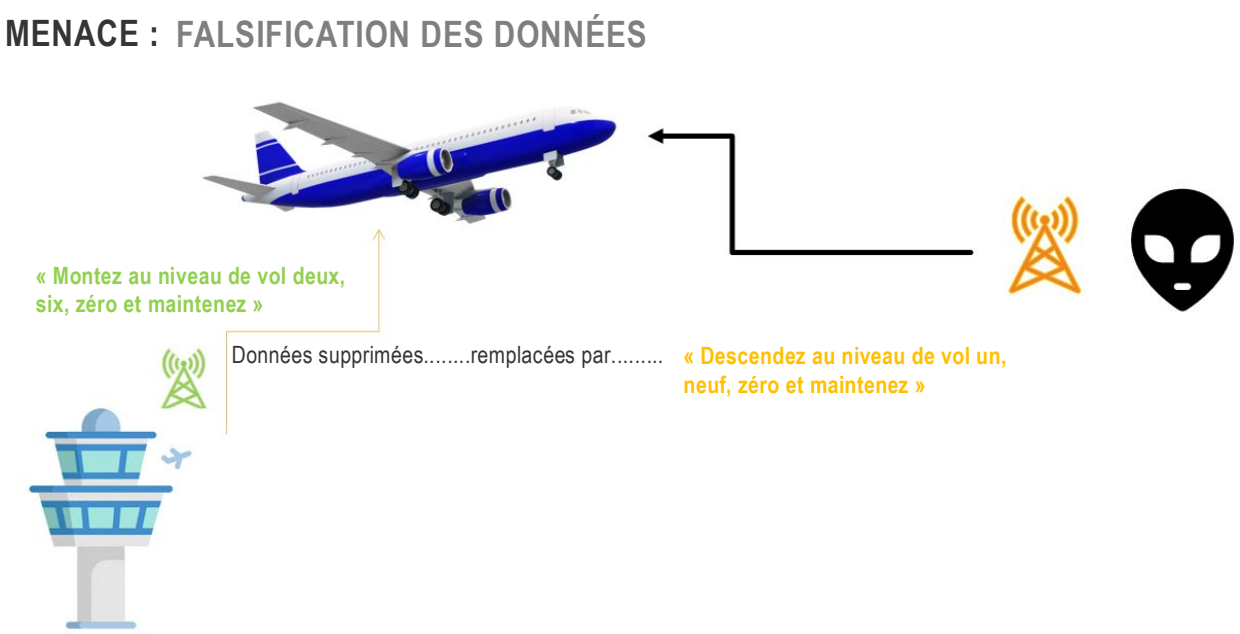
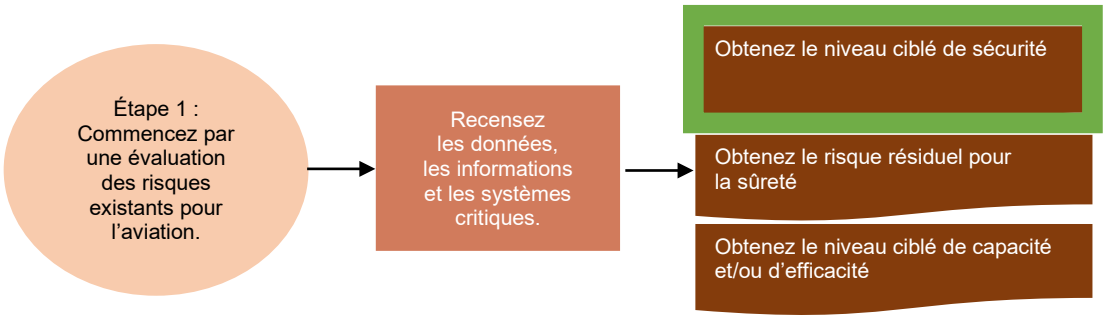


Figure 3. Menace : falsification des données
(voir la figure 4 dans la version en diffusion restreinte)

APPLICATION DE LA MÉTHODE ÉTAPE PAR ÉTAPE



- ⇨ Des experts en sécurité de l'aviation ont travaillé avec des experts en cybersécurité pour examiner les évaluations existantes des risques de sécurité concernant la fonction de communications air-sol, et ont considéré les CPDLC comme un système et des informations qui appuient la fonction critique devant faire l'objet d'une évaluation des cyberrisques.
- ⇨ Les experts en sécurité de l'aviation ont produit le diagramme original de l'arborescence des pannes de sécurité[17], sans cause liée à la cybersécurité. L'événement de haut niveau relatif à notre scénario de cybermenace CPDLC est le suivant : « une transmission parasite non détectée d'un ou de plusieurs messages destinés à accorder des autorisations à un ou plusieurs aéronefs ».
- ⇨ **Le niveau de sécurité ciblé pour l'événement de haut niveau « ne doit pas dépasser 10^−5 occurrences par heure de vol ».**

