AIX-MARSEILLE UNIVERSITE

FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

INSTITUT DE FORMATION UNIVERSITAIRE ET DE RECHERCHE
DU TRANSPORT AERIEN

« Cybersécurité et Cyber-résilience du transport aérien »

Mémoire pour l'obtention du

Master 2 Droit et Management du Transport Aérien

par

BOUTERBIAT Houssama

Sous la direction de

Mme Julie LABORDE DIT BOURIAT, codirectrice de l'IFURTA

Année universitaire 2019-2020

*"Où est passée la **VIE***
Que l'on a perdue en la vivant ?

*Où est passée la **SAGESSE***
Que l'on a perdue dans la connaissance ?

*Où est passée la **CONNAISSANCE***
Que l'on a perdue dans l'information ?"

T.S. Eliot (1888–1995)

F. Taddei ajouta[1]:

*"Où est passée l'**INFORMATION***
*Que l'on a perdue dans les **DATAS** ? »*

Il est encore temps de retrouver la vie, la sagesse et la connaissance que l'on a perdues.

[1] Dans l'excellent reportage de DATA GUEULE, Production Premières Lignes Télévision, « 2 degrés avant la fin du monde », 2015

REMERCIEMENTS

Tout d’abord, je voudrais remercier l’ensemble des intervenants et professeurs de l’IFURTA pour avoir partagé leur savoir et répondu à l’ensemble de mes interrogations qui pouvaient être parfois chronophages ;

Je tiens également à remercier l’équipe pédagogique de l’IFURTA. Malgré cette crise sanitaire, nous avons pu compter sur leur présence ainsi que leur bienveillance.

Je remercie ma compagne, Léa, pour son aide, ainsi que son soutien durant ces sept dernières années.

Je remercie mes parents, mes petites sœurs et mon petit frère pour leurs encouragements et leur présence.

Enfin, je tenais à remercier tout particulièrement ma directrice de mémoire Madame Julie Laborde Dit Bouriat, pour ses conseils, son aide, sa bienveillance, et aussi pour m’avoir donné l’opportunité de vivre cette année exceptionnelle.

SOMMAIRE

Abréviations et définitions

- **AAE** : Académie de l'Air et de l'Espace
- **ADP** : Aéroports de Paris
- **AESA** : Agence Européenne de la Sécurité Aérienne
- **ATM** : Air Traffic Management
- **CAMO** : Continuing Airworthiness Management Organisation
- **CERT-UE**: Computer Emergency Response Team Union European
- **CERT-FR**: Computer Emergency Response Team France
- **CICDE** : Centre Interarmées de Concepts, de Doctrine et d'Expérimentations
- **CCTA** : Conseil pour la Cybersécurité du Transport Aérien
- **CLUSIF** : Club de la Sécurité de l'Information Français
- **CESAM** : Le Comité des Assureurs Maritimes et Transport
- **DG CONNECT:** DG for Communications Networks Content and Technology
- **DG MOVE**: DG for Mobility and Transport
- **DSAC** : Direction de la sécurité de l'Aviation Civile
- **DGAC :** Direction Générale de l'Aviation Civile
- **ENISA :** Agence Européenne chargée de la sécurité des réseaux de l'information
- **ECCSA:** European Centre for Cyber Security in Aviation
- **EATMN:** European Aviation Traffic Management Network
- **FAA:** Federal Aviation Administration
- **FSN:** Fournisseurs de service numérique
- **FMS:** Flight Management system
- **GAsep:** The Global Aviation Security Plan
- **IoT:** Internet of Things
- **IATA** : International Air Transport Association
- **LPM :** Loi de Programmation Militaire

- **MCAS:** Maneuvering Characteristics Augmentation System
- **NTIC :** Nouvelles Technologies de l'Information et de la Communication
- **NIS:** Network and Information System Security
- **NPA:** Notice of Proposed Amendment
- **OACI**: Organisation de l'Aviation Civile Internationale
- **ODS:** Operational Display System
- **ONU:** Organisation des Nations Unies
- **OSE:** Opérateurs de services essentiels
- **OIV:** Opérateurs d'Importance Vitale
- **PNR:** Passenger Name Record
- **QR CODE:** Quick Response Code
- **RADAR:** Radio Detection and Ranging
- **RGPD** : Règlement Général sur la protection des données
- **SARPS** : Standards and Recommended Practices
- **SGS :** Système de Gestion de la Sécurité
- **TIC :** Technologies de l'Information et de la Communication

Cyber : *Qui implique ou qui fait référence à l'utilisation des technologies de l'information*

Cybersécurité : *La cybersécurité consiste à réduire le risque d'atteinte à des infrastructures par des moyens physiques ou mesures de cyberdéfense contre des attaques et des incidents, dans le cadre de l'utilisation de systèmes d'information et de communication*

Cyber résilience : *La cyber résilience est la capacité à préparer et à s'adapter à des conditions changeantes, de résister et de récupérer rapidement suite aux perturbations subies du fait d'attaques ou d'incidents. La résilience est de la gestion de risque. La notion de cyber résilience est plus transversale que la notion de cybersécurité, cantonnée au domaine technique d'information. La cyber résilience est une approche globale du risque cyber impliquant le facteur humain et les techniques d'informations dans une vision à court, moyen et long terme, préventive et corrective.*

Cyber risque : *Aléa qui implique les technologies de l'information et qui est susceptible de produire des dommages immatériels et matériels. Le cyber risque est complexe, protéiforme et d'une évolution constante. Il est donc possible d'utiliser la notion au pluriel ou au singulier de façon indifférente.*[2]

[2] Inspiré et retravaillé à partir du mémoire de Roxanne DESLANDES, Présentation des programmes de cyberassurances et leurs limites

INTRODUCTION

Paragraphe 1 : La cybersécurité, un risque d'actualité

« Croire que le transport aérien est à l'abri de la menace cyber revient à se voiler la face. C'est un sujet sérieux auquel nous devons nous attaquer » a affirmé en 2016, Patrick Ky, directeur de l'Agence Européenne de Sécurité Aérienne AESA[3].

Patrick Ky annonça ceci à la suite d'une démonstration d'un piratage d'un système avionique lors d'une session à l'OACI[4]. Pour comprendre pourquoi un directeur d'une grande agence européenne a dû agir afin de démontrer à une assemblée ce qui semble aujourd'hui admis, il faut remonter un an en arrière, en 2015 et se pencher sur l'histoire du hacker qui avait prétendu pouvoir pirater un avion[5]. Cet hacker, Christ Robert, avait laissé les experts de l'époque dubitatifs. En effet, pour beaucoup d'entre eux le piratage d'un avion était impossible, les systèmes de communication avionique étant totalement sûrs à leurs yeux.

Patrick Ky, face au monde aérien perplexe, a dû démontrer à l'OACI que le hackeur avait raison. Nous sommes lors d'une session sur la cybersécurité en 2016 et pour un grand nombre d'experts un système avionique ne peut être piraté. Les exploits du prétendu hacker ne sont que de la poudre aux yeux. C'est alors qu'en pleine discussion, Patrick Ky fit entrer un employé de l'AESA avec un ordinateur,

[3] Organisme européen chargé de la sécurité du transport aérien, nous définirons plus en détail son rôle et objectif à la suite du mémoire
[4] Organisation Onusienne de l'Aviation Civile internationale, nous définirons plus en détail son rôle et objectif à la suite du mémoire
[5] https://www.europe1.fr/technologies/un-hacker-a-reussi-a-pirater-un-avion-de-ligne-942376

ainsi qu'une licence de pilote. Devant un public qui n'en croyait pas ses yeux, et en direct, l'employé de l'AESA expliqua qu'il avait réussi à pénétrer le système d'un avion au sol. Deux jours plus tard, Patrick Ky démontra qu'il pouvait envoyer des messages à cet avion. A la suite de cette extraordinaire démonstration, toute l'assemblée avait pris conscience de la menace en matière de cyber sécurité sur le transport aérien.

Juin 2020, dans les bureaux d'easy jet, la direction des systèmes informatiques se rend compte d'un drame absolu[6]. Il se passe quelque chose de terrible. En effet, l'on se rend compte que plus de 10 millions de fichiers clients ont été dérobés par des hackeurs mal intentionnés. Nous sommes toujours en pleine crise sanitaire. La santé financière d'Easy jet est au plus bas, comme celle de toutes les autres compagnies. Les conséquences vont être catastrophiques pour Easy jet que ce soit en termes d'e-réputation, de santé financière ou de confiance des clients et des partenaires. Néanmoins, ce hack ne met pas en cause la sécurité ni la sûreté des vols. Pour le moment, les attaques se concentrent sur le vol de données qui peut engendrer des conséquences désastreuses pour les victimes.

Septembre 2019, à Toulouse, nous sommes dans les locaux d'une PME travaillant comme sous-traitant d'Airbus. La direction de cette PME envoie un message à Airbus, ci-contre retranscrit : « *Nous avons été ciblés par une attaque, son but : vous atteindre* ». Chez Airbus, cette menace est prise très au sérieux. Et pour cause puisque ce n'est pas la première fois que l'on s'attaque à la supply-chain de l'industriel afin de lui dérober des données sensibles[7]. A la suite de ceci, un programme a été mis en place par Airbus et ses partenaires, nommé BoostAerospace. Cette structure a pour but de protéger les PME du risque cyber,

[6] http://www.francesoir.fr/societe-science-tech/easyjet-piratage-des-donnees-de-9-millions-de-clients-un-cabinet-avocat-reclame-20-milliards

[7] https://www.ladepeche.fr/2019/09/26/airbus-cible-de-plusieurs-cyberattaques-via-ses-sous-traitants,8439542.php

sous l'égide des grands donneurs d'ordre tel qu'Airbus, Dassault Aviation, Safran, Thales. [8]

Ces petites actualités récentes, contées et simplifiées au maximum ont pour objectif de faire comprendre que le risque cyber pour les acteurs du transport aérien constitue une véritable épée de Damoclès suspendue au-dessus de leurs têtes. En effet, une crise cyber majeure paralysant le transport aérien est un risque réel, que nous allons essayer à travers de ce mémoire d'expliciter. Nous allons également tenter de donner, autant que faire se peut, la méthodologie qui peut aider à éviter où atténuer le risque.

Paragraphe 2 : Objectif et limites de cette étude

Ce mémoire n'a pas pour but ni pour prétention d'être technique en matière de cybersécurité aérienne. Son objectif consiste à faire le tour d'horizon de la cybersécurité du transport aérien en matière de droit, mais aussi de management et d'assurance. Ce domaine étant naissant, il est clair que dans le futur les thématiques abordées dans ce mémoire devront être développées par d'autres auteurs. Aussi, il est tout à fait intéressant d'observer les avancées dans les autres domaines du transport en matière de cybersécurité comme le transport maritime. Ce dernier affiche de nombreux points communs avec le transport aérien en matière de développement et d'encadrement de la cybersécurité.

Pour bien comprendre les tenants et les aboutissants de ce mémoire, il est essentiel de bien définir les termes, mais aussi le domaine qui est par nature pluridisciplinaire. Nous devons tout d'abord définir succinctement le transport aérien pour se pencher par la suite sur la définition de la cyber sécurité et sur celle de la cyber-résilience.

[8] https://www.usinenouvelle.com/article/les-pme-de-la-filiere-aeronautique-n-ont-pas-suffisamment-conscience-du-risque-cyber-pour-romain-bottan-monsieur-securite-de-securite-de-boostaerospace.N856880

Paragraphe 3 : La cybersécurité

Pour un néophyte, la cybersécurité apparait comme un domaine complexe, accessible seulement aux spécialistes. Trop souvent, l'image du hacker ou du savant persiste dans les esprits. Mais en réalité, la cybersécurité est accessible au plus grand nombre, c'est là-même son objectif premier.

Pour comprendre la cybersécurité du transport aérien, il est essentiel de se pencher en amont sur ce qu'est la cybersécurité.

Le terme « cybersécurité » est composé de deux mots : cyber et sécurité. Le terme **cyber** est attribué à un professeur du MIT (Massachusetts Institute of technologie), Norbert Wiener. Le terme cyber puise son inspiration à partir du grec *kubernein* qui signifie « diriger ».

Dans sa genèse, le terme cyber se définissait tel qu'un « champ entier de la théorie de la commande et de la communication, tant dans la machine que l'animal ». Ce n'est que plus tard, en 1984, qu'un auteur de science-fiction, William Gibson utilisa le terme « cyberespace » dans Le Neuromancien.

A la suite, et de fil en aiguille, le préfixe cyber va rentrer dans le langage courant, définissant tout ce qui a trait aux technologies de l'information.

Nicolas Arpagian, coordonnateur d'enseignement à l'Institut national des hautes études de la sécurité et de la justice (INHESJ) et dirigeant la structure « Sécurité numérique », nous donne une définition claire et précise de ce qu'est la cybersécurité dans son ouvrage nommé « *La cybersécurité, 2017* ». Pour lui : « *La cybersécurité va concerner les usages défensifs et offensifs de ces systèmes d'information qui irriguent désormais nos organisations modernes. Elle prend en compte les contenants, c'est-à-dire les moyens techniques (réseaux informatiques, téléphoniques, satellitaires…) utilisés pour l'échange de données, qui peuvent faire l'objet d'opérations d'infiltration, d'altération, de suspension voire*

d'interruption, comme les contenus, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques (informatique industrielle, site Internet, bases de données, messageries et communications électroniques, transactions dématérialisées…).

La cybersécurité porte aussi bien sur la protection et l'attaque d'équipements informatiques (la guerre pour ou contre l'information), afin de les surveiller ou d'en prendre le contrôle, que sur les renseignements disponibles sur la Toile (la guerre par l'information), avec de possibles atteintes à la réputation, le vol de données sensibles, des actions de piratage numérique et autres campagnes de dénigrement. »

Cette définition démontre que la cybersécurité n'est rien d'autre que de la sécurité/sûreté des systèmes d'information. La cybersécurité concerne aussi les objets connectés (supports numériques).

En France, il existe une Agence nationale de la sécurité des systèmes d'information (ANSSI), qui donne aussi une définition plus managériale. Pour l'ANSSI, la cybersécurité est « *l'état recherché pour un système d'information lui permettant de résister à un évènement issu du cyberespace susceptible de compromettre la disponibilité, l'intégrité, ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* »[9]. L'ANSSI donne ainsi une définition proactive de la cybersécurité.

Un institut européen de la cyber sécurité, l'ENISA, dans son règlement 2019/881 du 17 avril 2019, donne une définition plus juridique de ce qu'est la cybersécurité. L'ENISA entend par cyber sécurité : « Les *actions nécessaires pour protéger les*

[9] L'ANSSI définit la cyberdéfense comme « l'ensemble des mesures techniques et non techniques permettant à une entité de défendre dans le cyberespace les systèmes d'information jugés essentiels »

réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces ».

Là encore le terme « action », dans la définition proposée par l'ENISA, signifie être actif en matière de cybersécurité[10].

La cybersécurité dispose d'un lexique dédié, technique, économique et juridique, qui compose son écosystème. Aussi, des règles de droit particulier lui sont applicables, caractérisant l'empreinte légale de la cyber sécurité, appelé également « *droit de la cybersécurité* ».[11]

La cybersécurité présente donc de nombreux points en commun avec le transport aérien. En effet, en matière de sécurité aérienne, il faut également être proactif. La « culture de la sécurité »[12] est essentielle dans le transport aérien, tout comme dans la cybersécurité.

Paragraphe 4 : Le transport aérien

La notion de « transport aérien » est souvent utilisée par les journalistes ou même dans le langage courant. Malheureusement, cette notion n'est souvent pas ou mal définie par ceux qui l'utilisent. Selon Etienne Billette de Villemeur[13], le « transport aérien » se présente « comme un complexe réseau de dessertes organisé pour assurer le transport des passagers. »

Cette définition s'attarde sur le transport de passagers, ainsi que l'organisation en réseau du transport aérien. Elle est imprécise et ne permet pas d'aborder le transport aérien dans sa globalité.

[10] Nous définirons a posteriori plus précisément le rôle de L'ANSSI et l'ENISA
[11] François Gorriez, Le droit de la cybersécurité, 2020
[12] Présentation PTT Séminaire IFURTA , Sandrine Krosheko, Aéroport Marseille
[13] Billette de Villemeur, Étienne. « Comment réguler le secteur aérien ? Structure optimale de l'offre de services », *Revue économique*, vol. vol. 55, no. 3, 2004, pp. 533-542.

Le transport aérien est régi par ce que l'on appelle le « droit aérien ». La définition de ce droit aide à mieux appréhender la notion de transport aérien. Cette branche spécifique du droit n'a pas de définition officielle dans le code des transports ni dans le code de l'aviation civile[14].

Madame Julie Laborde Dit Bouriat, ancienne responsable règlementation, référentiel et qualité à la direction de la sûreté d'Air France et Professeur associé à l'IFURTA, nous donne une définition du droit aérien. Pour elle, « *le droit aérien peut être défini comme étant constitué par l'ensemble des règles qui régissent les rapports juridiques nés de l'utilisation des aéronefs* ».

Cette définition juridique droit être complétée des différentes activités aériennes que l'on distingue sur le plan règlementaire :

- L'aviation commerciale de transport de passagers ou de fret entre aéroports,
- L'aviation militaire,
- L'aviation générale qui regroupe toutes les activités de loisirs, de sport ou de travail aérien (Recherche, sauvetage).

