



SAFE SKIES.
**SUSTAINABLE
FUTURE.**





Cadre réglementaire de l'OACI - Cybersécurité de l'aviation

Philippe MORIO

DAKAR, le 09 Juin 2026

Expert en cybersécurité ATB
Organisation de l'aviation civile internationale (OACI)

Ordre du jour

- **01 L'OACI et l'aviation civile**
- **02 Pourquoi la cybersécurité dans l'aviation ?**
- **03 Le cadre réglementaire de l'OACI**
- **04 La stratégie et le plan d'action en matière de cybersécurité**
- **05 Gouvernance, formation et matériels d'orientation**

01 L'OACI et l'aviation civile

OACI — Organisation de l'aviation civile internationale

- **Agence spécialisée des Nations Unies** créée en 1947 (Convention de Chicago de 1944)
- **193** États membres
- Assemblée, Conseil, Commission, Comités assistés par le Secrétariat
- Élaboration de conventions, protocoles, résolutions, normes et pratiques recommandées (SARPs) à l'intention des États
- Audits des États
- Fourniture d'une assistance, d'une formation et d'un renforcement des capacités aux États



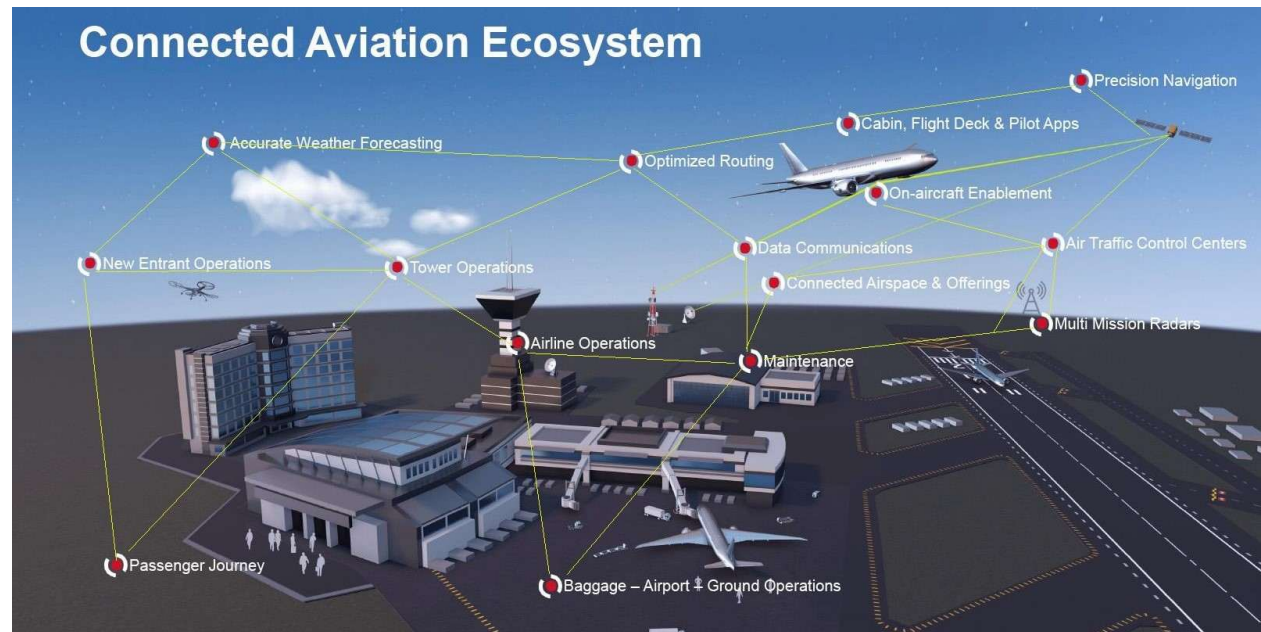
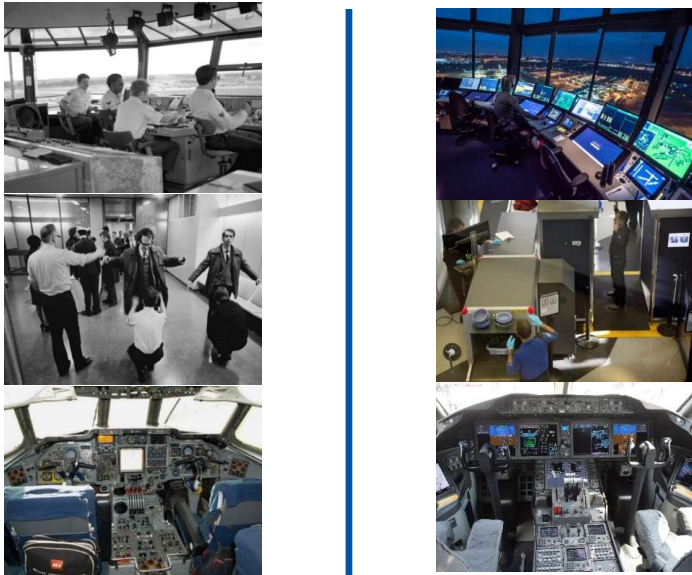
02

Pourquoi la cybersécurité ?