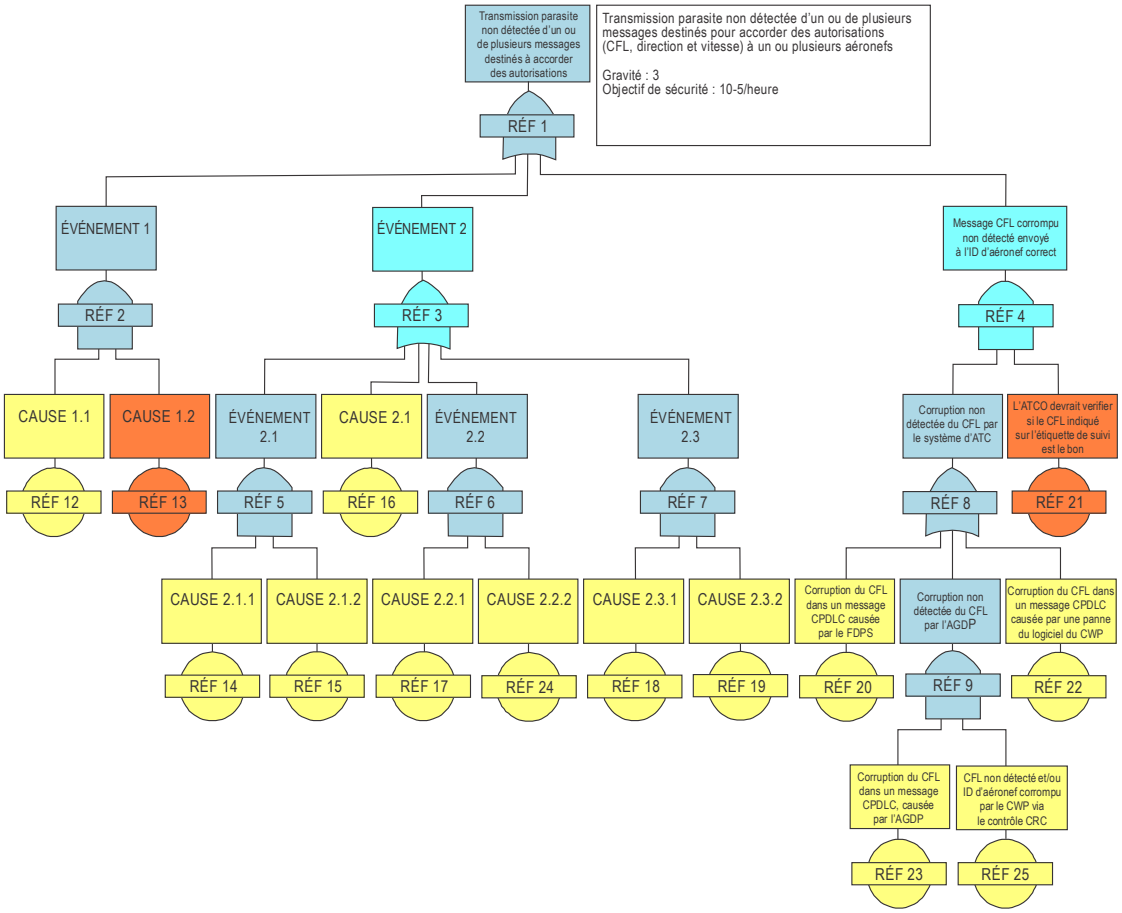
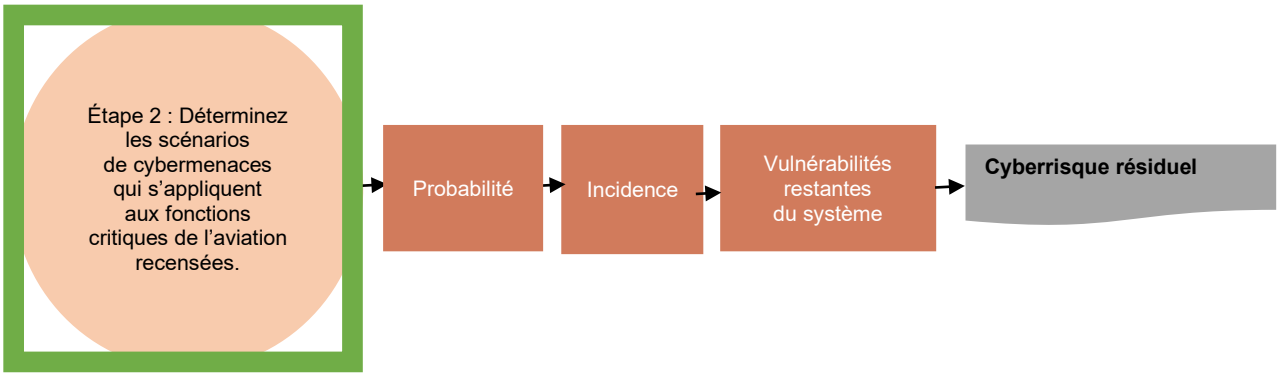


Figure 4. Diagramme original de l'arborescence des pannes (voir la figure 5 dans la version en diffusion restreinte)

17. Sigles utilisés dans le diagramme de l'arborescence des pannes :
    - AGDP : processeur de liaison de données air-sol, le serveur de données air-sol
    - CFL : niveau de vol autorisé
    - CWP : poste de travail de contrôleur (l'interface humain-machine)
    - FDPS : système de traitement des données de vol



- ⇨ Des experts en cybersécurité, en collaboration avec des experts en sécurité de l'aviation, ont identifié « la falsification des données d'un message CPDLC envoyé par un contrôleur de la circulation aérienne à un pilote » comme scénario de cybermenace plausible à évaluer et à intégrer dans l'évaluation des risques pour la sécurité de l'aviation ci-dessus.
- ⇨ L'évaluation des cyberrisques a été réalisée par les experts en cybersécurité de l'ANSP en collaboration avec des experts en sécurité. Les experts en cybersécurité connaissent les méthodes et les vecteurs d'attaque courants qui caractérisent les cybermenaces, tandis que les experts en sécurité connaissent l'architecture du système.

Les composantes de l'évaluation des cyberrisques de l'étape 2 sont développées pour prendre en compte les étapes suivantes :

Les étapes ci-dessous ont été ajoutées à l'évaluation des cyberrisques afin d'établir la matrice des cyberrisques.

- ⇨ **Probabilité :**
  - Les experts en sécurité se basent généralement sur les possibilités qu'un événement se produise pour déterminer les probabilités (par exemple, le nombre d'événements par heure de vol). De plus, certains experts tiennent compte de la « distance » par rapport à l'événement de haut niveau dans l'arborescence des pannes, lorsque celui-ci est utilisé, pour estimer la probabilité (par exemple, plus on est loin de l'événement de haut niveau, plus la probabilité d'avoir une incidence sur l'événement de haut niveau est faible en termes de changement du niveau de sécurité ciblé). D'autre part, les experts utilisent souvent des tableaux de probabilité avec des valeurs discrètes (comme le tableau 1 du chapitre 2). L'objectif de ce travail conjoint entre experts est de parvenir à une compréhension commune des différentes composantes du risque.
  - Ainsi, dans cet exemple, l'insertion de la cybermenace dans l'arborescence des pannes (les éléments rouges) rend plus aisée l'estimation de la probabilité, en termes de capacité et d'intention, que la cybermenace se matérialise[18].

18. Dans une évaluation complète des cyberrisques, de nombreux vecteurs d'attaque peuvent être ajoutés au diagramme d'origine. Pour simplifier, l'exemple ne comprend que deux vecteurs d'attaque possibles.