In fine, nous disposons de plusieurs définitions nous permettant de délimiter le périmètre du mémoire. L'on peut donc dire que l'on entend par **cybersécurité du transport aérien toute la sécurité des systèmes d'information liés à l'activité des aéronefs. Que ce soit les aéroports, les constructeurs et leurs partenaires, les compagnies aériennes, les centres de formation et les institutions en rapport avec l'activité aérienne (OACI, DGAC, AESA ...)**

[14] Cours de DROIT AERIEN Partie 1. Introduction au droit aérien 2019/2020 Julie Laborde dit Bouriat *Professeur Associé Directrice de l'IFURTA*

L'activité spatiale sera aussi abordée de manière succincte pour comprendre la cybersécurité du transport aérien. Les satellites, qui appartiennent au domaine spatial et au droit spatial, sont des vecteurs d'attaque des aéronefs.

Le transport aérien défini comme tel est donc vaste en apparence. En réalité, chacune des composantes participe à la résilience d'un système décrit comme un idéal type[15]. La cybersécurité du transport aérien concerne toutes les composantes de l'activité, chacun participant à la résilience du transport aérien.

Paragraphe 5 : La résilience et la cyber-résilience

Après avoir défini la cybersécurité et le transport aérien, nous avons donné une définition du champ d'étude de ce mémoire : la c**ybersécurité du transport aérien.** Puis nous avons évoqué le lien supposé entre les acteurs du transport. Ce lien abstrait unissant, dans notre définition, les acteurs du transport aérien est un concept, devenu à la mode ces derniers temps à savoir **la résilience.**

La résilience est un terme que l'on a beaucoup entendu ces derniers temps. En mars 2020, Le Président de la République Emmanuel Macron utilisa même le terme « opération résilience » lors de la crise sanitaire du coronavirus.[16]

Afin de réellement comprendre l'utilité de ce terme dans cette étude, il faut s'éloigner de l'utilisation récente de la résilience. Il s'agit de retrouver l'épistémologie du terme dans les études universitaires.

[15] Définition de Max Weber de l'idéal type, notion abstraite pour étudier une structure, une idée
[16] https://www.leparisien.fr/politique/coronavirus-qu-est-ce-que-l-operation-resilience-lancee-par-emmanuel-macron-26-03-2020-8288583.php

Boris Cyrulnik, neuropsychiatre, directeur d'enseignement à l'université de Toulon, est une des personnalités qui a participé à l'essor dans les années 1990 du terme résilience. Avec d'autres universitaires tels que Michel Mancieux et Stanislas Tomkiewicz, ils puisent leurs influences dans les travaux de John Bowlby, un américain utilisant le terme résilience.[17]

Pourtant, certains considèrent que le terme résilience est un dérivé du féminin français « Résilient », défini en 1911. Le terme résilient exprime « le rapport de l'énergie cinétique absorbée nécessaire pour provoquer la rupture d'un métal, à la surface de la section brisée. Il qualifie ainsi une certaine résistance au choc. »[18]

Par conséquent, la résilience se définit dans les différents domaines scientifiques de recherche auxquels elle a été appliquée (l'écologie, la psychologie, le management, l'informatique, ou encore l'économie) **comme la capacité d'un « système » à pouvoir continuer à opérer, si possible normalement, après un incident, un choc, une perturbation ou une panne.**

Par extension, la résilience sous-entend être proactif face au risque, de la même manière que la cybersécurité.

En économie, Valérie Brun, maîtresse de conférence à l'IFURTA, étudie la résilience économique du transport aérien. Ses travaux ainsi que ses recherches portent sur la capacité du secteur aérien à se relever économiquement après de gros chocs tels qu'une crise terroriste (11 septembre) ou bien une crise économique (2008). [19] En informatique, l'on parle souvent de cyber-résilience d'un système d'information.

En ce qui concerne la cybersécurité du transport aérien, nous considérons que tous les acteurs forment une sorte de réseau de partage d'informations essentielles.

[17] Boris Cyrulnik. Plongée dans l'univers de la résilience.
[18] Ghernaouti, S. & Aghroum, C. (2012). Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cybersécurité. *Sécurité et stratégie*, 11(4), 74-83.

[19] Cours économie IFURTA chapitre 1 Madame Brun

L'objectif de ce réseau de partage est de maintenir la sécurité des données ainsi que des supports (objectifs, aéronefs, satellites).

Ainsi, la *cyber-résilience du transport aérien* correspond à la capacité des acteurs du transport aérien à pouvoir continuer à opérer, si possible normalement, après un incident, un choc, une perturbation, ou une panne. Les acteurs du transport aérien étant tous liés et interconnectés par l'objectif de sécurité et de sûreté de leurs données et de leurs supports.

La cyber-résilience sous-entend la mise en place d'un cadre pour atteindre l'objectif de la résilience du système. Souvent, dans les autres domaines comme l'écologie, la résilience et la cyber-résilience passent par l'instauration d'un écosystème global qui intègre la plupart du temps le juridique, le managérial, l'assurantiel et la technique.

Paragraphe 6 : Les cadres juridique et réglementaire, managérial et assurantiel.

L'objectif de ce mémoire n'étant pas d'étudier de manière technique la cybersécurité du transport aérien, nous exclurons ce cadre de notre étude. `

La résilience, comme cela est observé dans d'autres domaines tels que celui de l'écologie, passe par la mise en place d'un cadre juridique, managérial et assurantiel venant créer un écosystème permettant de rebondir. Ces cadres peuvent être comparés à des ressorts de soutien.

Nous devons tout d'abord définir ce que l'on entend par :

- Cadre juridique et réglementaire
- Cadre managérial
- Cadre assurantiel

Dans un premier temps, nous pouvons relever le point commun entre ces trois domaines : tous appartiennent aux sciences humaines et sociales.

La formule sciences humaines et sociales désigne l'ensemble des disciplines scientifiques qui étudient les humains et la société. Ces sciences s'intéressent aux activités, aux comportements, à la pensée et aux intentions, aux modes de vie, à l'évolution de l'être humain, dans le passé ou dans le présent, qu'il soit seul ou en groupe.

Les sciences humaines et sociales, en opposition avec les sciences de l'ingénieur, sont souvent considérées dans la cybersécurité comme optionnelle. Certains auteurs tels que Solange Ghernaouti et Christian Agrhoum démontrent que la dimension technique ne suffit pas à assurer la sécurité des systèmes d'information.[20] Pour ces auteurs, « Réduire la sécurité à sa dimension technologique, c'est assurer son échec ».

- Le cadre juridique et règlementaire : il correspond à l'ensemble des lois et règlements qui délimitent les activités et les comportements dans une activité donnée.

- Le cadre managérial : issu du terme management qui correspond aux techniques d'organisation et de gestion des structures, le management fait partie des sciences de gestion. Son approche universitaire est très différente du management d'entreprise. Ici, nous entendons par cadre managérial tout ce que l'organisation met en place pour gérer le risque.

[20] CYBER-RÉSILIENCE, RISQUES ET DÉPENDANCES : POUR UNE NOUVELLE APPROCHE DE LA CYBERSÉCURITÉ Solange Ghernaouti, Christian Aghroum

- Le cadre assurantiel : il n'existe pas de définition précise du cadre assurantiel. L'expression est souvent utilisée pour désigner l'ensemble des promesses ou garanties qui assure quelqu'un ou quelque chose. Mais ici, nous ajouterons à la définition l'accompagnement des assureurs en matière de sécurité.

Paragraphe 7 : Problématique et annonce du plan

Le domaine de la cybersécurité n'est pas récent. L'intégrité des réseaux est une question essentielle pour les ingénieurs depuis la naissance des premiers systèmes. A contrario, ce qui est récent, c'est l'étude de la cybersécurité, le droit de la cybersécurité, le management du risque de la cybersécurité.

Cette caractéristique du domaine nous a obligés à développer et à expliciter tous les termes de cette longue introduction.

En ce qui concerne le transport aérien, l'étude de la cybersécurité est aussi toute récente. Ce n'est qu'en 2018 qu'a été institué en France le Conseil de la Cybersécurité du Transport aérien, à la suite des assises du transport aérien. Dans ce domaine, tout est à construire au niveau de la recherche.

Dans une première partie de l'introduction, nous nous sommes attelés à présenter des actualités récentes pour définir, par la suite, les termes de cybersécurité, transport aérien, résilience, cadre juridique et règlementaire, cadre managérial, et cadre assurantiel.

Nous avons pu comprendre à travers l'introduction qu'en matière de cybersécurité il reste tout à construire pour le transport aérien. La cyber-résilience apparait comme l'objectif ultime des acteurs du transport aérien.

C’est ainsi que ce mémoire s’organisera autour de la question suivante : En quoi les cadres juridique et règlementaire, managérial et assurantiel en matière de cybersécurité participent-ils à la cyber-résilience du transport aérien ?

Dans une première partie, nous verrons que le transport aérien a une véritable épée de Damoclès au-dessus de lui en matière de cybersécurité, entrainant tout l’écosystème du transport aérien. Il s’agit d’établir un état des lieux des enjeux actuels et futurs en matière de cybersécurité du transport aérien.

Puis dans une seconde partie, nous démontrerons que si la cybersécurité n’est pas le point fort du transport aérien contrairement à la culture de la sécurité des vols, le secteur dispose déjà de bases solides et nécessaires pour construire la cyber résilience.

PARTIE 1. LE TRANSPORT AERIEN EN ETAT DE CYBER(IN)SÉCURITÉ.

Il est intéressant de voir que pour les professionnels de la cybersécurité, l'aérien est un modèle à suivre. Ainsi, Michael Simantov, auteur sur la cybersécurité et consultant, écrivit en 2018 un article sur son blog intitulé : L'aérien, un modèle pour la cybersécurité[21].

Dans son article, il observe qu'en matière de sécurité, le transport aérien obtient beaucoup de confiance. Le philosophe Paul Virilio disait « L'invention de l'aviation, c'est aussi l'invention des catastrophes aériennes ». Pourtant, ces dernières années ont été les plus sûres pour le transport aérien.

Cet article traite en réalité du niveau de sûreté et de sécurité du transport aérien, mais pas de son niveau de cybersécurité. Pour l'auteur, le transport aérien est arrivé à un niveau élevé de confiance grâce à la culture de sécurité/sûreté insufflée.

« *Apprentissage permanent, culture de la sûreté, partage, autant de pratiques du secteur aérien dont la cybersécurité devra prendre modèle. Pour atteindre la renaissance. Et instaurer une confiance comparable à celle de l'aérien*. ». L'auteur consultant en cybersécurité est en consensus avec tous les experts : le transport aérien dispose d'une culture de la sécurité et/ou sûreté lui permettant de créer la confiance. Il n'a cependant pas interrogé le niveau de cybersécurité du

[21] https://medium.com/@mike7501/la%C3%A9rien-un-mod%C3%A8le-pour-la-cyber-s%C3%A9curit%C3%A9-a3cbb318157b

transport aérien. Ce texte, « l'aérien un modèle pour la cybersécurité », a été publié en 2018 par son auteur.

En 2019, il a cette fois-ci interrogé les capacités du transport aérien en matière de cybersécurité. Son constat est affligeant. Il nomma son article « La cybersécurité, ou l'épée de Damoclès du secteur aéronautique »[22]. Michael Simantov fait le constat que les avions deviennent de plus en plus connectés et dépendants des systèmes : « *l'avion et son écosystème sont de plus en plus connectés, l'exposant donc plus aux risques cybers* ».

Alain Robic, associé chez Deloitte France, nous explique que « *le secteur aéronautique est un secteur lucratif pour les attaquants car il relève de la capacité technologique, financière, intellectuelle mais aussi de la compréhension du monde aéronautique de la souveraineté d'un État* ».

Par conséquent, il sera intéressant d'analyser en quoi la cybersécurité est un nouvel enjeu pour le transport aérien (Titre 1) avant d'étudier le développement et l'encadrement juridique de la cybersécurité du transport aérien (Titre 2).

[22] https://portail-ie.fr/analysis/2105/jdr-la-cybersecurite-ou-lepee-de-damocles-du-secteur-aeronautique-12

TITRE 1. L'HISTOIRE DU TRANSPORT AERIEN AVEC LE PRISME DE LA CONNECTIVITE

Le transport aérien est une activité qui a su créer la confiance en matière de sécurité et de sûreté. Le transport aérien est un système complexe et intégré qui est constitué de technologie de l'information et des communications essentielles à la sécurité et à la sûreté des vols. Le transport aérien dépend de plus en plus de la disponibilité des systèmes de technologie de l'information et des communications, ainsi que de l'intégrité des données. On voit alors apparaitre une nouvelle menace, la menace cyber qui évolue rapidement et qui arbore différentes formes, spécifiques au transport aérien.

Nous allons donc revenir sur l'histoire du transport aérien du point de vue de la connectivité (Chapitre 1) puis nous verrons par la suite pourquoi 30 ans après l'apparition d'internet, la cybersécurité devient aujourd'hui un sujet crucial pour le transport aérien. (Chapitre 2)

CHAPITRE 1. L'interdépendance du transport aérien et de la connectivité

En comparaison avec l'histoire de l'humanité, celle du transport aérien est récente. Dès les débuts de l'aviation, la question de la communication et de l'information était centrale. Cette prédominance de la question de l'information et de la communication s'explique du fait de l'importance de faire voler et de guider les aéronefs en sécurité (Section 1). L'électronique et la connectivité ont toujours accompagné le développement du transport aérien. (Section 2)

SECTION 1. La genèse du transport aérien

A. Les Pionniers de l'aviation, aïeuls du transport aérien

On les appelle les « pionniers de l'aviation ». Il est impossible d'attribuer la naissance de l'aviation à un seul individu. Comme pour beaucoup de grandes innovations humaines, le transport aérien est né grâce à l'assemblage des efforts de plusieurs individus dans une période donnée. Ces individus ont chacun participé à leur échelle aux fondations de l'aviation et par extension du transport aérien.

Le 17 décembre 1903, les frères Wright réalisent leur rêve. Un rêve qui était sans doute commun à beaucoup d'hommes : voler. C'est ainsi qu'ils ont fabriqué un engin motorisé permettant, quelques années plus tard, le premier vol international : Décalais France et Douvre en Grande Bretagne.[23]

Le transport aérien n'était pas encore né, mais l'homme pouvait imaginer son développement. Pour cela, fallait-il encore rendre l'aéronef sûr.

C'est admis, l'industrie militaire est le berceau idéal pour développer une technologie. En période de guerre, cela devient même un impératif. L'avion, et par extension le transport aérien, ne dérogera pas à cette règle. En effet, la Première guerre mondiale va faire entrer l'aéronef dans une nouvelle dimension.

Suite à la guerre, les États ont compris le rôle crucial que jouait le transport aérien pour leur survie et leur développement.

L'anecdote historique du militaire Charles Godefroy illustre parfaitement nos propos. Le 14 juillet 1919[24], c'est la fin de la première guerre mondiale. Les

[23] L'évolution du Transport Aérien de 1903 à 1995 : Les compagnies de pavillon aux alliances stratégiques, Walid Daoudi, 1996
[24] **Histoire De L'aviation Edmond Petit**

aéronefs ont été beaucoup utilisés. Leurs pilotes sont perçus par la population comme de véritables héros. Mais l'Etat-major décide que les pilotes de l'armée doivent défiler à pied. C'est un véritable affront pour la plupart qui ont risqué leur vie dans des machines peu fiables. Le 7 aout 1919, Charles Godefroy décida de prendre son biplan Nieuport 11, de décoller de l'aérodrome de Villacoublay, et de passer sous l'arc de triomphe.

Cet exploit démontre à la population et aux politiques que l'aéronef est devenu une technologie sûre, in fine prête à se développer.

B. Une volonté d'organiser le transport aérien

A l'avenir, le transport aérien s'est donc organisé au niveau international. L'on peut citer tout d'abord la Convention de Paris de 1919 qui regroupe les Etats européens. Puis est apparue la Convention de La Havane en 1928 et celle de Varsovie en 1929, où les notions de responsabilités ont déjà été abordées.

Même si le transport aérien n'est pas démocratisé, nous assistons à l'apparition des premières compagnies aériennes (par exemple, la française « La Farman »).

C'est après la deuxième guerre mondiale que naquit l'OACI[25] en 1944, à la suite de la conférence de Chicago le 7 décembre 1944. Nous développerons plus-tard dans ce mémoire le rôle de l'OACI, ainsi que son importance en matière de cybersécurité du transport aérien.

Pour nombre d'auteurs, l'organisation du transport aérien international est perçue comme la première réussite de coordination mondiale[26]. De par sa dimension unique, le transport aérien se doit d'être organisé de manière coordonnée.

[25] OACI : Organisation de l'aviation civile internationale

[26] Question internationale **Le transport aérien : une mondialisation réussie**
Parution : 9 mars 2016

Le but du transport aérien est de connecter. Pour ce faire, le transport aérien a lui-même besoin de développer ses systèmes d'information et de communication afin de garantir sa sécurité.

SECTION 2. Historique des technologies de l'information du transport aérien

A. Les débuts de la communication dans les airs : La radiophonie

Afin de comprendre l'histoire des technologies de l'information, nous allons, dans cette partie, rester à la même période à savoir le commencement du transport aérien.[27]

En effet, les premières applications de communication sans fil des aéronefs datent de la Première Guerre mondiale. Les pilotes de l'époque étaient équipés de moyens de communication leur permettant de recevoir du sol des messages en morse. C'était là les débuts des communications « sol-air ».[28]

Durant la deuxième guerre mondiale, souvent surnommée « la guerre des technologies », l'on vit se développer au sein des aéronefs les premiers systèmes RADAR.

A la suite de cela, est apparu le développement de la phonie puisque la radio devint rapidement le premier moyen de communication du transport aérien[29].