Pourquoi la cybersécurité dans l'aviation civile ?

7

Impact de la technologie

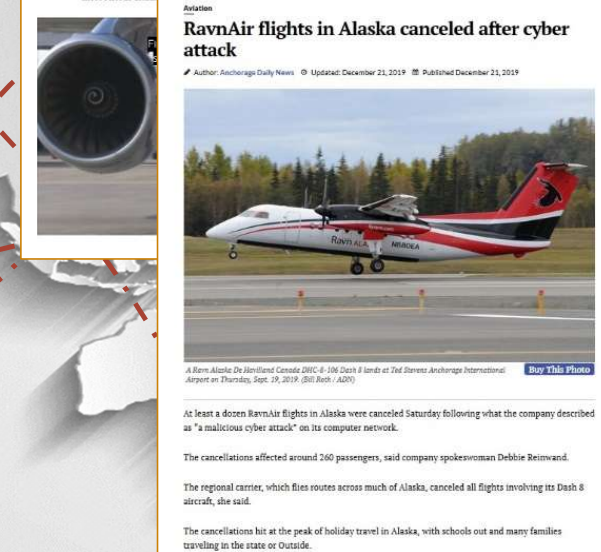
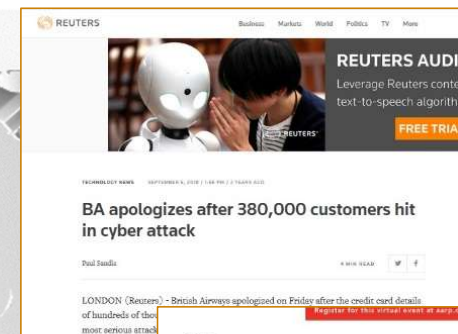


La technologie facilite la croissance du transport aérien tout en améliorant sa sécurité, sa sûreté, son efficacité, sa capacité et sa durabilité.

Cependant,
L'interconnexion et la digitalisation des systèmes de l'aviation entre les différents acteurs augmentent la surface d'attaque de l'aviation.



Pourquoi la cybersécurité dans l'aviation civile ?



Pourquoi la cybersécurité dans l'aviation civile ?

Les efforts visant à traiter la cybersécurité de l'aviation doivent être :

- Cohérents
- Clairs
- Harmonisés
- Fiables
- Transversaux à tous les domaines de l'aviation
- En phase avec les priorités mondiales
- Coordonnés avec les parties prenantes concernées hors du secteur de l'aviation



Comprehension de Cybersécurité de l'aviation

11

Intersectoriel



“The process of protecting information by preventing, detecting, and responding to attacks”



“The preservation of confidentiality, integrity and availability of information in the cyberspace”