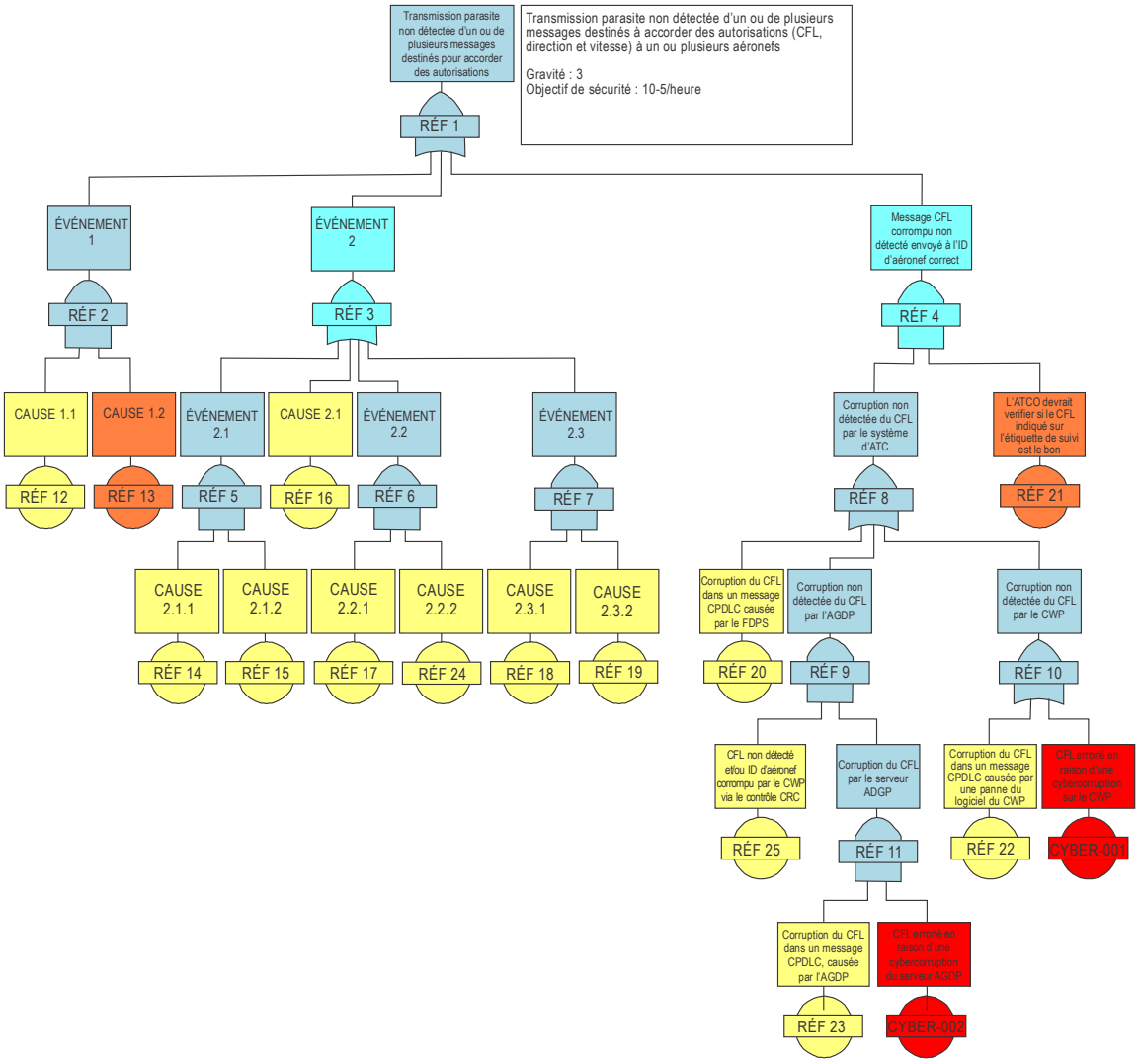


Figure 5. Diagramme actualisé de l'arborescence des pannes (voir la figure 6 dans la version en diffusion restreinte)

- Un score de 2 a été attribué à la probabilité que la cybermenace se réalise, ce qui correspond au niveau MOYEN-FAIBLE (à savoir un scénario pour lequel il n'y a pas d'exemple, ou pas d'exemple récent, à part quelques preuves d'intention, mais la méthode de réalisation ne semble pas être suffisamment développée pour déboucher sur un scénario d'attentat réussi, ou elle va probablement être remplacée par d'autres formes d'attentat).

⇨ **Incidence/Conséquence/Effet :**

- L'évaluation de l'incidence implique une évaluation d'un scénario plausible le plus défavorable, ce qui signifie en l'occurrence que la cyberattaque a réussi et que l'événement de haut niveau n'a pas été évité. En tant que telle, l'évaluation des incidences repose sur le postulat de la gravité la plus élevée possible de l'événement de haut niveau avant l'introduction de la cybermenace, qui est et correspond à un niveau d'incidence MOYEN (incidence majeure sur la sécurité : « un incident grave entraînant une réduction des marges de sécurité et une perte de la capacité du personnel opérationnel à faire face à des conditions d'exploitation négatives suite à une augmentation de la charge de travail en raison de conditions réduisant leur efficacité »).

⇨ **Vulnérabilité :**

- L'évaluation des vulnérabilités s'effectue en tenant compte des mesures d'atténuation existantes.
- À cet égard, la FTA indique qu'un contrôle de redondance cyclique (CRC)[19] du message CPDLC est effectué. À ce titre, elle est prise en compte en même temps que des mesures liées à la sécurité informatique (protection des systèmes et des serveurs) et à la sûreté de l'aviation (vérification des antécédents et contrôle d'accès).