---

[27] Technologies de l'information et de la communication (TIC : transcription de l'anglais *information and communication technologies, ICT*) est une expression, principalement utilisée dans le monde universitaire, pour désigner le domaine de la *télématique*,

[28] « *La communication Air/Sol à liaison radio VHF est une communication bilatérale entre une station au sol et une autre station à bord d'un aéronef véhiculée par une onde porteuse dans la bande VHF et qui est utilisée pour les besoins des services de la circulation aérienne* »

[29] Marie BENEJEAN, Informatisation des productions d'information et des activités de communication dans les relations pilotes-contrôleurs :
Contradictions et reconfigurations entre technologies en projet et mises en pratiques

En 1960, le développement de l'informatique permet l'automatisation de l'envoi des données du contrôle aérien. Cette même année, l'on observe également l'augmentation du trafic aérien. Cette dernière entraine un accroissement des données à traiter et donc à automatiser. L'informatique a toujours accompagné le développement du transport aérien.

B. Informatique et automatisation, indissociables du transport aérien

En 1960, pour faire face à l'augmentation du trafic aérien en France, Jacques Villiers, ingénieur issu de la première promotion de l'ENAC décide d'étudier les perspectives d'automatisation du contrôle aérien. Il s'adresse au constructeur IBM pour mettre au point un système informatique du contrôle aérien.

« Les informations sur les plans de vol sont préparées par des opératrices à partir de cartes perforées ; le calculateur génère l'impression des strips, ensuite distribués dans la salle via un réseau de tubes [30] pneumatiques ».

Il est important de souligner qu'informatique et automatisation ne veulent pas dire « connecté ». Le transport aérien a toujours été à la pointe des technologies de l'information et de la communication, sans pour autant être connecté au réseau.

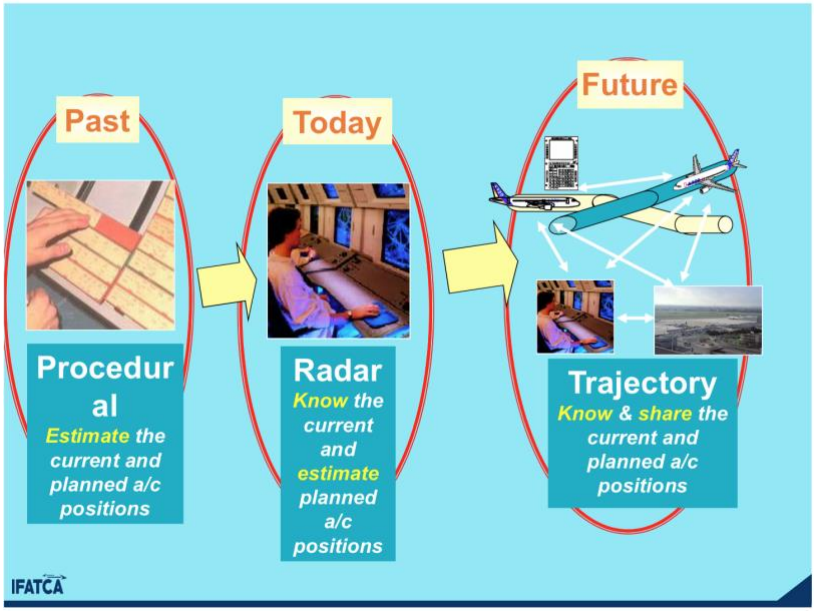
Dès 1970, « *Dans la salle de contrôle, de nouveaux postes de travail sont installés (ODS : Operational Display System) : « les écrans ronds et monochromes sont remplacés par de grands écrans Sony, carrés, en couleur et à haute définition. Le digitatron*[31] *disparaît au profit du clavier et de la souris* » (Jousse et al., 2007, p.47).

[30] Jousse et al., 2007, p.29

[31] « *Jacques Villiers invente ainsi dès les années 60 le Digitatron, un moyen de saisie tactile permettant aux opérateurs de modifier de façon intuitive les plans de vol des avions* ».

Ainsi, l'on voit bien que l'informatique a toujours été présent par exemple dans les salles de contrôle. Puis vint la formidable épopée franco-anglaise du Concorde. Le Concorde fut la genèse du cockpit informatisé. Il va permettre de développer des outils informatiques mettant fin au pilotage dit « manuel »[32].

Schéma 1 : Le passé, le présent et le futur du contrôle aérien



(Source : Présentation Académie de l'Air et de l'espace.)

Nous nous sommes attardés sur l'aéronef ainsi que sur le contrôle aérien. Pour être véritablement complet sur ce que l'on définit comme transport aérien, il faut également évoquer les aéroports.

Un aéroport est un lieu disposant de nombreuses informations à traiter. Il est le garant du bon décollage et atterrissage des aéronefs. L'aéroport doit aussi guider et informer le passager lors de sa venue.

[32] *« Les commandes de vol électriques (en anglais, fly-by-wire ou FBW) sont un ensemble de dispositifs électriques, électroniques et informatiques, par l'intermédiaire desquels le pilote contrôle un aéronef, par opposition aux traditionnelles commandes de vol mécaniques où le pilote agit sur les gouvernes de l'avion par une liaison mécanique directe ou assistée par des servocommandes. On utilise parfois le terme anglais de fly-by-wire ».*

Un mémoire a été réalisé en 2017 par Alexandre Brillaut, étudiant à l'IFURTA. Son étude a pour thématique les NTIC (nouvelles technologies de l'information et de la communication) et l'aéroport. Il explique le développement dans un premier temps des TIC dans le parcours passager, puis il s'interroge sur les NTIC et le futur de l'expérience client en aéroport.

CHAPITRE 2. L'apparition d'un risque nouveau pour le transport aérien : La cybersécurité

Le transport aérien s'est développé en même temps que sa connectivité. Internet est apparu il y a plus de 30 ans maintenant. Jusqu'il y a quelques temps, le secteur aérien semblait épargné du risque cyber. En comparaison à d'autres industries ayant une forte culture de sécurité telles que celle du nucléaire, l'aérien semble avoir un retard considérable en matière de cybersécurité[33] (Section 1).

Néanmoins, il semblerait que nous sommes entrés dans une ère où les innovations technologiques connectées font plus rapidement leurs apparitions dans le transport aérien. Ce dernier, de par sa culture de la sécurité, est habitué aux temps longs en ce qui concerne les innovations. Il lui faut donc s'adapter rapidement à ces évolutions[34] (Section 2).

[33] Cybersécurité du nucléaire ? Où en est-on ? Tribune de Loïc GUEZO, CyberCercle, 2015

[34] https://www.assisesdutransportaerien.gouv.fr/comprendre/les-actualites/le-transport-aerien-lere-du-numerique-5440

SETION 1. La cybersécurité et le transport aérien ou la cybersécurité du transport aérien

Le transport aérien, n'est pas une industrie dans laquelle les innovations sont rapidement intégrées (A). Paradoxalement, le niveau de cybersécurité du transport aérien connait un réel accroissement (B).

A. Transport aérien, un long cycle de vie

Le transport aérien est une industrie dont on dit qu'il connait un temps long. En effet, le développement des aéronefs ainsi que celui des logiciels embarqués et des techniques de gestion prennent beaucoup de temps. Ceci s'explique par la **certification de ces systèmes**[35].[36]

Tel que vu précédemment, le transport aérien s'est organisé de manière homogène au niveau international. Pour atteindre ses objectifs en matière de sécurité aérienne, l'OACI a demandé aux Etats d'organiser la certification des appareils et des aéroports.

Tous les acteurs du transport aérien respectent donc les même normes et standards. Ces normes et standards dictés dans les annexes de l'OACI sont précisés par les Etats[37].

Ainsi, entre son développement et son approbation par les autorités, l'application d'une innovation dans le transport aérien prend en moyenne 5 ans.

---

[35] « *Les aéronefs répondant à des standards de conception, de fabrication et de maintenance reconnus internationalement peuvent faire l'objet de certificat de navigabilité de niveau OACI autorisant la circulation internationale. Pour les aéronefs relevant de l'Annexe I ces certificats sont le CDN ou le CDN spécial (CDNS)* ». **https://www.ecologie.gouv.fr/certificat-navigabilite-niveau-oaci-cdncdns#:~:text=Un%20certificat%20de%20navigabilit%C3%A9%20de,%C3%A0%20l'Aviation%20civile%20internationale.**

[36] Définition Larousse : Certificat délivré par un organisme indépendant attestant la conformité (d'un produit, d'un service) aux normes et règlements en vigueur. Nous définirons plus tard le rôle et l'importance de la certification dans le transport aérien.

[37] Annexe 8 de la Convention relative à l'Aviation Civile internationale

La certification est prégnante dans le développement d'un aéronef. Nous pensons ici au cas du Boeing 737 Max et de la re-certification du système anti-décrochage MCAS. C'est à la suite de deux accidents ayant fait 346 victimes que le grand public a découvert que les logiciels embarqués dans les avions pouvaient avoir des failles.

Ces dernières décennies, la cybersécurité n'a pas été la principale préoccupation du secteur aérien. Le temps de vie long des appareils et des logiciels pouvait, en apparence, protéger le transport aérien.

Il faut bien comprendre que malgré l'apparition d'internet il y a de cela 30 ans, la notion « d'aviation connectée» est très récente. Pour beaucoup, l'informatique signifie être connecté. Sauf que l'aviation démontre bien le contraire.

Le transport aérien, comme vu dans la partie historique de la connectivité, a toujours été en lien avec le traitement de la donnée. Il doit son développement au développement de l'informatique et plus précisément des modes de calcul.

De nos jours, avec le « *pilotage électronique* » certains comparent même les pilotes à des informaticiens qui doivent seulement « *rentrer des données brutes que l'ordinateur calculera* ».

B. La cybersécurité de certains appareils assurée par le long temps de vie

Pour illustrer nos propos, concernant le temps de vie des logiciels dans le transport aérien, nous baserons notre réflexion sur un article.

« Pour ses mises à jour, Boeing utilise des disquettes des années 80 »[38] : voici le titre de l'article que publia Jeremy Joli, journaliste chez Capital, le 11 août 2020. L'article nous expose la problématique à laquelle fait face Boeing à savoir les mises à jour critiques de leur appareil 747-400 lancé en 1988. L'on a pu voir précédemment, le temps de vie des appareils est long. Il y a aujourd'hui dans le ciel international plus de 300 Boeing 747-400 datant de 1988.

Le problème est que pour faire les mises à jour de logiciel, Boeing se retrouve à utiliser des disquettes. Ces disquettes sont aujourd'hui une technologie devenue complètement obsolète en dehors du transport aérien.

En matière de cybersécurité, cela peut apparaitre comme un risque majeur. Mais en réalité, il s'agit d'une protection. En effet, cette technologie est tellement ancienne, qu'il n'existe aujourd'hui aucun moyen d'attaquer ce système informatique avec les outils modernes.

Cette protection n'est pourtant pas une volonté de la part des constructeurs. Mais il faut bien comprendre que dans le transport aérien, les mises à jour sont très rares. A partir du moment où un logiciel embarqué obtient sa certification, toute modification doit être signalée. In fine, tout le processus doit être répété. C'est pour cela que le constructeur offre un produit fini quasiment parfait.

Quand l'on s'intéresse à la définition de la cybersécurité, certain considèrent que les « bug » seraient un problème de sécurité, et donc par extension de cybersécurité. En informatique, le bug (de l'anglais insecte) correspond à un défaut de conception d'un programme qui va entrainer un dysfonctionnement. « *Un bug peut résider dans une application, dans les logiciels tiers utilisés par cette application, voire dans le firmware d'un composant matériel comme ce fut le cas du bug de la division du Pentium*2. ».

[38] ttps://www.capital.fr/economie-politique/pour-ses-mises-a-jour-boeing-utilise-des-disquettes-des-annees-80-1377706

Avant même le développement d'un transport aérien connecté, certains considéraient les bug d'affichage dans le cockpit, les pannes de logiciels informatiques (hors connexion), comme des problèmes de **cybersécurité du transport aérien.**

SECTION 2. Le transport aérien du futur : de plus en plus connecté

Le transport aérien connait depuis quelques années une réelle transformation digitale (A). De plus en plus connecté, le transport aérien a fait l'objet de grands changements. Ces changements concernent les constructeurs, les aéroports, et les compagnies aériennes (B).

A. <u>Vers un transport aérien connecté</u>

Les sources de cette partie seront les Actes du colloque de l'académie de l'air et de l'espace (AAE) : Vers des navires et aéronefs sans équipage ? Jusqu'où la machine peut-elle remplacer l'homme, ainsi que leurs dossiers nommés « Cybermenaces visant le transport aérien ». La limite des travaux de l'AEE est de se concentrer seulement sur l'avion connecté comme vecteur de risque.

Dans l'introduction de leur dossier « Cybermenaces Visant le transport Aérien, » il est précisé toutefois : « *Afin d'appréhender le sujet dans sa globalité, il faut noter que le monde du transport aérien commercial forme un Système de systèmes (SoS) composé des éléments suivants : • les avions de ligne ; • les compagnies aériennes ; • les constructeurs, les équipementiers et les sous-traitants ; • les gestionnaires de la circulation aérienne (Air Traffic Management – ATM) ; • les aéroports ; • les fournisseurs d'accès et de service5 ; • les entreprises de maintenance ; • et tous les personnels concernés* ».

Cette définition est semblable à celle utilisée dans ce mémoire pour définir « le transport aérien ». Contrairement à ce mémoire, le dossier n'étant pas destiné à des néophytes, la définition est tout de même plus précise et plus technique. Pour les auteurs du dossier, le transport aérien est donc un système de système dont chaque élément devient de plus en plus connecté.

Il nous faut définir tout d'abord ce qu'est la transformation digitale pour bien comprendre les nouvelles problématiques auxquelles font face les acteurs du transport aérien.

« La transformation digitale » est difficile à définir et à conceptualiser. Nous utiliserons la définition d'Ugo Roux dans son article « La transformation digitale des entreprises ». Pour l'auteur, la transformation digitale « conduit *à un changement d'échelle et à un développement accru du numérique dans les pratiques de travail, mais aussi dans les produits et services à proposer au clien*t ».

D'après le groupe Thalès, *« Les technologies du secteur aéronautique connaissent, grâce à la transformation digitale, une profonde mutation : les systèmes qui communiquaient hier un à un en circuit fermé sont aujourd'hui totalement interconnectés, de plus en plus ouverts sur le monde extérieur, notamment via le partage de données en temps réel. La sécurisation des infrastructures (protection des aéroports, des avions ou des bases aériennes par exemple) n'est donc plus suffisante : l'ensemble des systèmes, des communications et des données doivent être protégés* ».

Ainsi, le secteur aéronautique au vu du développement et de sa croissance (avant la crise du coronavirus) doit se moderniser. Pour cela il doit changer de paradigme grâce à la connectivité.

Malheureusement, cette connectivité accrue à travers les nouvelles innovations engendre des failles.

Le transport aérien ne doit pas se faire surprendre par ces innovations. Il doit anticiper tout cela et prévoir sa cybersécurité. De la même manière qu'il le fait déjà en matière de sécurité aérienne.

B. Les innovations actuelles et futures : de nouveaux risques cyber pour les différents acteurs du transport aérien

Le transport aérien connait depuis ces dix dernières années de multiples innovations connectées. Nous allons ici faire un tour d'horizon de ces différentes innovations aériennes connectées. On les retrouve dans les aéroports, chez les constructeurs mais aussi les compagnies. Nous nous concentrerons ultérieurement sur les réels enjeux en matière de cybersécurité pour ces 3 catégories.

a) Les innovations des aéroports

En tant qu'infrastructures, les aéroports sont vitaux pour le transport aérien. [39] Ils sont considérés par certains comme de véritables villes. Au sein des aéroports, transitent parfois plus de 290 000 passagers dans une seule journée.[40] Ces derniers attendent un service rapide et, de nos jours, veulent également la simplicité que ce soit en termes d'accessibilité et d'informations données.

Nous renvoyons encore nos lecteurs au mémoire d'Alexandre Brillaud qui a consacré une entière partie sur les NTIC en aéroports et leurs développements. Dans le chapitre 1 de la partie 3 nommé « la cybersécurité des installations», il élabore une revue de tous les risques des nouvelles installations aéroportuaires.

Margot Lariday, journaliste, publia un article sur tom travel nommé « Sita : L'aéroport du futur sera autant connecté que ses passagers »[41].

[39] Jean François Guitard , Cours de gestion des aéroport 20 ème édition
[40] https://www.lefigaro.fr/flash-eco/2014/08/21/97002-20140821FILWWW00234-record-d-affluence-pour-l-aeroport-paris-cdg.php

[41] https://www.tom.travel/2019/12/13/sita-laeroport-futur-connecte-passagers/

En tant qu'innovations majeures, l'on peut citer :

- les contrôles de la documentation automatique,

- la localisation en temps réel des bagages,

- La gestion grâce à l'intelligence artificielle de pistes connectées,

- Véhicule autonome pour aider aux opérations aériennes,

- Développement de la 5G

Depuis 2018, le groupe aéroport de Paris a mis en place un concours d'innovations. Le but de ce concours est de trouver les futures innovations connectées pour l'aéroport du futur. En effet, les NTIC présentent un réel avantage concurrentiel pour les aéroports.[42]

b) Les constructeurs

Les constructeurs du secteur aéronautique font face à de réels défis. Outre la transformation digitale, le défi écologique est très prégnant. Il est vrai que ces derniers temps, le transport aérien a été victime d'un réel bashing concernant son impact sur l'environnement.

Pour certains, évolution technologique et écologie sont deux termes antinomiques. Mais la réalité est tout autre puisque le secteur aérien se doit d'innover tout en respectant l'écologie. Il s'agit d'un impératif pour le développement futur du transport aérien.