Aviation



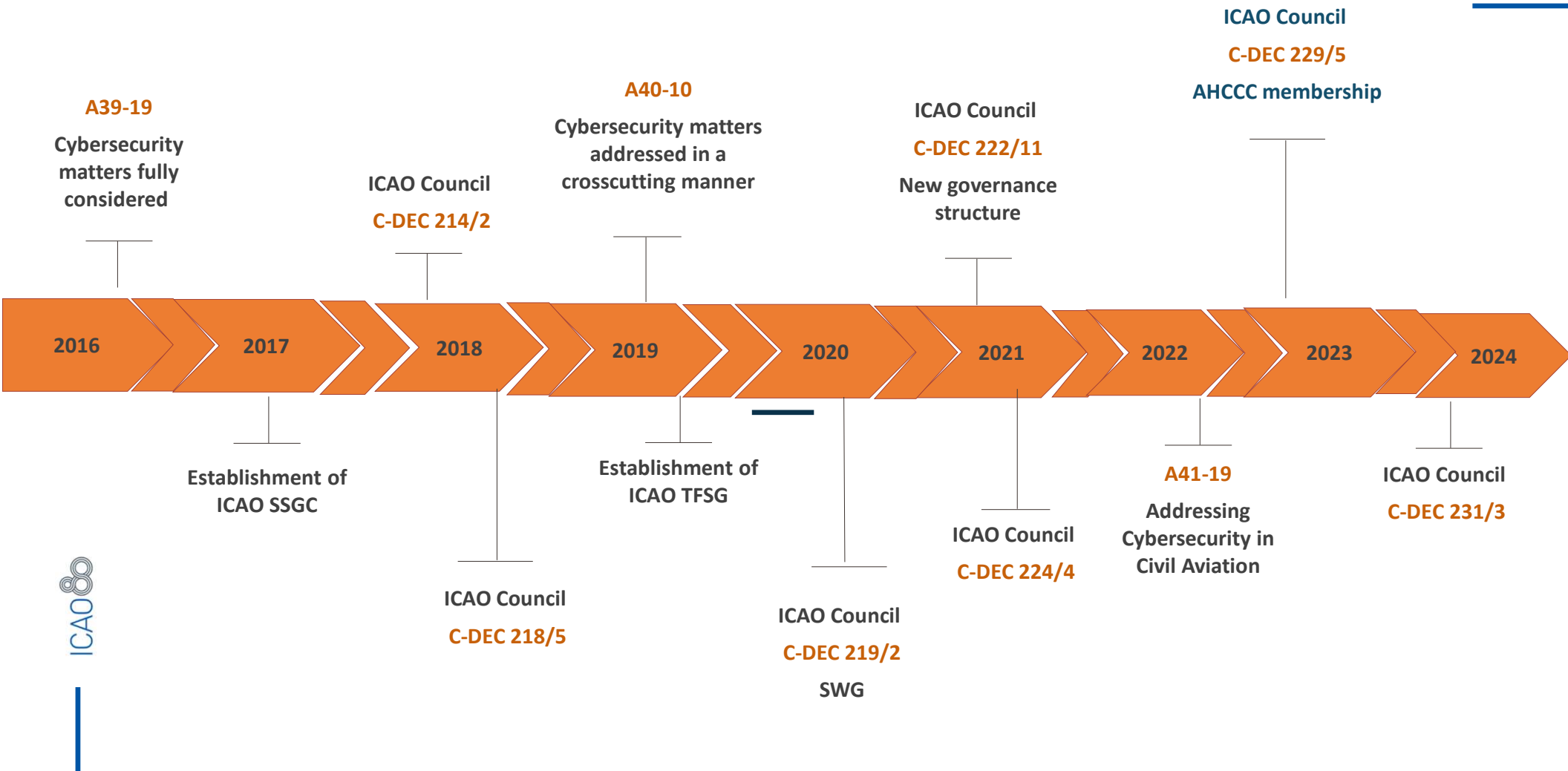
The body of technologies, controls and measures, processes, procedures and practices designed to ensure confidentiality, integrity, availability, and overall protection and resilience of cyber assets from attack, damage, destruction, disruption, unauthorized access, and/or exploitation

03

Le cadre réglementaire de l'OACI

ICAO Cybersecurity Governance Timeline

13



Les travaux de l'OACI sur la cybersécurité et la cyber-résilience de l'aviation

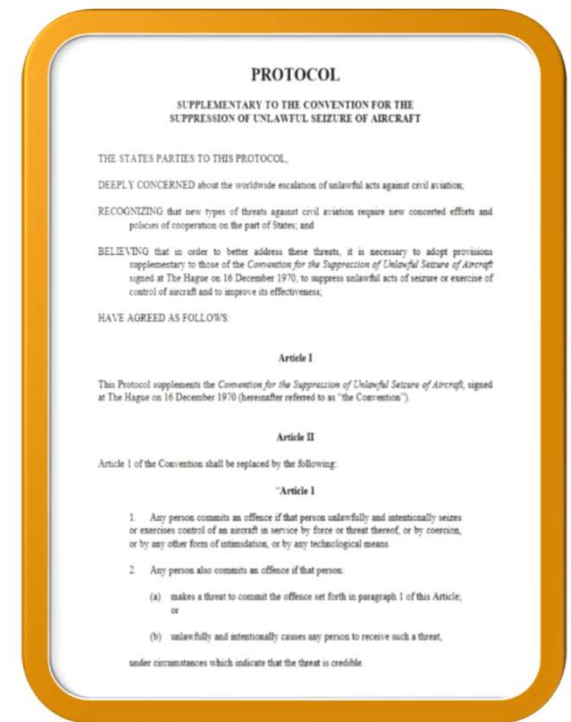
➤ Instruments juridiques :

- La Convention de Pékin et le Protocole de Pékin de 2010



Les travaux de l'OACI sur la cybersécurité et la cyber-résilience de l'aviation

L'adoption des Instruments de Pékin par les gouvernements constitue un important
FACTEUR DE DISSUASION des cyberattaques contre l'aviation civile



Les travaux de l'OACI sur la cybersécurité et la cyber-résilience de l'aviation

Beijing Convention 2010

- Defines **air navigation facilities to include signals, data, information or systems**.
- Such facilities could be directly applicable to cyber means of carrying an attack.