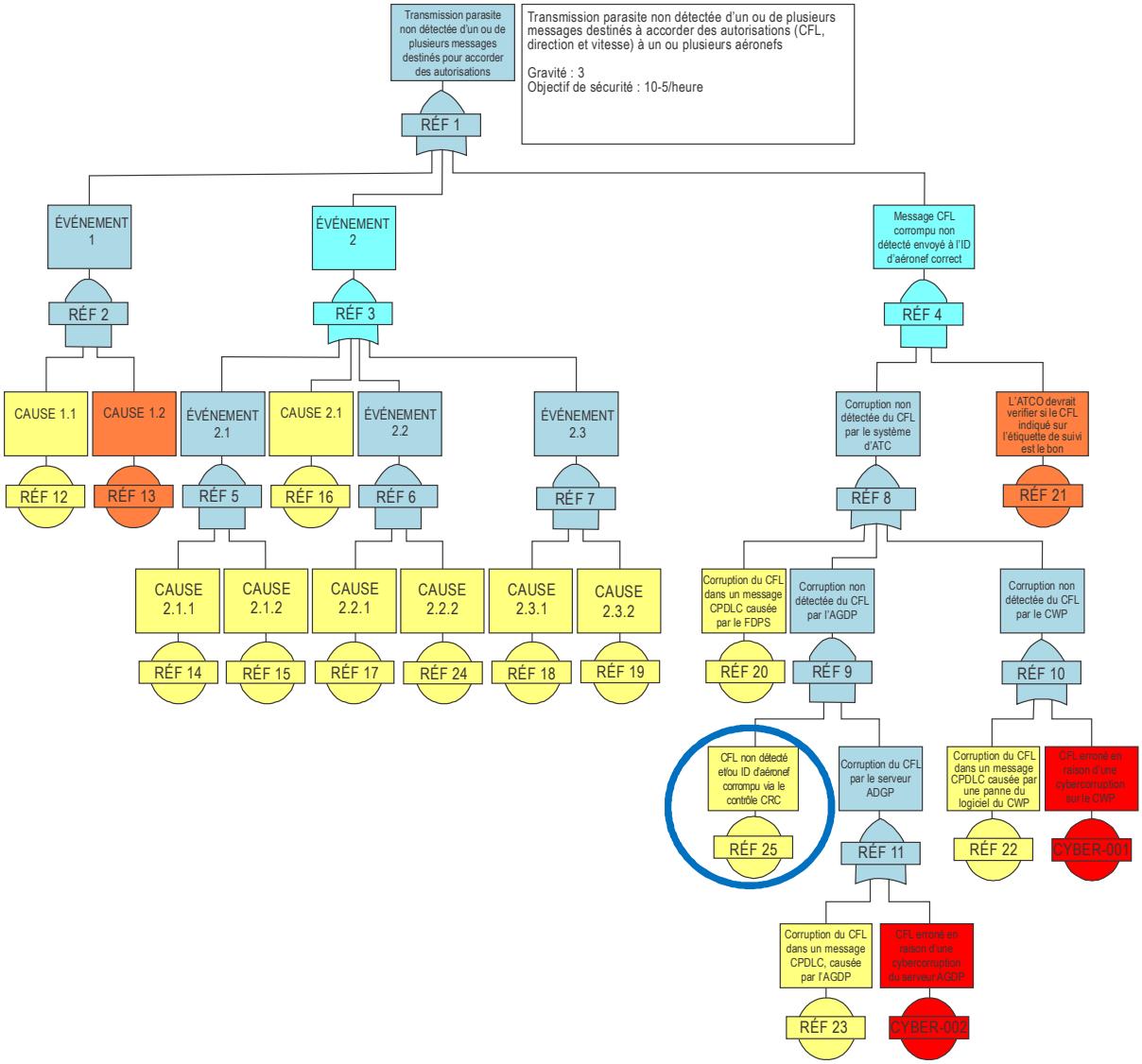


Figure 6. Diagramme actualisé de l'arborescence des pannes (voir le cercle)
(voir la figure 7 dans la version en diffusion restreinte)

19. Le CRC est défini comme « une méthode permettant de s'assurer que les données n'ont pas été modifiées après avoir été envoyées dans le cadre d'une communication ». Source : NIST SP800-72

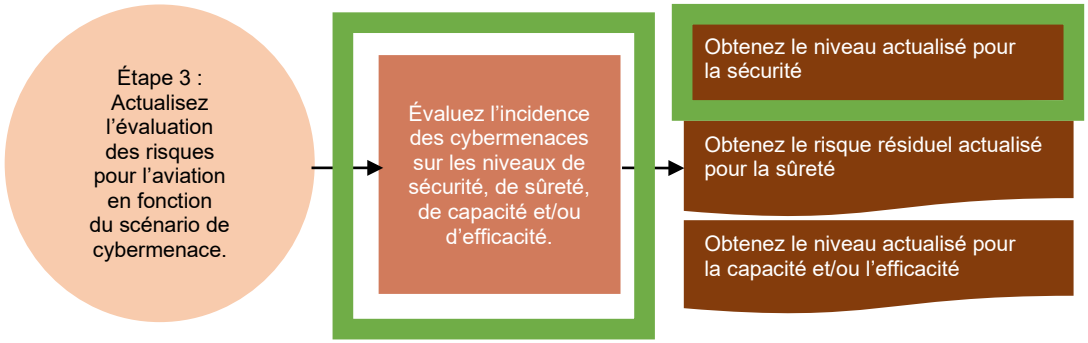
- Les experts en cybersécurité savent que le CRC est principalement utilisé pour détecter les erreurs involontaires dans les données. Cette méthode n'est pas efficace contre les interférences intentionnelles, car l'attaquant est capable de modifier le hachage du CRC en même temps que le message change et, par conséquent, la conclusion des experts est que les contrôles de cybersécurité existants pourraient ne pas être suffisants pour atténuer le risque.
- De plus, l'évaluation des vulnérabilités a permis de conclure qu'une cyberattaque externe serait difficile à préparer et à exécuter. Les réseaux et les systèmes de communication ANSP sont protégés de manière adéquate contre les attaques externes et l'organisation a mis en place des capacités de surveillance et de détection adéquates. Une attaque interne (menace interne) serait relativement plus facile à organiser, car les mesures de sécurité physique mises en œuvre sont aussi adéquates (contrôle d'accès aux salles concernées et vérification des antécédents du personnel ayant accès à ces zones).
- En conséquence, la vulnérabilité se voit attribuer un score de MOYEN-ÉLEVÉ (0,8).

⇨ **Cyberrisque résiduel :**
- Le cyberrisque résiduel peut désormais être calculé en multipliant les scores de probabilité, d'incidence et de vulnérabilité : **2 x 3 x 0,8 = 4,8**.

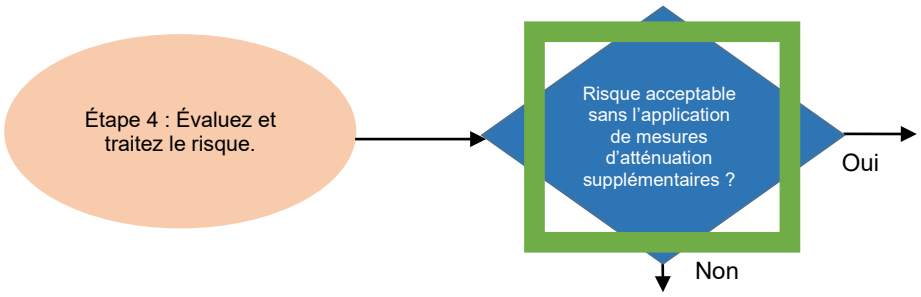
⇨ Le score de cyberrisque résiduel de 4,8 a été arrondi à 5, car les experts l'ont considéré comme plus proche de MOYEN-FAIBLE que de FAIBLE.

La matrice des cyberrisques se présentera alors comme suit :

MATRICE DES CYBERRISQUES					
Scénario	**Probabilité**	**Incidence**	**Stratégies d'atténuation**	**Vulnérabilités**	**Risque résiduel**
Intrus falsifiant la charge utile de données d'un message CPDLC envoyé par un contrôleur à un pilote.	**Score de 2** MOYEN-FAIBLE Scénario pour lequel il n'y a pas d'exemple, ou pas d'exemple récent, à part quelques preuves d'intention, mais la méthode de réalisation ne semble pas être suffisamment développée pour déboucher sur un scénario d'attentat réussi, ou elle va probablement être remplacée par d'autres formes d'attentat.	**Score de 3** MAJEUR Événement de sécurité de haut niveau : Transmission parasite non détectée d'un ou de plusieurs messages utilisés pour accorder des autorisations.	CRC Des capacités de surveillance et de détection des intrus sont déjà mises en œuvre. Mesures de sécurité informatique Contrôle d'accès physique et vérification des antécédents	**Score de 0,8** MOYEN-ÉLEVÉ Le CRC n'est pas un outil adapté pour détecter une falsification malveillante des informations, car il peut être falsifié en même temps que les informations.	**Score de 4,8 (arrondi à 5)** MOYEN-FAIBLE Ce score sera comparé aux scores des autres scénarios de menace et utilisé pour classer les menaces.



- ⇨ Maintenant que le diagramme de l'arbre des défaillances a été mis à jour et que l'organisation en sait beaucoup plus sur la cybermenace qui est devenue un cyberrisque correspondant à des objectifs de sécurité, l'évaluation originale des risques de sécurité peut être mise à jour, y compris l'évaluation de la cybermenace, conduisant potentiellement à une nouvelle probabilité d'occurrence de l'événement de sécurité de haut niveau (« livraison parasite non détectée d'un ou de plusieurs messages utilisés pour accorder des autorisations »).
- ⇨ Cela servira de base pour les prochaines étapes, à savoir l'évaluation et le traitement des risques.