[42] https://www.parisaeroport.fr/groupe/groupe-et-strategie/notre-strategie/innovation/actualit%C3%A9s/play-your-airport

Prenons par exemple le cas d'un nouvel avion supersonique. Aujourd'hui, nous avons les capacités de le construire. Cependant, la conscience écologie est telle que les constructeurs ont de nouvelles obligations liées à celle-ci dans les innovations. Nous ne devons plus innover pour innover sans contrainte (même si cela a parfois servi l'humain). Nous devons innover avec l'impératif écologique. Fini les avions supersoniques, qui consomment à outrance, dans le but d'aller le plus vite possible. Actuellement, les constructeurs aéronautiques sont dans l'obligation légale et morale d'innover de manière écologique.

L'on peut citer comme innovations connectées des constructeurs :

- Le cockpit connecté,[43]
- Le taxi drone autonome,
- L'intelligence artificielle dans le cockpit et dans la cabine,
- Internet et le wifi à bord,
- Les tablettes connectées,
- Les satellites connectés

Par exemple, pour le cas de l'intelligence artificielle et de l'impératif écologique, les constructeurs mettent en avant une diminution du carburant consommé. D'après eux, la machine opte pour les meilleures trajectoires. Ces meilleures gestions de la trajectoire et de la vitesse ont des conséquences sur la consommation de carburant. In fine, ces nouvelles innovations sont bénéfiques du point de vu écologique.

En conclusion, il existe bien un développement exponentiel des nouvelles technologies dans le transport aérien. Nous avons vu que ce développement s'opère au sein des aéroports et chez les constructeurs. Les compagnies aériennes ne sont pas épargnées par le phénomène de digitalisation. [44]

[43] https://www.lesechos.fr/industrie-services/air-defense/thales-ouvre-la-voie-au-cockpit-connecte-et-sans-copilote-1152079

[44] https://www.voyages-d-affaires.com/compagnies-aeriennes-digitalisation-20190509.html

c) Les compagnies aériennes

Les compagnies sont celles qui semblent être le plus en avance en matière de transformation digitale. En effet, elles ont déjà numérisé les réservations et le check-in. Souvent, elles multiplient les innovations connectées dans l'objectif de proposer une véritable expérience au consommateur et non plus un simple vol.[45]

L'on peut citer comme innovations futures pour les compagnies :

- La **communication avec les pilotes** : La cabine étant de plus en plus connectée, les compagnies aériennes pourront donner des informations plus précises à leurs pilotes et cela même au milieu de l'Atlantique,

- Système de **reconnaissance facile** : La fin des cartes d'embarquement,

- **Les satellites : -** le wifi en avion est un nouveau service proposé par les compagnies aériennes. Il tend à se développer. Les satellites peuvent aussi perturber la navigation aérienne en cas d'attaque ou de dysfonctionnement.

En somme, le transport aérien est en pleine « transformation digitale ». Contrairement à d'autres secteurs moins réglementés et moins contrôlés, ces innovations mettent du temps à apparaitre. Le secteur aérien prend donc le temps d'étudier les risques en matière de sécurité et de sûreté.

[45] https://www.vol-retarde.fr/blog/2017/06/06/innovation-ce-que-nous-prepare-les-compagnies-aeriennes

TITRE 2. POLYMORPHISME DE LA CYBERSÉCURITÉ DU TRANSPORT AÉRIEN

Le secteur aérien opère une distinction bien précise entrer sûreté et sécurité.

Les nouvelles innovations connectées entrainent l'apparition d'un nouveau risque : le risque cyber. Comme vu précédemment, nous avons du mal à classifier le risque cyber. Il est polymorphe[46] dans sa définition et dans la pratique. Il appartient aussi bien à la sûreté qu'à la sécurité.

Par conséquent, nous allons vérifier si l'on peut classifier le risque cyber pour le transport aérien (Chapitre 1), puis nous verrons les enjeux qu'induisent les nouvelles innovations en matière de cybersécurité aussi bien pour les aéroports que pour les constructeurs ainsi que les compagnies. (Chapitre 2).

CHAPITRE 1. Le cyber-risque : Sécurité ou Sûreté.

La sécurité et la sûreté étant intimement liées au développement du transport aérien (Section 1), le risque cyber a fait émerger un nouveau terme fusionnant ces notions fondamentales et brisant en quelque sorte la frontière qui les séparait (Section 2).

SECTION 1. La sécurité et la sûreté liées au développement du transport aérien

Depuis le commencent de notre étude, les termes sécurité et sûreté ont été évoqués sans être réellement définis. C'est la raison pour laquelle il nous faudra

[46] Polymorphe est issu du grec, polumorphos, qui signifie : ayant plusieurs formes à la fois.

définir ces termes (A) avant de constater qu'ils constituent bien deux notions distinctes dans le transport aérien (B).

A. Définition

Tout d'abord, pour bien comprendre le sujet, il nous faut définir ce que l'on entend par sécurité et sûreté dans le transport aérien.

La sécurité aérienne a trait à la protection contre tout accident, erreur ou défaut volontaire dans la conception, la construction, la maintenance et l'exploitation des aéronefs. La sécurité a toujours été d'une importance vitale pour les acteurs du transport aérien.

A contrario, on entend par **sûreté aérienne**, l'ensemble des mesures et des moyens mis en œuvre pour prévenir les actes de malveillance (terrorisme), visant les aéronefs, leurs passagers et les membres d'équipage. Apparait donc ici la notion d'intention. En effet, la sûreté aérienne concerne les actions humaines délibérées.

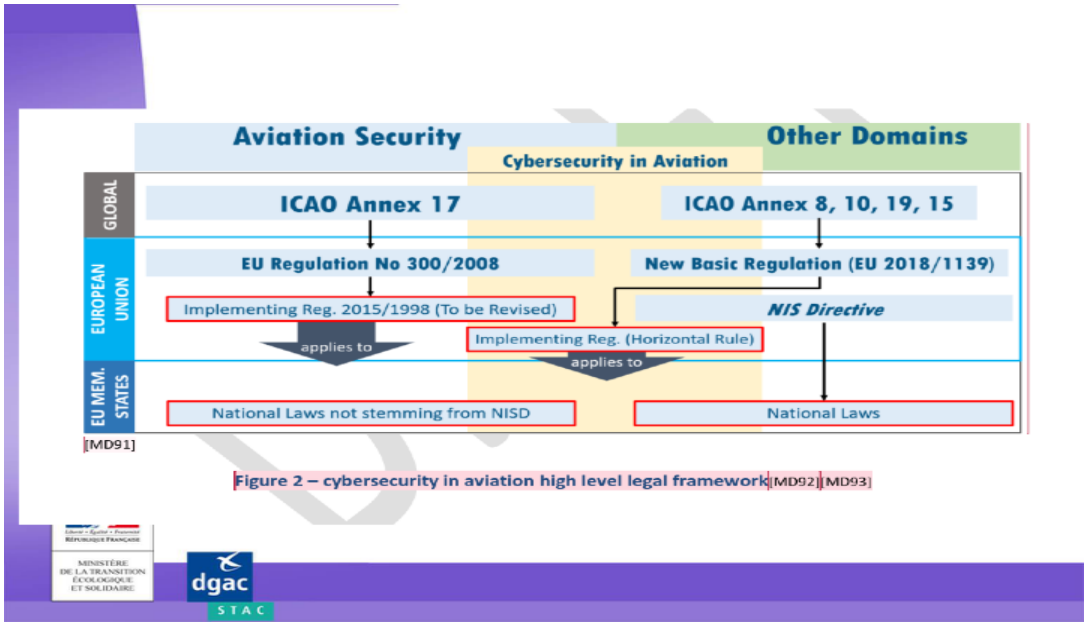
Depuis ses débuts, le transport aérien a toujours été très codifié. Il en va de même pour la sécurité et la sûreté. Les autorités de régulation ont dû distinguer ces deux notions dans les textes.

B. Sécurité et sûreté, deux notions bien distinctes pour les régulateurs du transport aérien

Les organes régulateurs du transport aérien font une distinction claire en matière de règlementation entre la sûreté et de la sécurité.

Ci-dessous, un schéma de la Direction Générale de l'Aviation Civile

(DGAC)



Ce schéma présente la distinction entre la sécurité et la sûreté. Il intègre également les nouvelles règles en matière de cybersécurité sur lesquelles nous nous pencherons ultérieurement dans l'étude.

Ce qui nous intéresse davantage au sein de ce schéma est la construction et la distinction que font les organes régulateurs entre la **sûreté et la sécurité**. Par exemple, pour l'OACI, la sûreté correspond à l'Annexe 17, tandis que la sécurité se trouve expliquée à l'annexe 19.[47] En effet, l'annexe 17 (3.1.1) dispose que « *Chaque État contractant établira et mettra en œuvre un programme national écrit de sûreté de l'aviation civile destiné à protéger les opérations de l'aviation civile contre les actes d'intervention illicite, au moyen de règlements, de pratiques et de procédures qui tiennent compte de la sécurité, de la régularité et de l'efficacité des vols* ».

[47] Convention Relative à l'Aviation Civile Internationale,1944

Le Programme national de sûreté de l'aviation civile expose qu'il incombe aux États (Annexe 17 – 4.9.1 et 4.9.2) « *de veiller à ce que des mesures appropriées soient élaborées pour* ***protéger la confidentialité, l'intégrité et la disponibilité des systèmes et données informatiques et de communications critiques utilisés aux fins de l'aviation civile*** *contre des interventions qui peuvent compromettre la sécurité de l'aviation civile et d' encourager les entités qui participent à la mise en œuvre de divers aspects du programme national de sûreté de l'aviation civile, ou qui en sont chargées, à identifier leurs systèmes et données informatiques et de communications critiques, y compris les vulnérabilités de ces systèmes et les menaces pesant sur eux, et d'élaborer et mettre en œuvre des mesures de protection, notamment en matière de sûreté intégrée, de sûreté de la chaîne d'approvisionnement, de séparation des réseaux et de contrôle d'accès à distance, selon qu'il convient ».*

En conclusion, la sécurité aérienne et la sûreté aérienne sont deux domaines bien distincts même si chacun peut avoir un impact sur l'autre. Prenons l'exemple d'un passager indiscipliné qui rentre dans le domaine de la sûreté. Si ce même passager perturbe la concentration du pilote amenant ce dernier à faire une erreur de calcul dans le cockpit, apparait alors un problème de sécurité.

La sûreté et la sécurité peuvent donc être liées mais dans l'aérien, on opère une distinction vitale entre les deux.

Par ailleurs, il nous faut évoquer la traduction anglaise qui ne facilite pas les choses. La sécurité correspond à « safety » et la sûreté correspond à « security ». Cela rend parfois compliquée la compréhension de la distinction dans l'aérien, entre les francophones et les anglophones.

Précisions que le français fait partie des 7 langues recommandées par l'OACI. Même si, en réalité, l'anglais domine le transport aérien, et donc par extension les notions de safety, et security.

Le risque cyber devenant une réalité pour le transport aérien, il faut se pencher sur ce risque qui semble rompre les barrières en la sécurité et la sûreté.

SECTION 2. Le risque cyber dans le transport aérien, point d'ancrage de la sécureté

Le terme de « sécureté » est un néologisme qui permet de cerner le risque cyber dans le transport aérien (A) et également de remettre en question l'existence de la frontière entre sécurité et sûreté (B).

A. Sécureté, un néologisme pour comprendre le risque cyber dans le transport aérien

« Safurty » est un néologisme que nous allons utiliser dans cette partie pour expliquer comment le risque cyber rompt la barrière entre la sécurité et la sûreté du transport aérien. La « safurty » constitue la synthèse des termes anglais Safety (sécurité en français), et Security (sûreté en français). Pour les besoins de ce mémoire qui se veut de rester en langue française, nous traduirons le néologisme safurty, en **sécureté**.

Pour comprendre pourquoi nous avons besoin de ce terme de sécurité du cyber risque dans le transport aérien, il faut se pencher sur la nature même du risque cyber qui casse les barrières entre la sûreté et la sécurité mises en place par le transport aérien.

B. La fin de la frontière entre la sécurité et la sûreté du transport aérien?

Le spécialiste en cybersécurité Michael Simantov a publié sur son blog en 2019 un article nommé « Cyber sécurité dans l'aéronautique : sécurité ou sûreté ? ». Dans cet article, il explique que du point de vue du domaine de la cybersécurité « *le découpage entre "safety" et "security" est perturbant* ». En effet, la menace cyber est, de par sa nature, protéiforme. Elle ne peut être classée de manière aussi distincte, sauf à donner une définition précise de chaque incident cyber dans l'aérien.

Michael Simantov revient sur l'histoire de Chris Roberts pour illustrer ses propos. L'hacker avait réussi en 2015 à modifier la puissance des moteurs d'un avion pendant le vol. Il a réussi à accéder aux commandes de l'avion, considéré comme un élément de sécurité aérienne. Pour arriver à réaliser cette attaque, il utilisa le système de divertissement des passagers à bord (IFE). Cet équipement n'est pas considéré comme un équipement de sécurité aérienne.

Pour l'auteur, « *ces différents cas nous prouvent que la nature même de la menace cyber fragilise toute frontière. Cette nouvelle menace oblige à imaginer de nouveaux chemins de compromission possibles, qui évoluent au cours du temps en fonction des avancées technologiques et de l'évolution des menaces. Les cyberattaques peuvent donc générer des conséquences de type "safety" en compromettant des équipements "non-safety*" ».

Revenons au crash du Boeing 737 max qui concerne un problème de conception de logiciel. C'est un problème de sécurité aérienne. Pour le moment, les logiciels comme celui du Boeing 737 Max ne sont pas encore connectés. Mais lorsqu'ils le seront, devra-t-on considérer le risque du point de vue de la sécurité ou bien de la sûreté ?

Dès lors que le transport aérien fait émerger la notion de cybersécurité dans son univers, il faut choisir sa classification.

La distinction entre cyber malveillance et cybersécurité des systèmes d'information doit être réalisée. La définition du risque cyber étant trop vaste, le transport aérien doit bien faire la distinction entre cybersécurité et cyber sûreté. Même si l'on a vu que le risque cyber pouvait prendre les deux formes à la fois, il faudra certainement, pour le transport aérien, s'interroger sur l'existence de cette barrière entre la sécurité et la sûreté.

Si la culture de la sécurité est plus ancienne que celle de la sûreté dans le transport aérien, nous pouvons constater que ces deux cultures fusionnent en matière de cybersécurité. Ainsi, la cybersécurité représenterait une sorte de chimère[48] des deux notions si chères au transport aérien.

In fine, peut-on réellement affirmer que le risque cyber perturbe l'ordre établi de la définition du risque dans le transport aérien ?

Il semblerait que pour le moment, le risque cyber s'intègre tout aussi bien en matière de sécurité aérienne que de sûreté. Il va permettre davantage de dialogue dans les organisations du transport aérien qui sont en charge de la sécurité et de la sûreté.

CHAPITRE 2. Les risques en matière de cybersécurité pour les différents acteurs du transport aérien

Depuis toujours, la sécurité aérienne a traité la sécurité des systèmes d'informations dans l'objectif de garantir la disponibilité des données et l'intégrité des systèmes. Il faut aujourd'hui que le transport aérien conçoive que la cybersécurité va devenir un enjeu majeur. Dans ce chapitre, nous étudierons les risques que les innovations connectées vont créer dans le transport aérien. Qui voudra voler dans un aéronef d'un **constructeur** ayant reçu des informations piratées du sol (Section 1) ? Quelle **compagnie** prendra le risque de faire voler ces

[48] Ici nous entendons chimère au sens grec du terme, c'est-à-dire un monstre imaginaire à tête de lion et queue de dragon, qui crache des flammes.

avions si un tel drame arrivait (Section 2) ? Enfin, comment **un aéroport** pourrait-il se relever d'une paralysie des systèmes durant seulement une petite heure ? (Section 3)

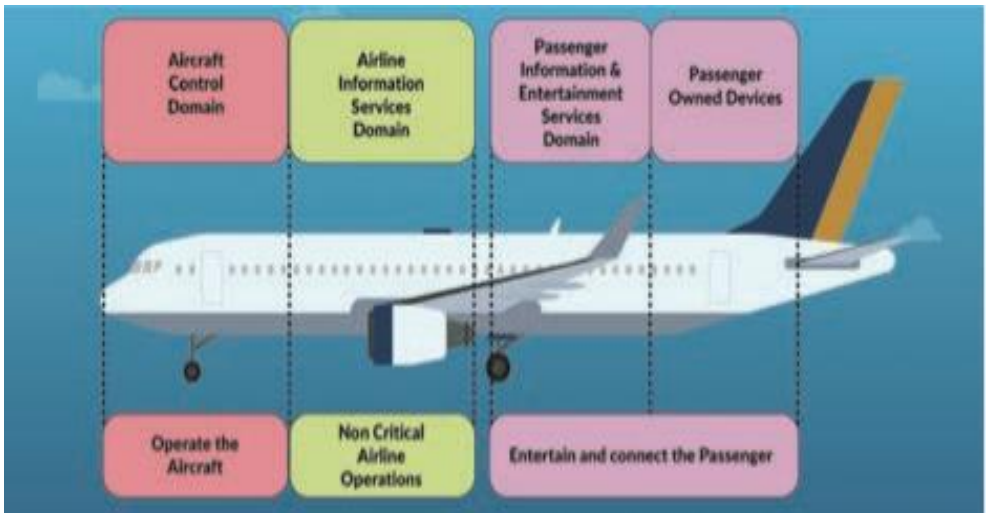
SECTION 1. Les constructeurs

Il est admis que la transformation digitale est en cours au sein du transport aérien. Des innovations connectées apparaissent pour améliorer la performance des aéronefs et des infrastructures. Ainsi, les constructeurs ont pour objectif d'augmenter l'automatisation et l'inter-connectivité dans le cockpit.