Beijing Protocol 2010

- Broadens scope to **aircraft in service** instead of in flight, adds **or by any technological means** to Article 1.
- No requirement for the offender to be on board.

Les travaux de l'OACI sur la cybersécurité et la cyber-résilience de l'aviation

➤ **Instruments juridiques :**

- La Convention de Pékin et le Protocole de Pékin de 2010

➤ **Normes et pratiques recommandées :**

- Annexe 17 – Sûreté de l'*aviation* : Norme 4.9.1 et Pratique recommandée 4.9.2



Les travaux de l'OACI sur la cybersécurité et la cyber-résilience de l'aviation

Annexe 17 à la Convention de Chicago – Sûreté de l'*aviation*

➤ Norme 4.9.1

- Chaque État contractant veille à ce que les exploitants ou entités — tels que définis dans le programme national de sûreté de l'aviation civile ou d'autres documents nationaux pertinents — programme utilisés à des fins d'aviation civile et, conformément à une évaluation des risques, élaborent et mettent en œuvre, selon que de besoin, des mesures visant à les protéger contre toute intervention illicite..

➤ Pratique recommandée 4.9.2

- Recommandation— *Chaque État contractant devrait veiller à ce que les mesures mises en œuvre protègent, selon que de besoin, la confidentialité, l'intégrité et la disponibilité des systèmes critiques identifiés et/ou des données. Les mesures devraient comprendre, entre autres, la sécurité dès la conception, la sécurité de la chaîne d'approvisionnement, la séparation des réseaux, ainsi que la protection et/ou la limitation des capacités d'accès à distance, selon que de besoin et conformément à l'évaluation des risques effectuée par les autorités nationales compétentes.*

ICAO Universal Security Audit Programme (USAP)



- **Évaluation** de la sûreté de l'aviation dans les États contractants de l'OACI.
- **Audit** des capacités de supervision de la sûreté de l'aviation des **États**.
- **Audit** des mesures de sûreté dans **des aéroports sélectionnés**.



ICAO Universal Security Audit Programme (USAP)

Mise en œuvre de la Norme 4.9.1 de l'Annexe 17 – *Sûreté de l'aviation*

- 54 États — Audits documentaires de la préparation à la cybersécurité :
 - 15 % — Aucune exigence imposant aux entités d'identifier leurs infrastructures critiques et d'élaborer, conformément à une évaluation des risques, des mesures de protection de ces infrastructures critiques.
 - 26 % — Absence de définition des responsabilités des entités en matière de cybersécurité de l'aviation.
 - 41 % — Absence de critères pour la protection des infrastructures critiques contre les interventions illicites.
- 35 États — Audits sur site :
 - 60 % — Absence de mise en œuvre de mesures de cybersécurité cohérentes et efficaces.



Programme universel d'audits de sûreté Programme (USAP)

Mise en œuvre de la Norme 4.9.1 de l'Annexe 17 – *Sûreté de l'aviation*

➤ **Raisons possibles** du faible niveau de mise en œuvre des obligations en matière de cybersécurité de l'aviation (liste non exhaustive) :

- Manque de savoir-faire.
- Manque de ressources.
- Les travaux sont **menés par une autorité nationale compétente distincte** en matière de cybersécurité, mais **sans coordination efficace** avec l'autorité nationale de l'aviation civile.



Les travaux de l'OACI sur la cybersécurité et la cyber-résilience de l'aviation



➤ Instruments juridiques :

- La Convention de Pékin et le Protocole de Pékin de 2010

➤ Normes et pratiques recommandées :

- Annexe 17 – Sûreté de l'*aviation* : Norme 4.9.1 et Pratique recommandée 4.9.2

➤ Résolutions de l'Assemblée :

- Résolutions A39-19, A40-10, A41-19 et A42-19 sur la cybersécurité

Les travaux de l'OACI sur la cybersécurité et la cyber-résilience de l'aviation

OACI 40^e Résolution A40-10 de l'Assemblée : *Traitement de la cybersécurité dans l'aviation civile*

- Reconnaît que le risque de cybersécurité peut simultanément affecter un large éventail de domaines ;
- Réaffirme les obligations des États en vertu de la Convention de Chicago ;
- Souligne la nécessité d'une adoption et d'une mise en œuvre universelles à l'échelle mondiale de la Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale (Convention de Pékin) et du Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs (Protocole de Pékin) ;
- Reconnaît la nécessité pour la cybersécurité de l'aviation d'être harmonisée ; et
- Demande aux États de mettre en œuvre la Stratégie de cybersécurité.