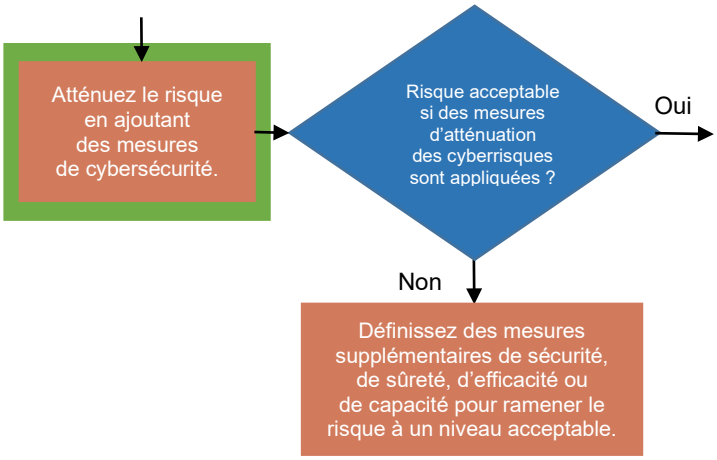


Dans le cadre des évaluations mises à jour, l'ANSP utilise sa matrice d'acceptabilité existante. Cette dernière peut comporter différents types de critères tels que :

- les critères de cybersécurité, dont la source comprend les règlements aéronautiques, les règlements et les lois sur les infrastructures critiques, la tolérance au risque organisationnel, etc.
- les critères de sécurité, qui couvrent la relation entre l'incidence sur la sécurité et la probabilité visée en matière de sécurité, ainsi que les sources liées à la réglementation aéronautique pertinente.
- les critères de capacité et d'efficacité de la navigation aérienne, qui dépendent de l'organisation (et sortent du cadre de cet exemple).

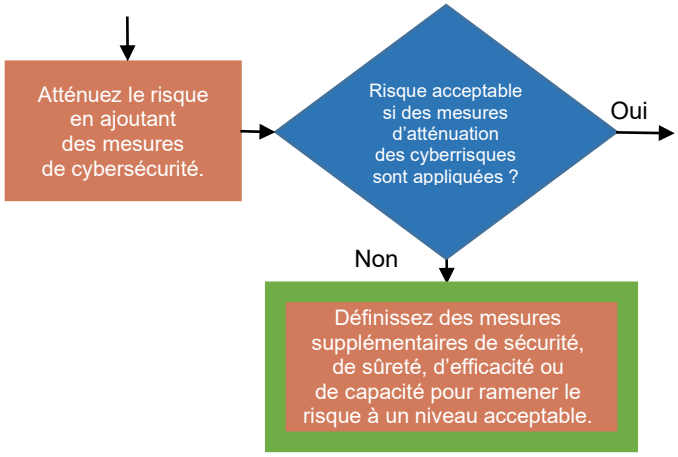
Cette évaluation à la lumière des critères organisationnels précités devrait mener à la prise d'une décision, à savoir **si le risque peut être accepté tel quel ou si des mesures d'atténuation des cyberrisques devraient être mises en place à l'appui des mesures de contrôle existantes**.

L'évaluation a mené à la décision que, même si le cyberrisque résiduel est MOYEN-FAIBLE, des mesures d'atténuation supplémentaires qui pourraient réduire encore plus le risque devaient être envisagées.



⇨ **Mesures d'atténuation dans le cadre de la cybersécurité :**

- Des experts en cybersécurité ont d'abord proposé l'ajout de nouveaux équipements pour mieux protéger le système contre toute intervention non autorisée. Cependant, cette idée a été rejetée par les experts en sécurité, car elle créerait de nouveaux points de défaillance qui nécessiteraient que l'évaluation de la sécurité du système dans son ensemble soit revue, ainsi que celle des autres systèmes touchés.
- Les experts en sécurité et en cybersécurité sont convenus que les contrôles mis en place pour protéger le système contre une cyberattaque extérieure étaient adéquats, et ont donc décidé de rechercher des mesures visant à atténuer la menace interne qui a été jugée plus crédible lors de l'évaluation des cyberrisques.
- Les experts en cybersécurité ont proposé des mesures tendant vers une plus grande rigueur dans la gestion des droits d'accès aux ordinateurs et aux serveurs concernés, ce qui a été accepté.



⇨ **Mesures d'atténuation supplémentaires**

- Grâce à ces mesures d'atténuation des cyberrisques, il a été déterminé que le risque peut être réduit davantage en envisageant d'autres types de mesures d'atténuation.
- Les experts en sûreté de l'aviation ont proposé que des mesures plus strictes soient prises en matière de vérification des antécédents et de contrôle d'accès pour le personnel ayant accès à l'ATC et aux salles des serveurs.
- L'évaluation du risque a été effectuée une deuxième fois en tenant compte des nouvelles mesures d'atténuation (mesures de cybersécurité et de sûreté de l'aviation) et il a été décidé que les nouvelles

mesures d'atténuation réduiraient le risque à un niveau acceptable, de sorte que la mise en œuvre des nouvelles mesures a été acceptée.

⇨ **Matrice des cyberrisques**

- Cela a permis de finaliser la matrice d'évaluation des cyberrisques en la complétant de mesures d'atténuation supplémentaires à consigner pour la mise en œuvre, et la matrice finale d'évaluation des cyberrisques a pris la forme suivante.

MATRICE DES CYBERRISQUES						
Scénario	**Probabilité**	**Incidence**	**Stratégies d'atténuation**	**Vulnérabilités**	**Risque résiduel**	**Stratégies d'atténuation supplémentaires**
Intrus falsifiant la charge utile de données d'un message CPDLC envoyé par un contrôleur à un pilote.	**Score de 2** MOYEN-FAIBLE Scénario pour lequel il n'y a pas d'exemple, ou pas d'exemple récent, à part quelques preuves d'intention, mais pour lequel la méthode de réalisation ne semble pas être suffisamment développée pour aboutir à un scénario d'attentat réussi, ou elle va probablement être remplacée par d'autres formes d'attentat.	**Score de 3** MAJEUR Événement de sécurité de haut niveau : Transmission parasite non détectée d'un ou de plusieurs messages utilisés pour accorder des autorisations.	CRC Des capacités de surveillance et de détection des intrus sont déjà mises en œuvre. Mesures de sécurité informatique Contrôle d'accès physique/ vérification des antécédents	**Score de 0,8** MOYEN-ÉLEVÉ Le CRC n'est pas un outil adapté pour détecter une falsification malveillante des informations, car il peut être falsifié en même temps que les informations.	**Score de 4,8 (arrondie à 5)** MOYEN-FAIBLE Ce score sera comparé aux scores des autres scénarios de menace et utilisé pour classer les menaces.	**Mesures de cybersécurité :** Optimisation et surveillance des droits d'accès numérique sur les ordinateurs et les serveurs concernés. Autre : Mesures plus strictes prises en matière de vérification des antécédents et de contrôle d'accès physique pour le personnel ayant accès à l'ATC et aux salles de serveurs.