Ont été précédemment évoquées les nouvelles innovations connectées, sans pour autant citer les nouveaux risques cyber qu'elles engendrent.

Afin d'illustrer le cas de ces nouveaux risque cyber, nous prendrons donc comme exemple le cockpit connecté.

Voici un schéma issu d'une présentation de l'AESA qui permet de comprendre ce que l'on entend par « cockpit connecté » :



Ici, l'AESA nous présente un schéma d'un avion connecté. Il s'agit du même schéma qu'utilise l'Académie de l'air et de l'espace dans son dossier « cyber menaces dans le transport aérien » pour évoquer les risques cyber liés à l'aéronef.

L’on peut voir à travers ce schéma que les aéronefs du futur seront entièrement connectés, que ce soit au niveau du cockpit et même de la cabine. Le 26 novembre 2019, à Toulouse, Thales présenta son nouveau système de gestion de vol surnommé PureFly. Il s’agit d’un tout nouveau système FMS (Flight Management système). D’après Paul Ebanga, Vice-Président de Thales :

« *Le FMS c'est un peu le « cerveau » de l'avion, toute l'électronique qui permet la préparation du vol, qui calcule et transmet les informations de vol à l'équipage, fixant les paramètres de vol et qui assure le guidage de l'aéronef au fur et à mesure de l'avancement du plan de vol, calculant notamment les procédures d'approche et d'atterrissage* »,[49]

Ces nouvelles connections ouvrent la possibilité à des cyberattaques. En effet, des hackers mal intentionnés pourraient envoyer à l’aéronef des mauvaises données durant la phase de vol, ce qui perturberait ainsi la sécurité du vol.

Après le 11 septembre 2001, la décision a été prise de sécuriser le cockpit. A la suite de l’accident de la Germanwing en 2017, le cockpit est devenu encore plus sécurisé.

Malgré le fait que le cockpit soit sécurisé physiquement, l’ouverture à la connectivité ne le rend plus aussi étanche qu’auparavant.

Ainsi, les constructeurs devront être vigilants quant au développement des innovations connectées.

[49] https://www.industrie-techno.com/article/a-toulouse-thales-devoile-son-cockpit-du-futur.58339

SECTION 2. Les compagnies

"*Être compétent en cybersécurité sera bientôt aussi important que de parler anglais" considère* Marc Leymonirie, responsable de la cybersécurité chez AirFranc KLM.[50]

En réalité, les compagnies aériennes ne peuvent plus se passer des innovations connectées. Elles adoptent même des stratégies pour devenir encore plus digitales. Par exemple, Air France a ouvert la Digital Factory dirigée par Amel Hammouda, Directrice de la Transformation d'Air France. Pour Air France, il faut même accélérer la transformation digitale des compagnies aériennes. [51]

Tout d'abord, avec la digitalisation, les compagnies traitent de plus en plus de data[52]. La data correspond à la donnée informatique. Les compagnies aériennes traitent surtout ce que l'on appelle la Data sensible.[53]

Toutes ces nouvelles innovations imposent aux compagnies aériennes d'être vigilantes en matière de protection des données personnelles. Le risque cyber est très présent ces dernières années.

Prenons là encore le cas d'Air France, qui, même dans ces processus interne, a commencé sa transformation digitale. Cela entraine des gains de performance pour les compagnies, mais cela ouvre aussi la porte au risque de ransomware. Un

[50] https://www.usine-digitale.fr/article/etre-competent-en-cybersecurite-sera-bientot-aussi-important-que-de-parler-anglais.N339247

[51] https://www.tom.travel/2018/11/09/comment-air-france-exploite-t-elle-le-digital-en-interne-et-en-externe%E2%80%89/

[52] Données

[53] L'article 9 du RGPD définit ce que sont les données sensibles comme suit : "Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits."

ransomware est un logiciel malveillant qui perturbe l'activité d'une entreprise. Pour pouvoir continuer son activité normalement, les criminels demandent une rançon aux victimes.

Dans le cas d'une compagnie aérienne, cela pourrait avoir des conséquences terribles.

Pour conclure, les compagnies aériennes ont une réelle épée de Damoclès au-dessus d'elles en matière de cybersécurité. Les datas doivent être sécurisées mais le réseau interne nécessaire au bon fonctionnement de la compagnie doit l'être également. Les compagnies aériennes travaillent en coopération avec les aéroports qui sont, comme vu dans la partie précédente, eux aussi en pleine transformation digitale.

SECTION 3. Les aéroports

En 2018, le Clusif (Club de la sécurité de l'information français) [54], dans son rapport annuel, alerta les aéroports de leur exposition face aux risques cyber. Ils mettent en avant les fait que les aéroports sont une cible de choix en matière de cyber-attaque, que ce soit de la part des Etats, pour perturber un ennemi, ou bien de la part d'individus ayant pour objectif l'appât du gain.

Il faut comprendre que les aéroports sont les garants du bon fonctionnement du transport aérien de passagers. Dans la partie précédente, nous avons évoqué les nouvelles innovations des aéroports connectés.

[54] Le CLUSIF, Club de la sécurité de l'information français, est une association indépendante de professionnels de la sécurité de l'information réunissant des Utilisateurs et des Offreurs de tous les secteurs d'activité de l'économie.

Ces innovations ouvrent des failles pour les aéroports. Entre les objets connectés en 5G tels que les voitures autonomes qui peuvent être piratées, ainsi que les véhicules sur piste qui deviennent aussi connectés, l'aéroport fait face à un risque accru en matière de cybersécurité.

Nous avons également évoqué les ransomware ainsi que les tableaux d'affichage dans les aéroports et leurs disponibilités. En 2020, à l'aéroport de Bristol, en Angleterre, une actualité est venue confirmer les théories des experts en cybersécurité. En effet, les tableaux d'affichage ont été éteints tout un week-end à cause d'un ransomware.

Image des tableaux d'affichage de l'aéroport de Bristol :

Pour continuer à opérer, les responsables de l'aéroport ont dû utiliser des tableaux d'affichage manuscrits durant tout le week-end. Aucun retard n'a été déploré.

En apparence, la transformation digitale des aéroports est donc un avantage pour le transport aérien. En revanche, elle fait émerger de nombreux risque cyber. Les aéroports sont déjà des cibles privilégiées d'attaques malveillantes.

Les aéroports doivent aussi se concentrer sur la disponibilité et l'intégrité de leurs

données. Les appareils ne doivent pas subir de ralentissement ou des bug qui pourraient gêner l'activité.

Au sein de la première partie, nous avons défini le secteur aérien comme un système interdépendant et connecté. Nous sommes revenus sur l'histoire du transport aérien pour comprendre que le développement technologique a toujours été lié au transport aérien.

La cybersécurité du transport aérien existe donc bel et bien, et devient de plus en plus présente au vu des évolutions connectées de ces dernières années. Dorénavant, il s'agit de s'interroger sur l'encadrement de la cybersécurité du transport aérien.

PARTIE 2. UN DROIT DE LA CYBERSECURITE DU TRANSPORT AERIEN INDISPENSABLE A LA CYBER RESILIENCE

Le transport aérien a toujours été très régulé comme on a pu le constater à travers l'histoire du transport aérien. Dès le départ, les Etats ont voulu créer un cadre strict pour le développement du transport aérien. L'on a vu que ces règles étaient regroupées dans une matière qu'est le droit aérien.

Le transport aérien a constamment réglementé ses activités par rapport aux évolutions de son environnement. En effet, il est possible de citer comme exemple le renforcement des règles de sécurité après le 11 septembre, ou encore les règles de certification aéroportuaire en matière environnementale. Ainsi, le corpus

règlementaire du transport aérien fait l'objet d'un perpétuel enrichissement.

L'apparition du risque cyber force les Etats et les organisations de l'aviation civile à créer des textes ou à se servir de dispositions existantes pour créer un cadre en matière de cybersécurité.

Le but pour l'aviation civile, comme le précise l'OACI dans sa stratégie, c'est d'être cyber-résiliente. Pour l'OACI, la cyber résilience du transport aérien passe par un cadre règlementaire harmonisé entre tous les Etats mais aussi par un partage de l'information.

A travers cette partie, nous allons tout d'abord étudier le développement d'un cadre juridique propre à la cybersécurité du transport aérien (TITRE 1), puis démontrer en quoi toutes ces dispositions vont permettre la cyber résilience du transport aérien (TITRE 2).

TITRE I. DEVELOPPEMENT D'UN CADRE JURIDIQUE PROPRE A LA CYBERSECURITE DU TRANSPORT AERIEN

« Si la cybersécurité n'a pas de prix, elle a son droit ! » [55]

Le droit a souvent accompagné le développement des activités humaines. Tout d'abord, donnons une définition de ce qu'est le droit. L'auteur Dreier définit le droit comme « la totalité des normes appartenant à la constitution d'un système de normes organisé par l'Etat ».

Le droit fait partie de la société. Il codifie les activités humaines et participe à leur développement ainsi qu'à leur fonctionnement. Qu'en est-il en matière de cybersécurité ?

[55] Alexandre MALAFAYE en préface du livre de François Gorriez « Le droit de la cybersécurité »

La cybersécurité est un domaine récent pour le juriste. On voit se développer le droit de l'internet. Plus récemment, certains auteurs évoquent le droit de la cybersécurité. En effet, c'est le cas pour François Gorriez, auteur du livre « Le droit de la Cybersécurité » publié en 2020 ». Pour son auteur, des règles de droit particulières sont applicables à la cybersécurité, ce qui caractérise l'empreinte légale de la cybersécurité, et qui sont encore appelées « droit de la cybersécurité » (Chapitre 1).

Le transport aérien ne déroge pas à la règle. Nous avons évoqué précédemment le droit aérien. On considère le droit aérien comme l'ensemble des normes qui viennent régir l'activité aérienne. Il existe donc un droit aérien.

Le droit aérien est un domaine vaste avec de multiples sous-domaines tels que le droit des passagers ou le droit social spécifique au transport aérien.

In fine, l'on pourrait se demander si les nouvelles règles de droit en matière de cybersécurité dans le transport aérien ne pourraient pas être compilées dans un sous domaine : Le droit de la cybersécurité du transport aérien (Chapitre 2).

CHAPITRE 1. Le droit de la cybersecurité

Pour appréhender ce que pourrait être le droit en matière de cybersécurité du transport aérien, il faut comprendre le droit de la cybersécurité. Dans cette partie, nous verrons de quelle manière s'est développé le droit de la cybersécurité. Nous étudierons la naissance de ce nouveau domaine du droit aussi bien au niveau international (Section 1), communautaire (Section 2) que national (Section 3).

SECTION 1. Le droit de la cybersécurité sur le plan international

Dans cette section, nous verrons en premier lieu l'existence d'institutions internationales en matière de cybersécurité (A). Nous verrons, en second lieu, s'il existe des textes juridiques à portée internationale en matière de cybersécurité (B).

A. Une volonté de normes internationales communes en matière de cybersécurité difficile à concrétiser

En 2009, la Chine et la Russie, connues pour avoir une politique assez floue en matière de cybersécurité, ont pourtant proposé un code de conduite à l'assemblée générale des nations unies (ONU)[56]. Les pays occidentaux ont rejeté cette proposition.

A la suite de cela, l'assemblée générale des Nation Unies a adopté en novembre 2011 la résolution 65/41 :[57] « *une **résolution** du Conseil de sécurité des Nations unies est un texte ayant une valeur juridique contraignante, contrairement à une **résolution** de l'Assemblée générale* ».

Cette résolution invite l'ONU à reprendre les travaux en matière de cybersécurité notamment sur la recherche d'un consensus de normes dans le cyberespace.

Depuis, plus aucun travail n'a été entrepris au niveau international pour définir des normes communes en matière de cybersécurité. La cause principale est que le domaine de la cybersécurité présente un atout stratégique pour les Etats. Certains ont également peur de la puissance des Etats Unis et de leur volonté à imposer leur vision au niveau international.

B. Une carence de textes au niveau international

[56] https://www.senat.fr/rap/r11-681/r11-68113.html

[57] https://www.capital.fr/entreprises-marches/thales-alerte-sur-la-multiplication-des-cyberattaques-des-etats-1366176

La cybersécurité étant stratégique pour les Etats, ces derniers n'ont pas réussi à mettre en place des organes régulateurs. Si une infraction en matière de cybersécurité est commise, alors c'est le droit du territoire national qui s'applique.

Oriane Barat-Ginies, conseillère juridique au centre interarmées de concept, de doctrine et d'expérimentation (CICDE), a écrit, en 2014, un article de recherche autour de la question suivante : « Existe-il un droit international du cyberespace ? ». La chercheuse en droit s'est intéressée aux accords diplomatiques et juridiques dans le cyber face aux divergences nationales.

Selon elle, malgré les tentatives de développement d'un « arsenal juridique international » en matière cybersécurité, les états développent en interne leurs propres visions. Ils proposent ainsi un arsenal juridique afin de se servir du droit de la cybersécurité pour protéger leurs intérêts.

La chercheuse évoque aussi le Manuel de Tallinn. Il s'agit d'un outil pour les juristes qui consiste en « *une analyse de haut niveau des problématiques d'interprétation du droit actuel au regard des nouveaux enjeux du cyberespace. Il est également utile pour les institutions gouvernementales ou tout organisme civil ou militaire (national ou régional, technique ou non technique) souhaitant avoir une vision globale des enjeux juridiques internationaux liés à ce nouveau champ* ».

Le manuel de Tallinn n'a pas de valeur juridique. Il n'est donc pas contraignant. Cet ouvrage élaboré par des experts qui ont pu aboutir à 95 règles de droit général est une piste de réflexion pour créer un cadre international en matière de droit du cyber espace.

L'Europe, arborant sûrement une volonté stratégique d'unir ses Etats membres en matière de cybersécurité face aux géants mondiaux, a rapidement mis en place des normes communautaires en matière de cybersécurité.

SECTION 2. Le droit de la cybersécurité au niveau communautaire

Dans une première partie, nous reviendrons sur l'histoire de l'encadrement juridique de la cybersécurité par l'Europe. Pour ce faire, nous évoquerons les institutions créées, garantes du développement des normes cyber. (A) Puis, nous étudierons le corpus de textes européens en matière de cybersécurité, comme la directive NIS, ou bien le Règlement des données personnelles, autrement dit RGPD (B).

A. L'émergence d'une politique et d'une stratégie spécifiques de l'Europe face au défi de la cybersécurité

Jean-Claude Juncker, ancien président de la Commission européenne, considère que « les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars »[58].

L'Europe prend conscience qu'elle doit construire un environnement de cybersécurité entre tous ses états membre.

A partir de 2016, le Conseil Européen, [59] convient des étapes à mettre en place pour arriver à une politique commune en matière de cybersécurité. Le conseil européen arrive aux conclusions suivantes en matière de justice pénale dans le cyberespace :

[58] Discours sur l'état de l'Union, septembre 2017

[59] Le Conseil européen est une institution qui réunit les chefs d'État ou chefs de gouvernement des vingt-sept États membres de l'Union européenne, sous la tutelle d'un président chargé de faciliter l'apparition d'un compromis

-Rationalisation des procédures d'entraide judiciaire,

-L'amélioration de la coopération avec les fournisseurs de services,

-Le lancement d'un processus de réflexion sur les éventuels critères de rattachement aux fins de la détermination de la compétence d'exécution dans le cyber espace.

On voit bien que l'Union Européenne a décidé de se rendre compétente en matière de cybersécurité. Pour cela, elle va mettre en place des institutions et des agences européennes pour pouvoir réguler le cyberespace européen, et par extension la cybersécurité.

On peut citer dans l'ordre chronologique la création en 2017 de la **CRET-UE** autrement dit une équipe permanente d'intervention en cas d'urgence informatique.

Au départ, la **CERT-UE** avait pour vocation « *d'apporter une réponse coordonnée de l'Union Européenne aux cyberattaques visant ses institutions*[60]. » Nous verrons plus tard qu'en France - celle-ci s'étant inspirée du modèle européen - s'est développé le CERT-FR.

En 2018, Le Conseil entame des négociations avec le Parlement européen,[61] dans l'objectif d'un accord concernant le règlement sur la cybersécurité. Nous développerons plus tard ce qu'est précisément ce règlement. En ce qui concerne les institutions européennes régulatrices en matière de cybersécurité, il prévoit de moderniser l'Agence de l'union européenne chargée de la sécurité des réseaux et de l'information, l'ENISA.

[60] https://www.consilium.europa.eu/fr/policies/cybersecurity/

[61] « *Le Parlement européen est l'organe parlementaire de l'Union européenne élu au suffrage universel direct. Il partage avec le Conseil de l'Union européenne le pouvoir législatif de l'Union européenne* ».

L'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est une agence européenne.[62] Elle est créé le 10 mars 2004 par un règlement de l'Union européenne (Règlement CE no 460/2004 du Parlement européen et du conseil). Au départ, elle a pour objectif d'encadrer les réseaux de l'information. La cybersécurité n'était pas encore un risque prégnant pour l'Europe. Elle a par la suite évolué, et aujourd'hui grâce au CybersécuritAct adopté par le Conseil de l'union et le parlement européen. Elle est aujourd'hui en charge de la cybersécurité de l'Union Européenne au travers d'un mandat permanant. Nous étudierons ensuite le CybersecurityAct.