Les travaux de l'OACI sur la cybersécurité et la cyber-résilience de l'aviation

OACI 41^e Résolution A41-19 de l'Assemblée : *Traitement de la cybersécurité dans l'aviation civile*

- Invite les Etats à désigner l'autorité compétente pour les questions liées à la cybersécurité de l'aviation dans le cadre du plan national de cybersécurité de l'aviation et définir les rapports entre cette autorité et les organismes aéronautiques et non aéronautique nationaux concernés;
- Invite les Etats à définir les responsabilités des organismes nationaux et des parties prenantes du secteur en ce qui concerne la cybersécurité de l'aviation civile ;
- Invite les Etats à obtenir des ressources suffisantes pour garantir la disponibilité et la formation continue de professionnels de l'aviation et de la cybersécurité qualifiés et compétents

Les travaux de l'OACI sur la cybersécurité et la cyber-résilience de l'aviation

OACI 42^e Résolution A42-19 de l'Assemblée : *Traitement de la cybersécurité dans l'aviation civile*

- Prie instamment les États membres d'adopter, de ratifier et de mettre en œuvre la Convention de Pékin;
- Réaffirme les obligations des États en vertu de la Convention de Chicago ;
- Invite les états a mettre en œuvre la Stratégie de cybersécurité de l'aviation civile de l'OACI et s'appuyer sur le Plan d'action pour la cybersécurité de l'OACI afin de faciliter la mise en œuvre de la Stratégie;
- Invite les Etats à développer les mécanismes de coopération avec les autorités nationales compétentes, notamment les forces de l'ordre et les autorités chargées de la cybersécurité, afin de recenser, protéger et surveiller les vulnérabilités et les flux susceptibles de porter atteinte aux systèmes de l'aviation civile,.

04

Stratégie et
plan d'action

01 | La Convention de Chicago (1944) – Socle du Droit Aérien

Convention relative à l'Aviation Civile Internationale (Chicago, 1944)

Art. 33

Reconnaissance des navigabilités et licences

Art. 37

Adoption de normes et pratiques recommandées (SARPs) via les Annexes

Art. 44

Objectifs de l'OACI : promouvoir la sécurité de vol dans la navigation aérienne internationale

Annexes

19 Annexes à la Convention – force contraignante pour les États membres

Cyberlink

Pas de mention explicite «cyber» – mais application étendue via Annexes 17 & 19

Faits Clés

193 États membres
(presque universel)

19 Annexes
techniques

SARPs : force
contraignante

Dérogations possibles
(Article 38)

Révisée régulièrement
par l'Assemblée

Principe fondamental : la cybersécurité en aviation n'est pas une fin en soi – elle est un enabler de la safety et de la continuité des opérations aériennes internationales.

ICAO Assembly Resolutions on Aviation Cybersecurity

A41-19 : Traitement de la cybersécurité dans l'aviation civile

Adoption mondiale



Instruments de Pékin

Coopération



National, Regional and Global States and Industry

Mise en œuvre



Stratégie et Plan d'action de l'OACI

Gouvernance



Définir les responsabilités, identifier l'autorité compétente...

Autres



Cadre de gestion des risques, culture de cybersécurité...

ICAO

PROVISIONAL EDITION
OCTOBER 2022

RESOLUTIONS
ADOPTED BY THE ASSEMBLY



ASSEMBLY – 41st SESSION
Montréal, 27 September–7 October 2022

INTERNATIONAL CIVIL AVIATION ORGANIZATION

<https://www.icao.int/aviationcybersecurity/Documents/A41-19.pdf>

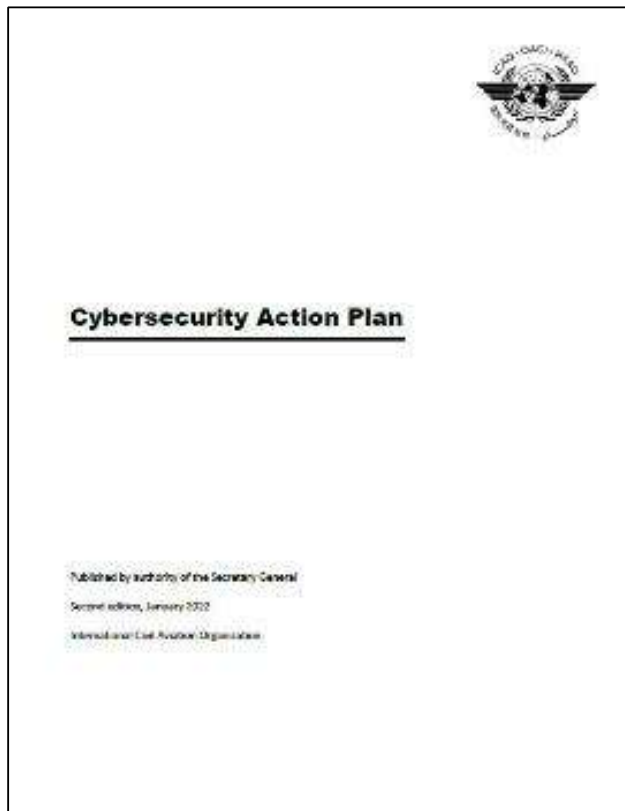


The 7 Pillars of the ICAO Cybersecurity Strategy

- International Cooperation
- Governance
- Effective Legislation and Regulation
- Cybersecurity Policy
- Information Sharing
- Incident Management & Emergency Planning
- Capacity Building, Training and Cybersecurity Culture