CONCLUSION

L'approche étape par étape présentée dans cet exemple illustre comment les évaluations de la sécurité et des cyberrisques doivent être interconnectées pour faire face aux cybermenaces et aux cyberrisques pour l'aviation civile. Dans un environnement réel, ce processus se déroulerait de manière plus itérative et plus intégrée, en fonction de la structure de gouvernance organisationnelle et des cadres réglementaires ou juridiques en place.

Appendice B

EXEMPLE D'APPLICATION DE LA MÉTHODE DE GESTION DES RISQUES POUR LA SÛRETÉ DE L'AVIATION

Hypothèses et aperçu

L'exemple présenté ci-dessous illustre l'intégration de l'évaluation des cyberrisques dans l'évaluation des risques pour la sûreté de l'aviation, à l'aide d'un scénario de menace hypothétique en cours d'évaluation par un État.

Hypothèses :

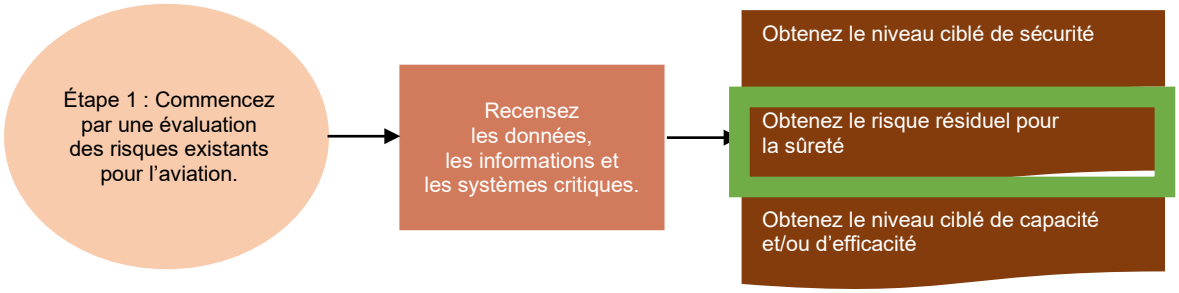
- L'État a déjà examiné, évalué et atténué les risques pour la sûreté de l'aviation pertinents au moyen des matrices de risques pour la sûreté de l'aviation.
- Les experts en sûreté de l'aviation ont déterminé que l'inspection-filtrage des bagages de cabine constituait une fonction essentielle de l'aviation.
- À des fins de simplification, on suppose que la cybermenace évaluée n'a d'incidence que sur la sûreté de l'aviation (en d'autres termes, elle n'a pas d'incidence sur la sécurité, ni sur l'efficacité ni sur la capacité de la navigation aérienne).
- L'État utilise les mêmes tableaux de notation pour la probabilité, l'incidence et la vulnérabilité que ceux utilisés dans le présent document.
- Par souci de cohérence, la notation utilisée dans l'évaluation des cyberrisques reprend les mêmes valeurs que celles du chapitre 3 de la version en diffusion restreinte du présente document. Cependant, en réalité, les scores de probabilité, d'incidence et de vulnérabilité des États et des organisations varient en fonction des différentes variables qui influent sur ces évaluations (capacités, intention, mesures d'atténuation existantes, etc.).
- En raison de la sensibilité des évaluations des risques pour la sûreté de l'aviation, la description concerne uniquement le processus visant à insérer l'évaluation des cyberrisques dans l'évaluation de la sûreté de l'aviation. Le processus d'évaluation des cyberrisques fait l'objet d'une description détaillée.

Scénario de cybermenace

- L'État a entamé une analyse des différents modes opératoires possibles d'un adversaire tentant d'introduire des engins explosifs improvisés portés par une personne (PBIED) à bord d'un aéronef dans des bagages de cabine avec l'intention de détruire l'aéronef.
- Des experts en sûreté de l'aviation ont travaillé avec des experts en cybersécurité pour examiner les évaluations de risques de sûreté de l'aviation existantes concernant l'inspection-filtrage des bagages de cabine, et ils ont déterminé que la composante de l'équipement d'inspection-filtrage destiné à la détection constituait un système et une source d'informations essentiels (à l'appui d'une fonction critique de l'aviation) et devrait faire l'objet d'une évaluation des cyberrisques.
- Des experts en sûreté de l'aviation ont réalisé une évaluation des risques pour la sûreté concernant les PBIED (portés par la personne ou placés dans des bagages de cabine) et n'ont pris en compte que cette dernière méthode dans le cadre du présent exercice d'évaluation.
- À l'issue de discussions avec des experts en sûreté de l'aviation, les experts en cybersécurité ont déterminé que « la falsification des données de la composante de détection dans le but de modifier les résultats du processus automatisé d'inspection-filtrage » constituait un scénario de cybermenace à évaluer et à intégrer dans l'évaluation des risques pour la sûreté de l'aviation présentée ci-dessus.
- Vecteur d'attaque : cette attaque pourrait être menée par une interférence avec les capacités de détection des équipements en accédant physiquement ou à distance à l'équipement en question.

- En se basant sur l'exemple de catégorisation des cybermenaces figurant dans l'appendice C (voir la version en diffusion restreinte du présent document), cette cybermenace peut être classée comme suit :
  - Domaine : Aéroport.
  - Fonction : Sûreté.
  - Sous-fonction : Inspection-filtrage des bagages de cabine.
  - Cybermenace : Altération (interférence avec les logiciels ou les systèmes de détection).

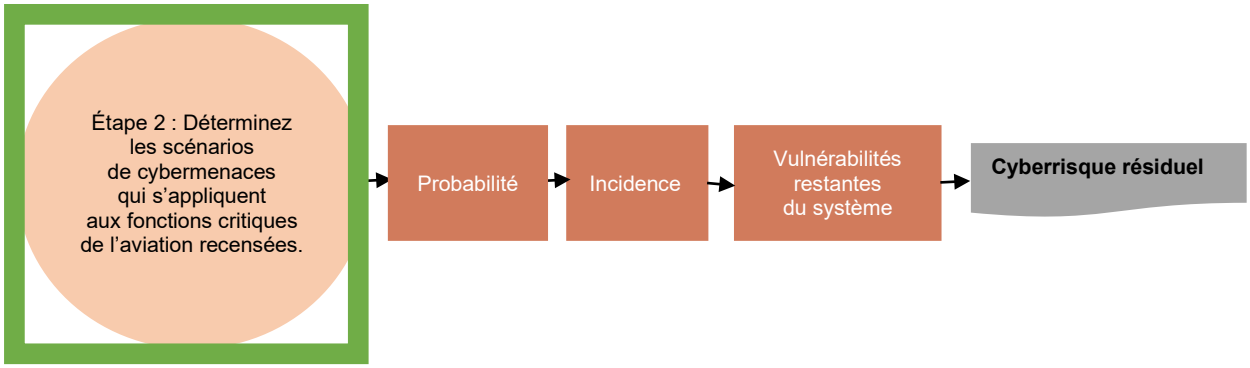
APPLICATION DE LA MÉTHODE ÉTAPE PAR ÉTAPE



⇨ Des experts en sûreté de l'aviation ont travaillé avec des experts en cybersécurité pour examiner les évaluations des risques de sûreté existants concernant les PBIED dans les bagages de cabine, et ils ont déterminé que la composante de détection de l'équipement d'inspection-filtrage constituait un système et une source d'informations qui venaient à l'appui de la fonction critique devant faire l'objet d'une évaluation des cyberrisques.