Dans le but de créer un marché unique numérique au sein de l'Europe, la Commission Européenne a créé un Commissaire européen à la société numérique. Ce commissaire s'appuie notamment sur l'aide de la direction générale des réseaux de la communication, du contenu et des technologies, autrement appelé DG CONNECT. La DG CONNECT va de plus en plus étendre son rôle. Elle se rapproche même de la direction générale de la mobilité et des transports (DG MOVE) dans le cadre d'expérimentation du fait de l'évolution du transport en Europe.

En conclusion, l'Union Européenne considère la cybersécurité comme un domaine stratégique, l'on peut même dire vital, pour la continuité de l'Europe. Ce domaine qu'est la cybersécurité est aussi récent que la construction européenne. Avoir une Europe forte en matière de cybersécurité permet de résister aux tensions mondiales dans le cyberespace. Pour avoir une Europe forte, cela passe, comme nous l'avons vu, dans un premier par la construction d'une **politique et d'une stratégie en matière de cyber sécurité.** Dans un second temps, il faut que cette volonté soit

[62] *« Créée en 2004, l'ENISA joue un rôle clé en matière d'aide au développement des capacités nationales de cybersécurité et de soutien à la coopération entre les Etats membres. Elle est placée sous l'autorité d'un conseil d'administration composé de représentants des 28 Etats membres de l'UE et de deux représentants de la Commission européenne. Le Conseil d'administration, dont la France assure la présidence depuis 2016,et est notamment chargé d'adopter le programme de travail annuel de l'ENISA, ainsi que son budget et son plan en matière de personnel. »*

accompagnée d'un corpus juridique, permettant d'agir et d'encadrer la cybersécurité à l'échelle européenne.

B. La naissance d'un droit de la cybersécurité européen

L'Union européenne a très vite eu sa propre vision en ce qui concerne la cybersécurité.

Dans cette partie, nous allons nous concentrer sur les trois grands textes qui viennent construire l'Europe de la cybersécurité. Tout d'abord, est apparue la directive « Network and Information System Security appelée aussi NIS. Ensuite, a été adopté le règlement général sur la protection des données, (règlement n°2016/679°) appelé RGPD puis le règlement sur la cybersécurité (Règlement 2019/881°), appelé aussi CyberSécurity Act.

Nous n'étudierons pas en détail ces règlements dans cette étude. Nous présenterons seulement le but et l'objectif de ces textes afin de comprendre leur possible impact sur le transport aérien.

La directive européenne 2016/1148, appelée directive NIS, a pour objectif : « *d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'informations de l'Union Européenne*[63]. » Elle définit alors des mesures permettant d'atteindre ce but. La directive NIS crée des nouvelles catégories d'acteurs. Ces acteurs spécifiques devront être soumis à des mesures plus contraignantes en matière de cybersécurité :

- Les opérateurs de services essentiels « OSE »,

-Les fournisseurs de services numériques « FSN »

[63] ANSSI

Dans notre étude, ce sont les OSE qui nous intéressent. En effet, ces derniers sont définis dans la directive par rapport à leurs activités. La directive identifie six secteurs clé en matière de protection des systèmes d'information : l'énergie, le transport, les banques, infrastructures de marchés financiers, santé, fourniture et distribution d'eau potable, infrastructures numériques.

Les opérateurs du secteur du transport son identifiés par la directive comme étant des OSE. La directive s'applique donc au transport aérien.

« *Les OSE devront en vertu de la directive NIS :*

- *Prendre les* ***mesures techniques et organisationnelles nécessaires, proportionnées et adaptées*** *à la gestion des risques menaçant la sécurité des réseaux et des systèmes d'information ;*
- *Prendre* ***les mesures appropriées pour prévenir les incidents*** *qui compromettent la sécurité des réseaux et systèmes d'information ;*
- ***Veiller à notifier à l'ANSSI*** *(« Agence nationale de la sécurité des systèmes d'information »), sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels, dès qu'ils en ont pris connaissance.* »[64]

Ensuite, nous avons le **Règlement général sur la protection des données personnel**, dit RGPD (2016/679). L'Objectif de ce règlement est d'harmoniser le droit européen en matière de protection des données personnelles. Ce règlement est applicable depuis le 25 mai 2018. Le RGPD est un règlement complexe qui est étudié par de nombreux juriste du droit du numérique. Il définit aussi les relations avec les partenaires commerciaux des entreprises en matière de données. Le RGPD comporte également un volet RH concernant les données personnelles des salariés des entreprises.

[64] http://www.staub-associes.com/transposition-de-la-directive-nis-en-droit-francais/

Le RGPD concerne tous les secteurs donc le transport aérien n'y échappe pas. Beaucoup de questions se posent concernant son articulation avec le PNR.

Doit-on considérer les données du secteur aérien comme spéciales ? Doit-on avoir un règlement spécifique pour les acteurs du transport aérien afin de maintenir le plus haut niveau de sécurité et de sûreté du transport aérien ? La crise du coronavirus nous prouve que dans le transport aérien la question du traitement de la donnée personnelle est spécifique à l'activité.

Enfin, le CybersécurityAct est le tout dernier texte européen, et le plus récent en matière de cybersécurité. Ce règlement constitue une réelle avancée en matière de cybersécurité.

En effet, il renforce les compétences de l'ENISA. Cette dernière devait voir son mandat se terminer en 2020 avec l'objectif du marché unique numérique. Mais à la suite du Cybersécurity Act, le mandat de l'ENISA est devenu permanent. Ainsi, pour faire face au risque cyber, l'Europe a attribué de nouvelles compétences à l'ENISA (lesquelles ?)

La question se pose si l'ENISA va également s'immiscer dans les affaires du transport aérien. Il est précisé dans les textes que les réseaux des domaine vitaux doivent être sécurisés. Le transport étant un des domaines relevés par le directive NIS, l'ENISA est dopée par conséquent d'un pouvoir règlementaire.

L'autre point important du CybersécurityAct est la volonté d'instaurer une politique de certification en matière de cybersécurité au niveau européen. Au vu du développement des objets connectés (appelé aussi Iot), l'Union européenne a l'objectif de créer un cadre de certification de sécurité de ses innovations[65]. Ce cadre législatif est une avancée majeure en matière de cybersécurité. Il harmonise

[65] **Article** 73 du Règlement 2019/881 en matière de cybersécurité, sur la régulation des **objets connectés**

la sécurité des objets connectés au niveau européen, tout en permettant une transparence du marché[66].

L'on a pu voir dans la partie précédente que la transformation digitale du transport aérien a entrainé l'apparition de multiples objets connectés. Du fait de sa spécificité, le transport aérien devra-t-il procéder à du lobbying pour disposer de ses propres règles en matière de certification d'objets connectés ? C'est déjà le cas pour les appareils de navigation aérienne.

En conclusion, l'Europe a donc légiféré en matière de cybersécurité, créant ainsi un réel cadre législatif. Cependant, l'une des particularités du droit communautaire est qu'il doit être transposé en droit national.

SECTION 3. Le droit de la cybersécurité au niveau national

En France, l'Agence nationale de la sécurité des systèmes d'information, autrement appelé l'ANSSI, créée par décret en juillet 2009, est l'institution nationale par excellence en matière de cybersécurité. (A). La France dispose aussi d'un fort cadre législatif en matière de cybersécurité issu de sa volonté propre mais aussi de la transposition des normes européennes (B).

A. L'ANSSI, le Cerbère[67] de la cybersécurité française

Créée en juillet 2009, à la suite du « Livre blanc 2013 »[68], l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a pour mission de sécuriser les

[66] https://www.datanaos.com/blog/Le-cybersecurity-act-la-sentinelle-contre-les-cybermenaces

[67] « *Dans la mythologie **grecque**, Cerbère (en **grec** ancien Κέρβερος / Kérberos) est le chien à trois têtes gardant l'entrée des **Enfers**, empêchant les morts de s'échapper de l'antre d'Hadès et des vivants de venir récupérer certains morts* ».

[68] « *Le Livre blanc sur la défense et la sécurité nationale 2013, publié le 29 avril 2013, est un livre blanc chargé de définir une stratégie globale de défense et de sécurité pour la France* » La France place la cybersécurité comme cruciale au niveau stratégique.

systèmes d'information, des administrations et ceux des entreprises dénommés « opérateurs d'importance vitale », les OIV.

Les OIV ont été définis dans l'article 22 de la loi de programmation militaire (loi n°2013-1168 du 18 décembre 2013). D'après le site de l'ANSSI, « *la France est le premier pays à s'appuyer sur la réglementation pour définir un dispositif efficace de cybersécurité de ses infrastructures d'importance vitale* » [69].

L'ANSSI est considérée comme une véritable autorité nationale en matière de cybersécurité et de cyberdéfense. L'ANSSI a pour mission l'élaboration des textes règlementaires. Elle co-construit les textes avec les parties prenantes au travers de groupes de travail avec les différents secteurs concernés par les OIV.

Ci-dessous, une chronologie de l'ANSSI issue des informations du site internet :

« 2016/2017 Entrée en vigueur des mesures de cybersécurité

Suite aux groupes de travail, l'ANSSI propose une réglementation adaptée aux secteurs d'activité. Les premiers arrêtés sont signés par le Premier Ministre et définissent les critères d'exécution des mesures qui entreront en vigueur au 1er juillet 2016.

2014/2016 Lancement des groupes de travail

Pour chaque secteur d'activité, les groupes de travail regroupent autour de l'ANSSI les OIV, le ministère coordonnateur et les autorités de régulation. Les règles de sécurité et les délais d'application sont discutés entre les différentes parties prenantes.

2014/2015 Définition des modalités d'application de la LPM

Le décret d'application de l'article 22 de la LPM précise les modalités d'application des nouvelles mesures de cyber sécurité. Il est accompagné d'un décret sur la qualification. 2014/2015

2013 : Adoption de la loi de programmation militaire

La LPM est l'outil législatif qui va permettre aux opérateurs publics et privés critiques pour la Nation de mieux se protéger et à l'ANSSI de mieux les soutenir en cas d'attaque informatique. 2013

[69] https://www.ssi.gouv.fr/actualite/cybersecurite-des-oiv-publication-dun-nouvel-arrete-pour-le-secteur-nucleaire/

2013 : Le livre blanc 2013

L'Etat prend en compte les enjeux de cybersécurité des opérateurs vitaux pour la Nation lors de la définition des grandes orientations stratégiques en matière de Défense et de sécurité nationale. »[70]

Certains aéroports sont concernés par la Loi de programmation militaire et définis par celle-ci comme des opérateurs d'importance vitale. Nous verrons dans la suite de notre étude quelles sont plus précisément les obligations qu'entraine cette loi pour le transport aérien.

B. Arsenal juridique français en matière de cybersécurité

Comme vu à travers l'histoire de l'ANSSI, la France est l'un des premiers pays européens à se doter d'un véritable corpus règlementaire en matière de cybersécurité.

Nous nous attarderons dans cette partie à développer ce que l'on considère comme les principaux textes juridiques en matière de cyber sécurité :

- La loi informatique et libertés.
- La loi de programmation militaire (Code de la défense)
- Arrêté du 18 mai 2018 concernant les drones

L'on peut distinguer deux périodes. La période avant la prise de position européenne en matière de cybersécurité, et la période post prise de conscience

[70] ANSSI 2020

européenne. Effectivement, de nombreux textes juridiques français sont issus de la transposition du droit communautaire en matière de cybersécurité.

Le RGPD, la directive NIS ainsi que le Cybersécurityact ont été transposés dans le droit français, comme l'exigent les règles de l'Union Européenne dans la Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité. Nous ne nous attarderons pas sur ces transpositions car nous avons déjà présenté les textes originaux.

Nous présenterons donc les 4 textes précédemment cités.

- **La loi informatique et libertés du 6 janvier 1978 :**

En matière de cybersécurité, et donc par extension de protection de la donnée personnelle, l'on évoque souvent le RGPD comme une incroyable avancée. C'est oublier que la France, avant la transposition du RGPD dans la loi informatique et libertés, avait déjà institué des règles en matière de protection de la donnée. En effet, si la loi informatique et libertés vient être réécrite en 2018[71] en incluant le RGPD, c'est parce qu'elle présentait des défauts.

Le titre 1er, chapitre 1 Principe et définitions de la loi informatique et libertés dispose : « ***Article 1er*** *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale.* ***Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques****. Les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant et les obligations incombant aux personnes qui traitent ces données s'exercent dans le cadre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 et de la présente loi* »

71

- **La Loi de Programmation Militaire :**

L'article 22 de la loi de programmation militaire (LPM), qui a été promulguée le 18 décembre 2013, prévoit l'adoption de renforcement de la sécurité des OIV. Comme vu précédemment « *Un OIV (Opérateur d'Importance Vitale) est un organisme, privé ou public, qui exerce des activités comprises dans un secteur* ***d'activité d'importance vitale*** *; gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de* ***survie de la Nation*** *ou de mettre gravement en cause la santé ou la vie de la population* ».[72]

« *Pour faire face aux nouvelles menaces cyber, l'article 22 de la LPM, qui fait suite aux préconisations du Livre Blanc sur la défense et la sécurité nationale de 2013, rajoute une pierre à l'édifice en imposant aux OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale* », d'après l'ANSSI.

Ainsi la Loi de programmation militaire devient une véritable pierre angulaire en matière de cybersécurité. Elle impose différentes obligations pour ces mêmes OIV, comme le fait de faire part de tout accident/incident de sûreté de leurs systèmes d'information.

L'arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Transport aérien » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10

[72] https://www.oodrive.fr/blog/reglementation/securite-des-systemes-dinformation-des-oiv-une-legislation-stricte-pour-proteger-les-entreprises-strategiques/

du code de la défense, vient préciser pour le transport aérien les modalités d'application de l'article 22 de la Loi de Programmation Militaire.

- **Arrêté du 18 mai 2018 relatif aux exigences applicables aux télé pilotes qui utilisent des aéronefs civils circulant sans personne à bord à des fins autres que le loisir :**

L'article de Laurent Archambault, « Le concept de « privacy by design » à la rescousse des drones civils européens », nous explique comment un texte européen a forcé les constructeurs de drone à prendre des mesures de cybersécurité. L'auteur n'utilise à aucun moment le terme cybersécurité mais il est sous-entendu à chacun des paragraphes. « *Le concept de Privacy by Design ou de « protection de la vie privée dès la conception » impose aux entreprises de mettre en œuvre des mesures de protection dès la conception et lors de chaque utilisation de nouvelles technologies. Il concerne donc potentiellement aussi bien les centres de R&D, les fabricants que les opérateurs de drones*. »[73]

Ainsi l'Europe, et par extension la France, ont obligé les entreprises du secteur du drone à prendre des mesures en matière de cyber sécurité. Ce sont des textes règlementaires de cybersécurité qui répondent à la spécificité des drones, composantes du système aérien.

Pour François Gorriez, « *le droit de la cybersécurité se caractérise en premier lieu par une gouvernance juridique consistant à mettre en œuvre un système global et technologique de respect du droit. Il en est par exemple ainsi de l'obligation de « protection by design » imposant de prendre les mesures nécessaires pour toute nouvelles technologie traitant de données à caractère personnel garantisse dès sa conception et lors de son utilisation un haut niveau de protection de ces données*. » Ainsi, il existe bien un droit de la cybersécurité, agile et réactif.

[73] https://www.aerobuzz.fr/debat/le-concept-de-privacy-by-design-a-la-rescousse-des-drones-civils-europeens/

Dès lors, l'on pourrait s'interroger sur le cas d'une sous-catégorie du droit aérien, qui rassemblerait toutes les règles en matière de sécurité des systèmes d'information, de protection des données et même de certification. Ce sous-domaine pourrait se nommer « Le droit de la cybersécurité aérienne » ou autrement dit « le droit de la cybersécurité du transport aérien. »

CHAPITRE 2. Le droit de la cybersécurité du transport aérien

« *L'objectif principal de la* ***législation et de la réglementation*** *internationales, régionales et nationales* ***sur la cybersécurité de l'aviation civile*** *est d'appuyer la mise en œuvre d'une stratégie exhaustive de cybersécurité afin de protéger l'aviation civile et les voyageurs des effets des* ***cyber dysfonctionnements*** **» OACI, 2019**

Comme vu précédemment, le transport aérien est un secteur très codifié. Le cadre juridique du transport aérien s'est développé depuis 1929 jusqu'à nos jours. Ce cadre juridique strict est le ciment de la sécurité et la sûreté du transport aérien.

Depuis quelques temps le transport aérien commence à être règlementé en matière de cybersécurité. L'on voit apparaitre des lois, des règlements ainsi que d'autres textes spécifiques (comme les certifications) en matière de cybersécurité. Tous ces textes ont été regroupés dans une sous matière que l'on a appelée « droit de la cybersécurité de l'aérienne ». Nous étudierons dans ce chapitre toutes ces normes et institutions juridiques qui concernent la cybersécurité du transport aérien au niveau international (Section 1), communautaire (Section 2) et national (Section 3).

SECTION 1. L'OACI, vision d'une stratégie en matière de cybersécurité

Nous verrons dans cette section la prise de conscience de l'OACI en matière de risque cyber (A), associée à cette volonté d'avoir une stratégie et une vision en la matière (B).

A. L'OACI au-devant de la cybersécurité du transport aérien

L'OACI accompagne le développement du transport aérien comme nous l'avons présenté précédemment dans ce mémoire. L'organisation de l'aviation civile internationale joue un rôle primordial dans la réglementation internationale du transport aérien. L'OACI dispose en effet d'un pouvoir normatif à travers l'annexe de la convention de Chicago du 7 décembre 1994. Elle fonctionne grâce à des normes et pratiques recommandées, les « SARPS » dit en anglais « standards and recommanded pratices ».