Plan d'action pour la cybersécurité

30



First Edition
published in
November 2020



Second Edition published
in January 2022



Available on ICAO
Public Website



Provides the Foundation
for ICAO, States and
stakeholders to work
together



Develops the **7 Pillars** of the Aviation
Cybersecurity Strategy into **32 Priority Actions**,
which are further broken down into **51 Tasks** to be
implemented by ICAO, States, and Stakeholders

<https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx>

05 | Cybersecurity Action Plan (CyAP) – Structure et Actions

Le CyAP décline la Stratégie en actions concrètes pour les États et l'industrie

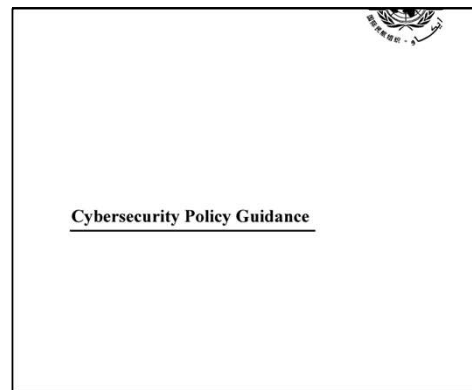
CyAP 0	ÉLABORER UNE VISION MONDIALE CONCERTÉE	• élaborer une vision exhaustive et concerté	• modèle de politique de cybersécurité	• mis en œuvre la Stratégie pour la cybersécurité de l'aviation de l'OACI
CyAP 1	RÉALISER LA COOPÉRATION INTERNATIONALE	• Inclure la cybersécurité dans les programmes de supervision de la sécurité et de la sûreté de l'OACI	• recenser les initiatives et pratiques en matière de cybersécurité	• Planifier, organiser et soutenir des manifestations internationales et régionales
CyAP 2	DÉVELOPPER LA GOUVERNANCE ET LA TRANSPARENCE	• Établissement d'une structure de gouvernance	• principes généraux pour des systèmes de gestion adéquate de la cybersécurité de l'aviation civile	• Procédures de signalement des cyberincidents/nombre d'incidents signalés selon les procédures
CyAP 3	ÉLABORER UNE LÉGISLATION ET UNE RÉGLEMENTATION EFFICACES	• Nombre d'États ayant ratifié les instruments de Beijing.	• Examen et analyse des écarts des SARP de l'OACI	• Publication d'éléments indicatifs sur la cybersécurité de l'aviation civile.
CyAP 4	ÉLABORER UNE POLITIQUE DE CYBERSÉCURITÉ	• Campagne de sensibilisation	• Formulation d'une politique de sûreté du cycle de vie des systèmes d'aviation civile.	• Disponibilité de 10 scénarios de cyberrisques.

05 | Cybersecurity Action Plan (CyAP) – Structure et Actions

Le CyAP décline la Stratégie en actions concrètes pour les États et l'industrie

CyAP 5	RENFORCER LES CAPACITÉS DE PARTAGE D'INFORMATIONS	• élaborer une vision exhaustive et concerté	• modèle de politique de cybersécurité	• mis en œuvre la Stratégie pour la cybersécurité de l'aviation de l'OACI
CyAP 6	DÉVELOPPER LA GESTION DES INCIDENTS ET LA PLANIFICATION D'URGENCE	• Publication d'orientations pour les capacités d'intervention	• Publication d'une liste de cibles et de niveaux minimums acceptables de fonctionnalités pour la continuité de l'aviation.	• Partage des enseignements tirés, le cas échéant.
CyAP 7	DÉVELOPPER LE RENFORCEMENT DES CAPACITÉS, LA FORMATION ET UNE CULTURE DE LA CYBERSÉCURITÉ	• Intégration de la cybersécurité dans les stratégies NGAP	• Élaboration d'une formation appropriée et axée sur les rôles dans le domaine de l'aviation et de la cybersécurité	• Disponibilité de programmes de formation sur la cybersécurité dans l'aviation.

Matériel d'orientation sur la cybersécurité de l'aviation



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

Gestion des risques cybernétiques de l'aviation

34



"WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US, HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."