⇨ Les experts en sûreté de l'aviation ont réalisé la première évaluation des risques posés par les PBID sans cause liée aux cyberrisques. Le scénario de sûreté de l'aviation lié à notre scénario de cybermenace est le suivant : « article interdit apporté à bord par un passager dans l'intention de détruire l'aéronef ».

⇨ **Le résultat de ce processus est d'obtenir le risque résiduel de sûreté pour le scénario ci-dessus.**



⇨ En collaboration avec des experts en sûreté de l'aviation, des experts en cybersécurité ont déterminé que « la falsification des données de la composante de détection dans le but de modifier les résultats du processus d'inspection-filtrage » constituait un scénario de cybermenace plausible devant être évalué et intégré dans l'évaluation des risques pour la sûreté de l'aviation présentée ci-dessus.

⇨ L'évaluation des cyberrisques a été réalisée par les experts en cybersécurité de l'État en collaboration avec des experts en sûreté de l'aviation. Les experts en cybersécurité connaissent les méthodes avérées et les vecteurs d'attaque de la cyberattaque, tandis que les experts en sûreté de l'aviation connaissent l'équipement et ses niveaux de tolérance.

Les composantes de l'évaluation des cyberrisques de l'étape 2 sont élargies pour inclure les étapes suivantes :

Les étapes suivantes ont été prises pour effectuer l'évaluation des cyberrisques dans le domaine de la sûreté de l'aviation afin d'établir la matrice des cyberrisques :

⇨ **Probabilité :**

- Les experts en sûreté de l'aviation et les experts en cybersécurité utilisent souvent des tableaux de probabilité comportant des valeurs discrètes (comme le tableau 1 du chapitre 2), qui facilitent l'harmonisation de la compréhension des différentes composantes de risque.
- La capacité d'exécuter la cyberattaque évaluée nécessiterait une préparation minutieuse.
- Une attaque externe est difficile à mener, car l'équipement d'inspection-filtrage est soit autonome (non connecté à un réseau), soit connecté à un réseau local fermé, et nécessiterait beaucoup d'efforts et de connaissances techniques pour modifier le résultat du processus d'inspection-filtrage.
- Une menace interne est possible, mais il faudrait beaucoup d'efforts et de savoir-faire pour modifier le résultat du processus d'inspection-filtrage, par exemple :
    - Connaissance détaillée de l'aéroport, des points d'inspection-filtrage, des horaires, etc.
    - Haut niveau de coopération (l'attaque ne peut pas être menée sans aide).
    - Accès aux machines et/ou au réseau local.
- Il y a actuellement des preuves de l'intention.
- Par conséquent, la probabilité de la cybermenace a été fixée à 3, ce qui est MOYEN (c'est-à-dire qu'un scénario est dans l'ensemble plausible, et qu'il y a des preuves d'intention et de capacité et peut-être quelques exemples).

⇨ **Incidence/Conséquence/Effet :**

- L'évaluation de l'incidence implique une évaluation d'un scénario raisonnable le plus défavorable, ce qui signifie en l'occurrence que la cyberattaque a réussi.
- Il découlerait de la cyberattaque que l'équipement d'inspection-filtrage produise des résultats erronés, ce qui risque potentiellement de laisser passer des articles interdits. Cela pourrait entraîner la destruction de l'aéronef, des centaines de morts, dont certains éventuellement au sol. Une autre conséquence serait celle des coûts immédiats très élevés et des répercussions économiques à long terme. L'impact serait donc ÉLEVÉ (score de 5).

⇨ **Vulnérabilité :**

- L'évaluation des vulnérabilités est effectuée en tenant compte des mesures d'atténuation existantes.
- En ce qui concerne les mesures d'atténuation existantes :
    - L'État a rendu obligatoire l'application des normes et pratiques recommandées (SARP) de l'Annexe 17 – *Sûreté de l'aviation* sur l'inspection-filtrage des passagers à l'aide des systèmes de détection installés par l'aéroport.
    - L'État exige également de ses exploitants qu'ils mettent en œuvre la norme 4.9.1 et la pratique recommandée 4.9.2 relatives à la lutte contre les cybermenaces ; l'aéroport met donc en œuvre les mesures suivantes :
        - Il existe une séparation logique[20] ou physique entre les réseaux informatiques et les infrastructures commerciales et opérationnelles.
        - Des vérifications des antécédents du personnel sont effectuées et des mesures de sûreté de l'aviation sont en place pour protéger l'accès à l'équipement.

20. Une séparation logique consiste en une segmentation du réseau en zones logiques (virtuelles) sur le même réseau physique ou matériel.

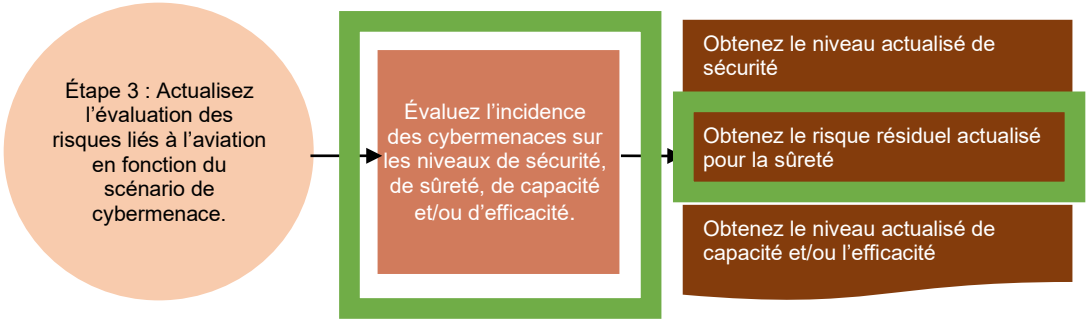
- Les experts en cybersécurité ont confirmé que les mesures de contrôle déjà en place sont satisfaisantes pour atténuer le cyberrisque. Cependant, comme les experts en sûreté de l'aviation sont conscients que les mesures obligatoires mises en œuvre par l'aéroport ne sont pas appliquées de manière cohérente à l'échelle mondiale (en particulier celles liées aux pratiques recommandées), il a été convenu de noter que la vulnérabilité est MOYENNE-FAIBLE (0,4).