L'OACI met aussi en place des politiques ainsi que des stratégies. *« Ces SARP et politiques sont utilisées par les États membres de l'OACI pour s'assurer que leurs opérations et réglementations locales d'aviation civile sont conformes aux normes mondiales, ce qui permet au réseau mondial de transport aérien*[74] *d'exploiter plus de 100 000 vols par jour, en toute sécurité et avec efficacité dans toutes les régions du monde ».*

Nous ne développerons pas le fonctionnement juridique de l'OACI, de très bonnes études existant pour expliquer le fonctionnement du Conseil ainsi que de l'Assemblée.

En ce qui concerne la cybersécurité, la prise de conscience de l'OACI peut être considérée comme tardive. Les premiers travaux en matière de cybersécurité remontent à 2016.

En effet, à la suite de la 39ème session du 6 octobre 2016, l'OACI vote sa première résolution en matière de cybersécurité : la résolution A39, Cybersécurité dans

[74] ICAO site internet

l'aviation civile[75]. Cette résolution est la première pierre de la construction de normes en matière de cybersécurité dans le transport mondial. Elle nous rappelle tout d'abord que le transport aérien est un transport connecté : « ***Considérant*** *que le système mondial de l'aviation est un système éminemment complexe et intégré constitué de technologies de l'information et des communications essentielles à la sécurité et à la sûreté des vols d'aviation civile,*

Notant *que le secteur de l'aviation dépend de plus en plus de la disponibilité des systèmes de technologies de l'information et des communications, ainsi que de l'intégrité et de la confidentialité des données*, ». L'OACI rappelle aussi que le transport aérien dépend de ces données.

L'OACI reconnait également la particularité de la cybersécurité du transport aérien que nous avons affirmée dans ce mémoire : « *Reconnaissant que tous* ***les problèmes de cybersécurité qui compromettent la sécurité de l'aviation civile ne sont pas illégaux et/ou intentionnels****, et devraient donc être traités par l'application de systèmes de gestion de la sécurité. En effet l'OACI reconnait que la cybersécurité ne concerne pas seulement la sûreté mais aussi la sécurité, et même parfois les deux.* »

Ainsi, l'OACI, « *invite les États et les parties prenantes de l'industrie à prendre des mesures pour contrer les cybermenaces auxquelles est confrontée l'aviation civile* ».

La résolution 39 A 19, charge le Secrétaire général :

« a) d'aider les États et l'industrie à prendre ces mesures et de leur faciliter la tâche en ce sens ;

d) de veiller à ce que les questions de cybersécurité soient dûment examinées et coordonnées dans toutes les disciplines pertinentes de l'OACI. »

[75] ASSEMBLÉE – 39e SESSION Montréal, 27 septembre – 6 octobre 2016

L'OACI, au travers de cette résolution de l'Assemblée, prouve que la cybersécurité et sa réglementation vont devenir un enjeu crucial pour le transport aérien.

B. L'affirmation de la stratégie de l'OACI concernant la cybersécurité de l'aviation

En 2019, l'édition du Plan mondial de navigation aérienne (doc9570) réaffirme l'importe de la cybersécurité pour le transport aérien. L'on évoque même la cyber résilience.

A la suite de la 39ème Assemblée, de multiples groupes de travail, ainsi que de conférences vont avoir lieu pour mettre en place la stratégie mondiale en matière de cybersécurité du transport aérien.

L'on peut citer par exemple « La deuxième conférence de haut niveau de la sûreté de l'aviation (hlcas/2) » qui a eu lieu à Montréal du 29 au 30 novembre 2018. Les objectifs de cette conférence sont en lien avec le Plan pour la sûreté de l'aviation dans le monde, autrement appelé GASep. Cette conférence reconnait que la question de la cybersécurité est une préoccupation pour la communauté de l'aviation. Elle fait également remarquer que plusieurs parties prenantes associées au transport aérien sont concernées par le problème de la cybersécurité. Cette conférence amorce la volonté de mettre en place une véritable stratégie en matière de cybersécurité du transport aérien. Aussi, l'OACI se veut d'être compétente en la matière : « *Dans un effort pour promouvoir la collaboration et l'échange d'information entre ces parties prenantes, la Conférence appuie l'élaboration d'une stratégie mondiale OACI de cybersécurité. De plus, les représentants des États ont considéré l'infrastructure de l'OACI en matière de cybersécurité, dont s'occupe à l'heure actuelle le Groupe d'étude du Secrétariat sur la cybersécurité* »

En 2019, lors de la 40 ème assemblé du 4 octobre, l'OACI réaffirme sa volonté de règlementé la cybersécurité.

Entre temps, la Convention sur la répression des actes illicites dirigés contre l'aviation civile a été adoptée (convention de Beijing) ainsi que le Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs (Protocole de Beijing). La Convention Beijing associée au protocole du même nom renforce le cadre juridique en ce qui concerne les cyberattaques contre l'aviation civile internationale.[76] L'Assemblée invite donc tous les Etats à ratifier le traité.[77]

Lors de cette 40ème Assemblée, l'OACI réaffirme sa position en matière de cybersécurité et publie en octobre 2019 « OACI : Objectif stratégique de sûreté et facilitation : stratégie de cybersécurité de l'aviation, octobre 2019 ». Ce document de 8 pages joint en Annexe de ce mémoire est très important.

Après des années de travaux avec toutes les parties prenantes, l'OACI exprime sa vision ainsi que sa stratégie en matière cybersécurité et invite tous les États à se les approprier. Tel qu'expliqué dans ce mémoire, l'OACI considère aussi que le secteur aérien va continuer à croître en innovant et en devenant de plus en plus connecté.

Elle reconnait au travers de ce document le polymorphisme de la cybersécurité défini dans cette étude : « *Reconnaissant **la nature multiforme** et m**ultidisciplinaire de la cybersécurit**é, et notant que les cyberattaques peuvent*

[76] *« Considérant que la Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale (Convention de Beijing) et le Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs (Protocole de Beijing) renforceraient le cadre juridique mondial visant à considérer les cyberattaques contre l'aviation civile internationale comme des crimes, et qu'en conséquence la ratification à grande échelle de ces instruments par les États découragerait et punirait de telles attaques où qu'elles se produisent » Extrait de la Résolution A40-10 : Cybersécurité dans l'aviation civile*

[77] « *Prie instamment les États membres et l'OACI de promouvoir l'adoption et la mise en œuvre universelles de la Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale (Convention de Beijing) et du Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs (Protocole de Beijing) comme moyen de viser les cyberattaques dirigées contre l'aviation civile » Extrait de la Résolution A40-10 : Cybersécurité dans l'aviation civile*

simultanément toucher une vaste gamme de domaines et s'étendre rapidement, il faut impérativement élaborer une vision commune et définir une stratégie mondiale de cybersécurité. »

Un autre fait intéressant à relever dans cette vision est la notion, là encore, de résilience. L'OACI définit la résilience comme nous l'avons fait dans ce mémoire. En effet, elle ne considère pas la cyber résilience comme limitée aux « systèmes d'information ».

Bien au contraire, elle considère que la cyber résilience inclut tous les domaines. On retrouve cette considération dans les 7 piliers de la stratégie de l'OACI en matière de cybersécurité :

« *La stratégie s'aligne sur d'autres initiatives de l'OACI liées à la cybernétique et coordonnées avec les dispositions correspondantes en matière de gestion de la sécurité et de la sûreté. Les objectifs de la stratégie seront atteints grâce à une série de principes, de mesures et d'actions dont le cadre repose sur sept piliers, à savoir : Coopération internationale ; Gouvernance ; Législation et règlements efficaces ; Politique de cybersécurité ; Partage de l'information ; Gestion des incidents et planification d'urgence ; Renforcement des capacités, formation et culture de cybersécurité ».*

En conclusion, nous avons dû présenter longuement la vision de l'OACI en matière de cybersécurité. Malgré tout, nous sommes loin d'avoir pu réellement établir un historique exhaustif de la démarche. De nombreux éléments de la construction de cette stratégie n'ont pas été abordés dans ce mémoire. Ainsi, nous nous sommes concentrés sur les points les plus récents et les plus importants en ce qui concerne l'OACI et la cybersécurité.

Un mémoire complet pourrait être fait à l'avenir concernant la construction de la politique de la cybersécurité au sein de l'OACI.

L'OACI a donc incité les Etats à mettre en place des mesures. L'Union Européenne

a pris les devants et a commencé à légiférer en matière de cybersécurité aérienne.

SECTION 2 : L'AESA, pilier de la cybersécurité du transport aérien en Europe

« L'OACI *est l'instance mondiale compétente pour exhorter les États à s'occuper de la cybersécurité de l'aviation civile internationale. À cette fin, l'OACI organisera, facilitera et promouvra des événements internationaux servant de plate-forme à l'échange des connaissances entre les États, les organisations internationales et l'industrie. Les États sont encouragés à participer à des débats sur la cybersécurité de l'aviation civile***. » OACI, 2019**

Ainsi, l'Union Européenne n'avait pas attendu 2019 pour commencer à mettre en place une véritable politique en matière de cybersécurité du transport aérien à travers l'AESA.

Nous avons présenté succinctement l'AESA dans le titre I. L'AESA est une agence européenne créée en 2002 et opérationnelle fin 2003. Elle a pour mission de promouvoir le plus haut niveau de sécurité et de protection environnementale de l'aviation civile. « *Dès le départ, l'AESA a été conçue comme un organisme supranational. Elle détenait une compétence exclusive en matière de réglementation de la navigabilité des aéronefs et de leur certification. Elle a pu investir progressivement tous les domaines de la réglementation de la sécurité. L'idée, c'était d'en faire le "gardien de la sécurité aérienne en Europe" »,* explique Jean-Michel Bour, sous-directeur de l'Europe et de l'International à la Direction du Transport aérien.

Ses missions ainsi que son rôle ont été définis par le règlement CE n°216/2008. Au départ l'AESA avait un mandat initialement prévu en matière de certification

et de navigabilité des aéronefs.

Depuis, le mandat de l'AESA a été élargi par la modification du règlement CE n° 216/2008, en 2018. Aujourd'hui, la cybersécurité est l'une des compétences de l'AESA. Cette modification du règlement vient confirmer les thèses de ce mémoire. En effet, l'article 88 qui va donner lieu au futur règlement d'application « PART.AISS » dispose :

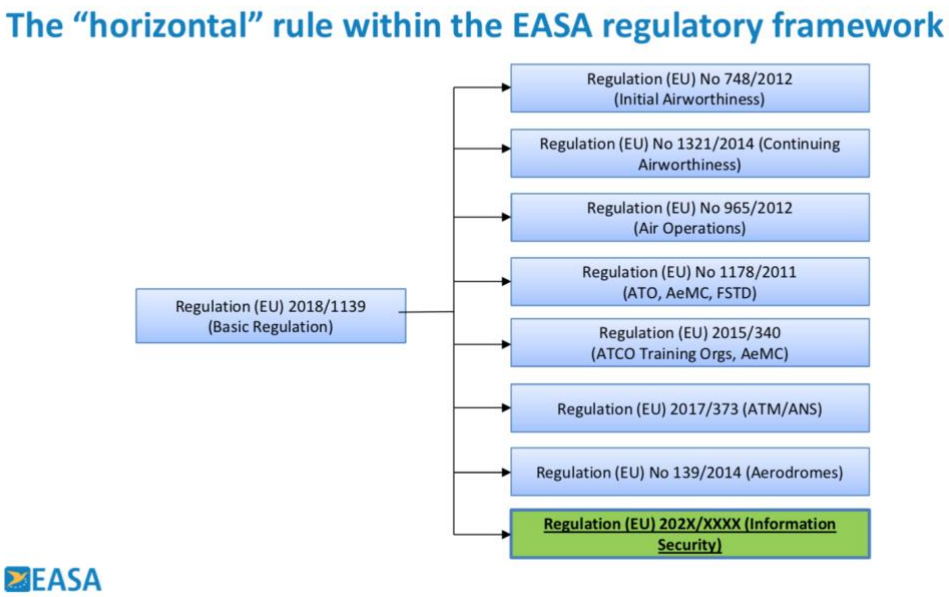
« *Article 88*

Interdépendances entre la sécurité et la sûreté de l'aviation civile

1. La Commission, l'Agence et les États membres coopèrent sur les questions de sûreté liées à l'aviation civile, ***y compris la cybersécurité, lorsqu'il existe des interdépendances entre la sécurité et la sûreté de l'aviation civile***. »

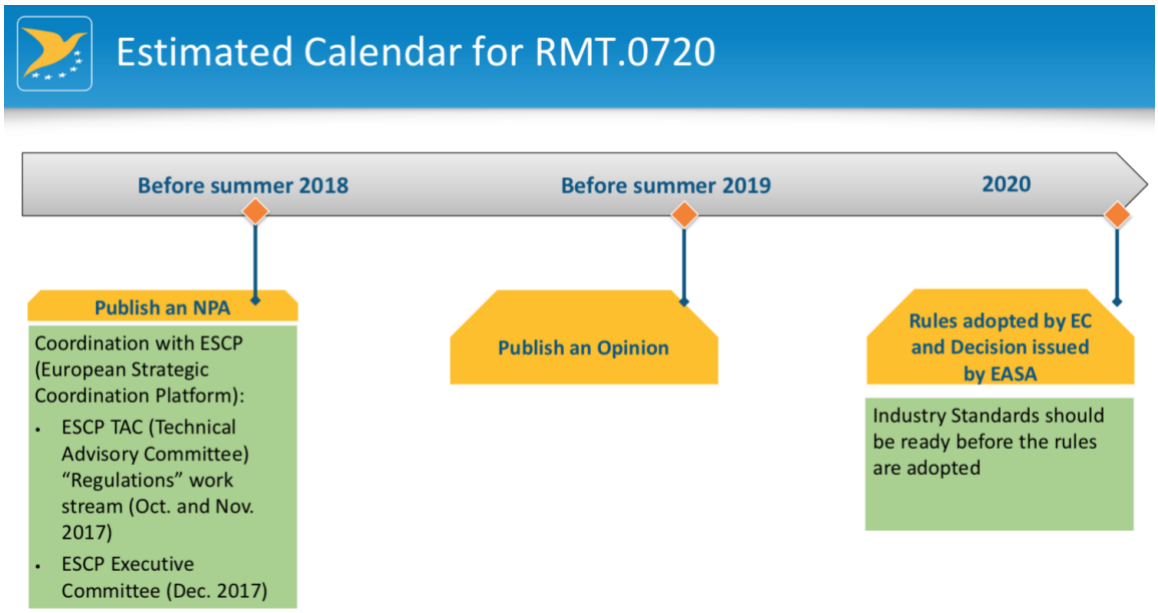
Ici, l'interdépendance entre la sécurité et la sûreté est clairement évoquée. C'est la raison pour laquelle le futur règlement d'application devra prendre en compte cette particularité.

Du fait de cette compétence l'AESA a donc commencé à légiférer en matière de cybersécurité. Mais la crise du corona virus est venue ralentir le processus. En somme, un règlement est en présentation. Ce nouveau règlement nommé provisoirement « PART.AISS » est un règlement d'application spécifique à la gestion de la cybersécurité des systèmes d'information. Nous ne pouvons pas étudier les articles de ce règlement car il est encore en préparation. En revanche, grâce au travail de Juan Anton de l'AESA, nous avons connaissance des principales obligations qui vont être issues de ce règlement spécifique à la cyber sécurité. Ce règlement va obliger les opérateurs du transport aérien à avoir un système de management du risque cyber, (ISMS). Nous développerons dans la partie 2 en quoi va consister cette future obligation.



Ce schéma démontre bien que l’AESA prévoit un règlement spécifique en matière de sécurité des systèmes d’information. D’après leurs travaux, le règlement devait être adopté d’ici 2020, après les opinions données par les professionnels. En effet, les grandes idées de ce règlement d’application ont été prépubliées sur le site de l’AESA sous forme de « Notice of proposed Amendment », autrement appelée NPA.

Grâce à cette dernière, nous allons vous présenter dans la deuxième partie en quoi consistera ce système obligatoire de management de la cybersécurité. On pressent ici l’inspiration du Système de management de la sécurité (SMS) dans le transport aérien.



Notons la participation d'Eurocontrol, l'organisation européenne de la navigation aérienne, à une réelle démarche proactive en matière de cybersécurité. Son spécialiste Patrick Mana est en charge de la politique de cyber-résilience au sein d'Eurocontrol. Ces travaux prennent la même direction que l'OACI.

Eurocontrol et l'AESA travaillent en coopération en matière de cybersécurité, ayant conscience de l'importance du collectif dans le cyber.

Dans cette idée de construction collective de la cybersécurité du transport aérien, l'AESA a créé l'European Centre for Cyber Security in Aviation (ECCSA). Nous avons présenté précédemment le CERT-UE[78], cette équipe faite pour répondre aux cybermenaces visant l'Union européenne. L'ECCSA représente la version spécifique au transport aérien du CERT-UE.

Tous les pays sont donc invités à participer à la construction de la cybersécurité, même si certains, comme la France, semblent vouloir être le premier pays de la cordée.

[78] CERT UE « *est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous* »

SECTION 3. La France, une volonté d'être pionnier en matière de règlementation de la cybersécurité du transport aérien

Elisabeth Borne, ancienne ministre chargée des Transports, a instauré le Conseil pour la Cybersécurité du Transport Aérien (CCTA) le 12 avril 2018 durant les assises du transport aérien [79]. Le CCTA a pour objectif d'« *appréhender globalement le cyber-risque français avec une coordination indispensable entre professionnels : les services de l'Etat, les constructeurs, les équipementiers, les exploitants et les fédérations professionnel*les » du transport aérien.