Doc 10213 — Restricted

Global Cyber Risk Considerations

(FIRST EDITION, 2025)

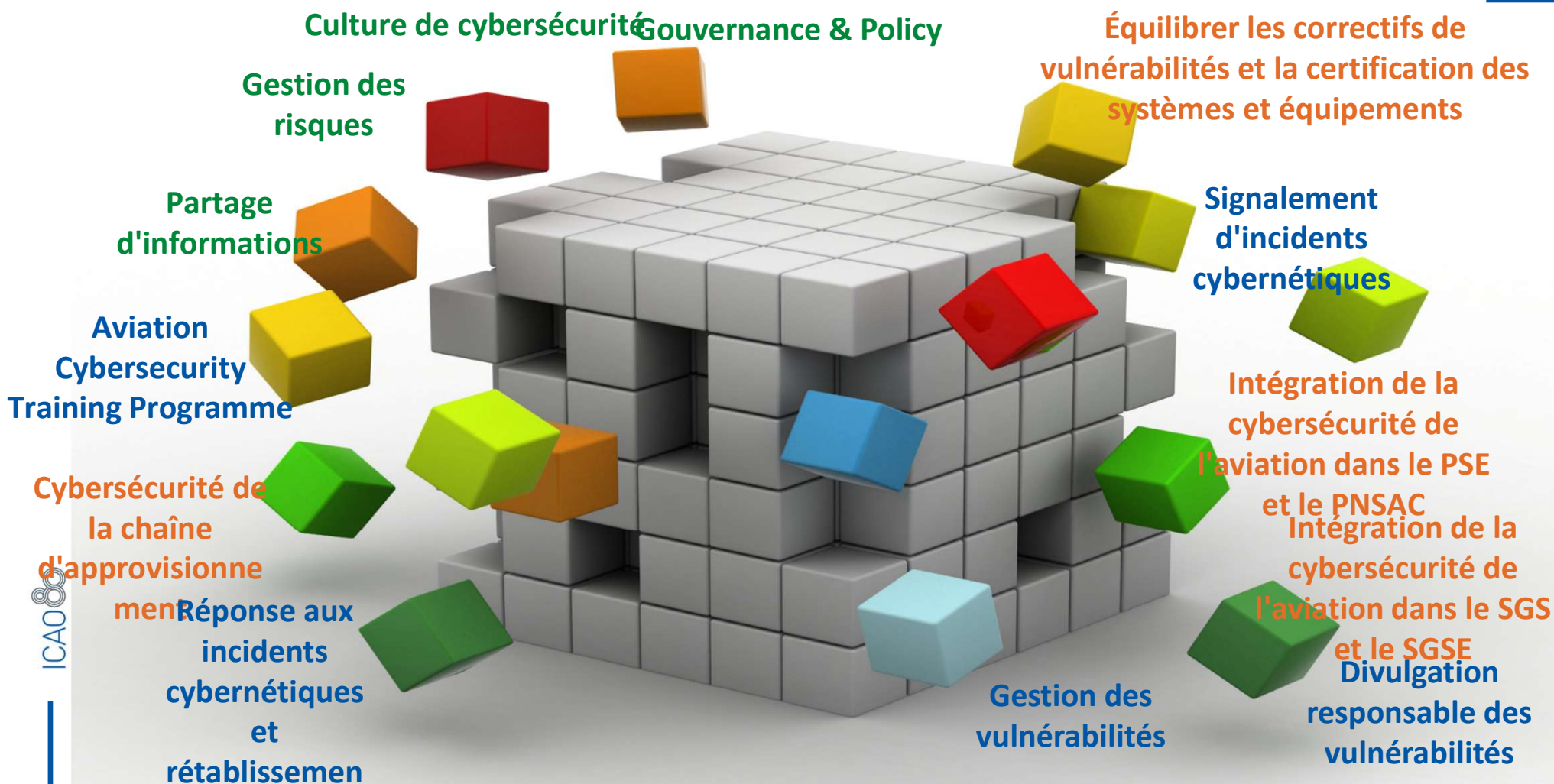
Approved by and published under
the authority of the Secretary General

First Edition — 2025

International Civil Aviation Organization

Matériel d'orientation en préparation

35



05 Gouvernance et formation et matériels

AHCCC Overview



Chairperson (Council)
Vice-Chairperson (ANC)

Membership:
14 Members

ATC
ASC
ANC
CYSECP
TFP
AVSECP
SMP

IMP
NSP
ATMRPP
RPASP
FALP
PTLP
CP-DCIWG



Qu'est-ce qu'est le AHCCC ?