⇨ **Cyberrisque résiduel :**

- Le cyberrisque résiduel peut désormais être calculé en multipliant les scores de probabilité, d'incidence et de vulnérabilité : **3 x 5 x 0,4 = 6, ce qui entraîne un risque résiduel de niveau MOYEN-FAIBLE**.

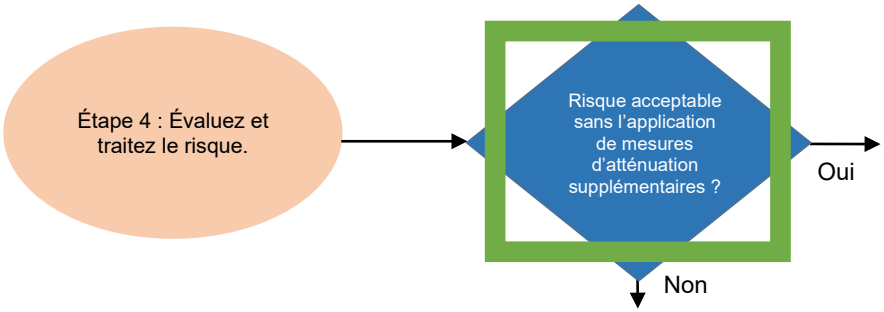
La matrice des cyberrisques est modifiée comme suit :

MATRICE DES CYBERRISQUES					
Scénario	**Probabilité**	**Incidence**	**Stratégies d'atténuation**	**Vulnérabilités**	**Risque résiduel**
Article interdit transporté à bord par un passager dans l'intention de détruire l'aéronef, en modifiant les résultats de l'équipement d'inspection-filtrage de sûreté.	**Score de 3** MOYEN Un adversaire en est-il capable ? Y a-t-il un intérêt à attaquer une cible de l'aviation civile ?	**Score de 5** ÉLEVÉ Dans le scénario le plus défavorable, quelles seront les pertes en vies humaines ? Des dommages aux infrastructures sont-ils à prévoir ? La confiance du public dans le transport aérien va-t-elle s'effriter ? Quel est le coût économique ?	La norme 4.9.1 et la pratique recommandée 4.9.2 de l'Annexe 17 s'appliquent à l'inspection-filtrage des passagers au moyen de systèmes de détection.	**Score de 0,4** MOYEN-FAIBLE En tenant compte des mesures d'atténuation actuelles, quel est le degré de vulnérabilité de l'aviation face à ce scénario de menace ?	**Score de 6** Ce score sera comparé aux scores des autres scénarios de menace et utilisé pour classer les menaces.



⇨ Une fois que la cybermenace a été reclassée en cyberrisque correspondant aux objectifs de sûreté de l'aviation, l'évaluation initiale des risques pour la sûreté de l'aviation peut être mise à jour, y compris l'évaluation de la cybermenace, qui est désormais prise en compte dans la matrice des risques pour la sûreté de l'aviation du scénario en question, conduisant potentiellement à un nouveau risque résiduel pour la sûreté.

⇨ Cela servira de base aux prochaines étapes, à savoir l'évaluation et le traitement des risques.



⇨ Avec ces données, l'État actualisera sa matrice des risques PBIED pour prendre en compte ce modus operandi.

L'évaluation devrait aboutir à une décision : **le risque peut-il être accepté tel quel, ou conviendrait-il de mettre en œuvre des mesures d'atténuation des cyberrisques en plus des contrôles existants ?**

⇨ Il a été conclu que le cyberrisque résiduel était trop faible pour justifier que l'évaluation initiale soit modifiée, et que, par conséquent, le risque résiduel du scénario de menace global de type PBIED n'était pas touché par ce scénario de cybermenace (c'est-à-dire que la menace pour la sûreté de l'aviation reste au même niveau élevé).

⇨ Les experts en cybersécurité étaient également satisfaits des mesures de contrôle mises en place pour soutenir l'intégrité du processus d'inspection-filtrage.

⇨ Cependant, les experts en cybersécurité ont noté que si l'équipement devait être modifié, il faudrait de nouveau le faire certifier par l'autorité compétente, ce qui pourrait exposer le système à de futures cybermenaces en cas d'incapacité à corriger à temps les vulnérabilités découvertes. À ce titre, un projet a été lancé pour trouver le juste milieu entre la certification et la mise à jour des mesures de contrôle de cybersécurité appliquées à l'équipement d'inspection-filtrage, et les résultats du projet ont été consignés en tant que mesure d'atténuation supplémentaire pour une mise en œuvre future à l'appui de l'atténuation des cyberrisques.

⇨ La matrice des cyberrisques mise à jour pour ce scénario est donc la même que celle de la matrice des cyberrisques qui suit.

MATRICE DES CYBERRISQUES

Scénario	Probabilité	Incidence	Stratégies d'atténuation	Vulnérabilités	Risque résiduel	Stratégies d'atténuation supplémentaires
Article interdit transporté à bord par un passager dans l'intention de détruire l'aéronef, en modifiant les résultats de l'équipement d'inspection-filtrage de sûreté.	**Score de 3** MOYEN Un adversaire en est-il capable ? Y a-t-il un intérêt à attaquer une cible de l'aviation civile ?	**Score de 5** ÉLEVÉ Dans le scénario plausible le plus défavorable, quelles seront les pertes en vies humaines ?	La norme 4.9.1 et la pratique recommandée 4.9.2 de l'Annexe 17 s'appliquent à l'inspection-filtrage des passagers au moyen de systèmes de détection.	**Score de 0.4** MOYEN-FAIBLE En tenant compte des mesures d'atténuation actuelles, quel est le niveau de vulnérabilité de l'aviation face à ce scénario de menace ?	**Score de 6** Ce score sera comparé aux scores d'autres scénarios de menace et utilisé pour éliminer les menaces.	Élaboration de processus visant à accorder une attention égale à la correction des vulnérabilités et à la nouvelle certification de l'équipement d'inspection-filtrage des bagages à main.

MATRICE DES CYBERRISQUES						
Scénario	**Probabilité**	**Incidence**	**Stratégies d'atténuation**	**Vulnérabilités**	**Risque résiduel**	**Stratégies d'atténuation supplémentaires**
		Des dommages aux infrastructures sont-ils à prévoir ? La confiance du public dans le transport aérien va-t-elle s'effriter ? Quel est le coût économique ?				

CONCLUSION

L'approche étape par étape présentée dans cet exemple illustre comment la sûreté de l'aviation et les évaluations de cyberrisques doivent être interconnectées pour contribuer à résoudre les cybermenaces et les cyberrisques pour l'aviation civile. Dans un environnement réel, ce processus se déroulerait de manière plus itérative et plus intégrée, en fonction de la structure de gouvernance de l'organisation ou de l'État et des cadres réglementaires ou juridiques en place.

— FIN —

ISBN 978-92-9275-950-6