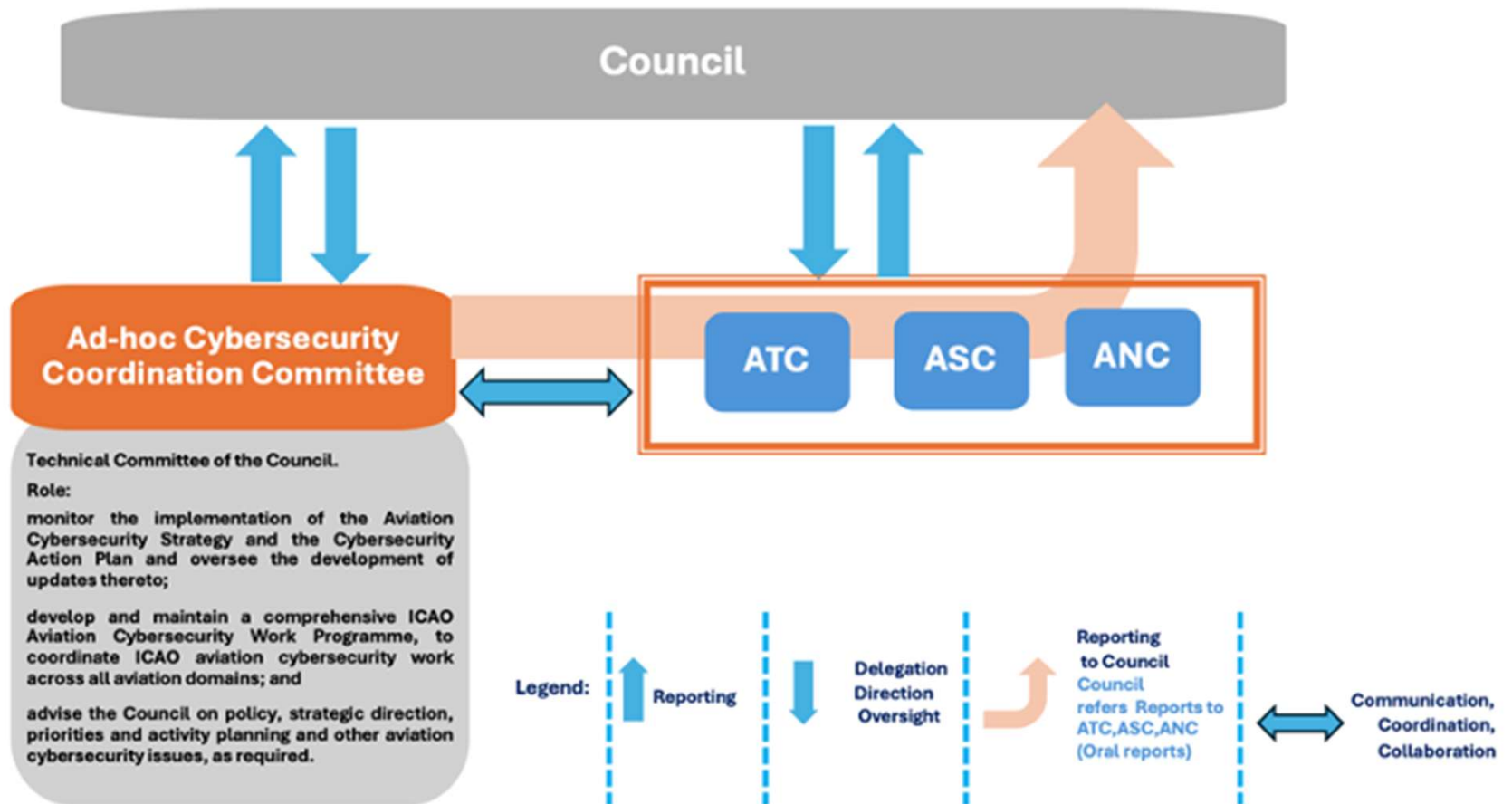
- Est un comité technique du Conseil
- Fournit au Conseil une vue complète des activités de cybersécurité
- Fournit des recommandations à l'ANC, ASC, ATC, via le Conseil incluant coordination et priorisation

Ce que n'est pas le AHCCC

- N'est pas un panel
- N'assigne pas de tâche
- N'est pas un organe décisionnel

Relation avec ATC, ASC, ANC et lignes de report

39



Ressources disponibles de renforcement des capacités de l'OACI

- Fondements du leadership en cybersécurité de l'aviation et gestion technique (avec l'Université aéronautique Embry-Riddle).

<https://www.enrole.com/erau/jsp/course.jsp?categoryId=5586BD00&courseId=SGC-1102>

- Aviation Cybersecurity Oversight (with UK CAAi)
<https://caainternational.com/course/icao-aviation-cybersecurity-oversight/>



Thank You