En effet, cette instance se veut être pour les acteurs du transport aérien « *un lieu de référence pour encadrer, structurer et coordonner les initiatives concernant la cyber sécurité du secteur aérien français* ». Ici, l'on peut voir que pour l'Etat français la cybersécurité du transport aérien français est vitale. L'Etat se veut être un catalyseur en partant que l'idée que le transport aérien ne peut s'organiser seul.

Les travaux européens en matière de règlementation de la cybersécurité du transport aérien avaient commencé en amont de l'instauration du CCTA. Même si Elisabeth Borgne précise que « *Ce conseil portera la voix de la France dans les groupes de travail techniques européens et internationaux*. ».

Cela a pu paraître étrange du point de vue des professionnels du secteur aérien qui s'étaient déjà organisés, et celui depuis plusieurs années, pour participer au travail de l'OACI, mais aussi de l'AESA. En réalité, la France avait déjà amorcé le lobbying en matière de cybersécurité à l'AESA, et à l'OACI. [80]

Aussi, la présidence du Conseil pour la Cyber sécurité du Transport Aérien est

[79] Les assises du transport aérien ont été mises en place durant 1 ans. Elles avaient pour but de réunir toutes les parties prenantes du transport aérien français afin de déterminer une stratégie. Pour certains professionnels tels que la FNAM, les assises du transport aérien n'auraient pas « servi à grand-chose ».
[80] Colloque de l'AAE, Vers des navires autonomes

confiée au direct général de l'aviation civile. Il est accompagné de trois vice-présidents :

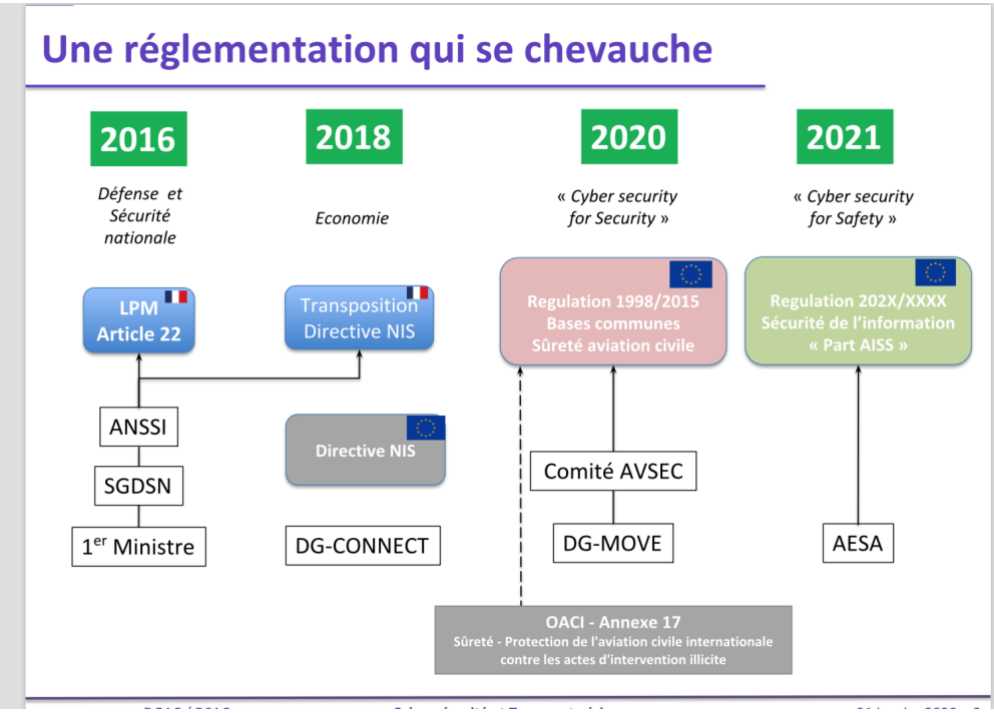
- Le directeur général de l'ANSSI, représentant l'Etat
- La direction d'Airbus, représentant l'industrie
- La direction du groupe ADP, représentant les opérateurs

Ce qui est intéressant de noter dans la construction de la gouvernance du CTTA est qu'en incluant tout un système (représentant de l'état, de l'industrie, des opérateurs) les concepts de résilience sont repris. Le CTTA, comme l'AESA et l'OACI ont compris l'importance de considérer la cybersécurité de manière systémique pour atteindre la cyberrésilience.

De plus, le CTTA a compris l'importance de la règlementation puisqu'il est également composé de trois comités techniques :

- *« CT1 : « risques cyber », chargé de tenir à jour une hiérarchie des risques pouvant affecter la filière du transport aérien ;*
- *CT2 : « impact », chargé de proposer des mesures d'atténuation de ces risques, en tenant compte de l'impact de ces mesures (sûreté, économie…) ;*
- ***CT3 : « réglementation », chargé de formuler des projets de textes nationaux et déployer une stratégie d'influence auprès des instances internationales.*** »

Le comité technique 3 a donc pour thème la réglementation. Il est important de comprendre qu'en matière de cybersécurité, comme on l'a vu dans le chapitre « le droit de la cybersécurité », la France a dû transposer des textes européens (Directive NIS, CybersécurityAct). Comme nous le montre ce schéma de la DGAC d'Anne Frish responsable de la cybersécurité, la « règlementation se chevauche »



L'on retrouve ainsi tous les textes que l'on a évoqués précédemment tels que la Loi de programmation militaire et son article 22, le règlement Régulation n°1998/2015, et enfin le futur règlement PART.AISS (regulation 202X/XXX).

Apparait ici toute la problématique à laquelle fait face la réglementation de la cybersécurité du transport aérien. Les opérateurs ainsi que les industriels vont être soumis à une multitude de textes, de règlementations et de certifications à respecter. Certains textes et règlements sont particuliers au transport aérien, comme le futur règlement PART.AISS, ou encore la règlementation sur les drones. A contrario, certains ont une vocation générale comme le RGPD ou bien la directive NIS.

Dans les années à venir, la France à la volonté de renforcer sa règlementation en matière de cybersécurité du transport aérien comme le prouve le CTTA. Il ne faut pas que cela entraine un mille-feuille administratif pour les acteurs du transport aérien. Il est indispensable de réunir toutes les lois, textes, règlements, certifications concernant la cybersécurité du transport dans un référentiel unique. C'est là un des objectifs de la DGAC comme le démontre la présentation d'ANNE

FRISH.

Ainsi, l'on voit apparaitre en France un vrai corpus de textes concernant la cybersécurité du transport aérien. Il est issu de la volonté de l'OACI, de l'AESA et du pays lui-même. Ce corpus tend à se développer au fil des années du fait de la transformation du transport aérien.

Pouvons-nous alors parler de « droit de la cybersécurité du transport aérien » ?

Il faudrait être nuancé dans nos propos mais il existe un réel corpus de textes complexes (RGPD, PART.AISS, certification mondiale à venir d'appareils embarqués) auquel devront être soumis les acteurs du transport aérien. Ainsi, dans les entreprises du transport, le juriste va devoir être proactif car il sera le garant de la conformité au vu de ces textes aussi nombreux que complexes. Il devra certainement coopérer davantage avec les responsables de la sûreté et de la sécurité puisqu'il sera responsable au niveau juridique de la protection des données. Le juriste se trouvera donc réellement impliqué dans la gestion du risque.

TITRE 2 : VERS LA CYBER-RÉSILIENCE DU TRANSPORT AERIEN

Dans la première partie, nous nous sommes attelés à présenter les tenants et les aboutissements de la cybersécurité et nous avons par la suite présenté les enjeux en matière de cybersécurité du transport aérien.

Les concepts de résilience puis de cyber résilience ont été définis et nous avons démontré que la cyberrésilience dans notre étude ne correspondait pas à la résilience des systèmes d'information isolés.

Notre démonstration s'est appuyée sur le fait que pour le transport aérien la cyberrésilience correspondait à un écosystème dont la cybersécurité faisait partie mais n'était pas la seule composante. Comme nous avons pu le voir, le domaine juridique fait partie de cette cyberrésilience. Le cadre managérial, ainsi que le cadre assurantiel favorisent celle-ci. L'on a aussi évoqué la culture de la sécurité dans l'aérien, qui était l'une des composantes de la sécurité du transport aérien.

Dans la partie suivante, nous allons donc essayer de démontrer le management des risques, et plus particulièrement les risque cyber et juridique, dans l'objectif de la cyberrésilience du transport aérien (Chapitre 1). Puis nous verrons que le cadre assurantiel et culturel en matière de cybersécurité du transport aérien est essentiel pour atteindre la cyberrésilience (Chapitre 2)

CHAPITRE 1. LE MANAGEMENT DES RISQUES CYBER ET JURIDIQUES, FONDEMENT DE LA CYBER-RÉSILIENCE

La culture de sécurité est présente dans le transport aérien grâce à des acteurs proactifs en la matière. Le système de gestion de la sécurité est le ciment de cette culture de la sécurité (Section 1). La multiplication des règlements contraignants en matière de protection des données personnelles fait apparaitre un nouveau risque que le transport aérien se doit de gérer, le risque juridique (Section 2).

SECTION 1. Management des risques et systèmes de gestion de la sécurité

Il s'agit ici de présenter le management du risque et son application au travers du Système de gestion de la sécurité (SGS) (A) avant d'apprécier en quoi le risque cyber pourrait être intégré à ces systèmes de gestion du risque préexistants comme le recommande le futur règlement PART.AISS (B).

A. Le système de gestion de la sécurité du transport aérien, outil du management du risque

Pour comprendre le management des risques, il nous faut définir les termes. Le terme management a été défini dans la partie introductive. Il nous faut désormais définir une notion que l'on a abordée tout au long de ce mémoire : le risque. Pour ce faire, nous nous servirons de l'excellent article d'Yvon Pesqueux, « Pour une épistémologie du risque » dans Management & Avenir 2011 n°42. Selon l'auteur, « *un risque peut être vu comme « un danger, inconvénient plus ou moins probable selon lequel (un individu, un acteur) est exposé » ou ; comme « une situation dont l'**occurrence** est incertaine et dont la réalisation affecte les objectifs de*

l'entreprise qui le subit » Ou encore, « un risque est un aléa dont la survenance prive un système (une entreprise par exemple) d'une ressource et l'empêche d'atteindre ses objectifs »[81] . Notons bien cette notion d'occurrence chère au transport aérien qui sera abordée plus tard dans l'étude. In fine, le management du risque correspond aux techniques organisationnelles mises en place dans un objectif de gérer le risque.

L'OACI, dans son rapport ICAO SMM (2006, P.1-1) Safety in Aviation, a défini la sécurité comme « l'état dans lequel le risque de nuisance des personnes ou des biens est réduit et maintenu à un niveau acceptable par **un processus continu d'identification des dangers et de gestion des risques** ».

Le risque est protéiforme par nature. Pour le transport aérien, le risque concerne aussi bien la sécurité des vols que l'atteinte aux infrastructures. Il existe également le risque juridique.

Le management du risque dans l'aérien est très présent, au travers du Système de management de la Sécurité. L'excellent mémoire de GAVRILL Lydia – Accident de Germanwings Symptomatologie d'un métier en évolution et intégration des risques, vient nous éclairer en matière de risque dans l'aérien. Nous renvoyons nos lecteurs au Chapitre 1, section 1 de son travail.

En effet, l'autrice revient sur l'historique de la gestion de la sécurité dans l'aérien. Elle définit précisément le Système de Gestion de la Sécurité :

« *Dans l'aviation, le « safety management » (gestion de la sécurité) est défini par l'autorité de l'aviation civile anglaise comme « la gestion systématique des risques liés aux opérations de vol, aux opérations au sol et aux activités d'ingénierie ou d'entretien des aéronefs pour atteindre des niveaux élevés de performance de sécurité » alors que le « safety management system » (système de gestion de la*

[81] Pesqueux, Yvon. « Pour une épistémologie du risque », *Management & Avenir*, vol. 43, no. 3, 2011, pp. 460-475.

sécurité)est un élément explicite de la politique de sécurité d'une entreprise et définit comment elle entend gérer la sécurité en tant que partie intégrante de son activité globale».[82]

Nous reviendrons à plusieurs reprises sur l'étude de Lydia GAVRILL qui est très complète. Lydia GAVRILL, au travers de sa démonstration, prouve que le transport aérien a su développer une véritable culture de la sécurité. Elle prouve que le système de gestion de la sécurité a participé à cette construction de la culture de la sécurité.

Précisons que le Système de gestion de la sécurité est une obligation règlementaire codifiée par **l'arrêté du 22 décembre 2008 relatif à la mise en œuvre des systèmes de gestion de la sécurité pour les entreprises de transport aérien public et les organismes de maintenance.**

Comme nous l'avons vu précédemment, le futur règlement AESA, PART.AISS va devoir être transposé en droit français.
Ce règlement prévoit que le risque cyber soit intégré dans les systèmes de gestion de la sécurité existants.

L'une des recommandations du dossier n¨45 Cybermenaces visant le transport aérien de l'Académie de l'Air et de l'Espace (AAE) vient appuyer cette idée.

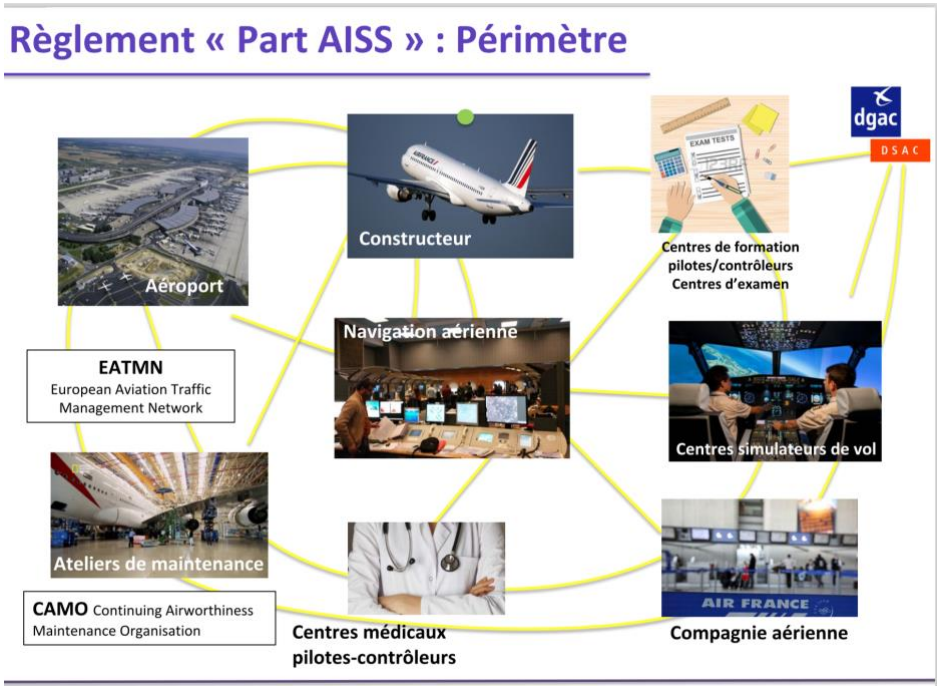
« Recommandation essentielle R11
*Tous les acteurs certifiés du transport aérien doivent avoir **l'obligation de déclaration, de partage, puis de traitement systématique des cyber-incidents**, **de la même façon** que les accidents et incidents aériens sont déclarés, partagés et analysés, ce qui a permis d'accroître **notablement la sécurité du transport aérien.***
Action : OACI, FAA, EASA et autorités nationales »

[82] Accident de Germanwings : « Symptomatologie d'un métier en évolution et intégration des risques », Lydia GAVRILL - IFURTA, Aix-Marseille Université - 2017

B. L'intégration du risque cyber dans les systèmes de management préexistants

« *Une intégration du système de management de la sécurité des systèmes d'information au système de Gestion de la Sécurité et aux process existants des organisations est une possibilité intéressante voire vivement souhaitable dès lors que les organisations ont la maturité pour le faire. En cas de systèmes de management non intégrés, les organisations devront impérativement montrer l'articulation entre les 2. Entre autres, il peut y avoir des arbitrages à faire entre des exigences safety et des exigences cyber security et l'opérateur doit avoir à anticiper le traitement de tels cas. La cyber sécurité ne peut être traitée indépendamment de la safety et de la sûreté. Elle nécessite pour autant une expertise spécifique cybersécurité* ». Anne Frisch, Directeur du programme Cybersécurité, de la DSAC**.**

Cette citation, issue d'une présentation de la DGAC, résume parfaitement la volonté du règlement PART.AISS. En effet, ce dernier va imposer aux acteurs du transport aérien le management du risque cyber dans ces domaines :



(Source DGAC/DSAC 2019)

Nous pouvons de nouveau percevoir les liens entre règlementation et management. Dans le transport aérien, ce lien est considéré comme garant de la sécurité.

Nous avons pu constater que le risque cyber était un risque polymorphe puisqu'on ne pouvait classer ce risque en sécurité ou en sûreté. En revanche, ces deux termes sont pourtant bien distingués dans le domaine du transport aérien.

S'agissant de la sécurité, dans le domaine aérien, la personne en charge de la gestion du management est le Responsable du système de gestion de la sécurité (Le SGS). Son rôle consiste à faciliter l'identification des dangers, l'analyse des risques et leur gestion. Il s'assure de la mise en œuvre du bon fonctionnement et de l'évolution du système de gestion de la sécurité sur l'ensemble du périmètre (documentation, animation, efficacité, animation, évènements, changement, promotion de la sécurité, enquêtes, retour d'expérience, formation, compétences, coordination).

Pour les auteurs du dossier de l'AAE : « ***Un système de management de la cybersécurité devrait exister*** *chez tous les acteurs du transport aérien, incluant la vérification que les règles d'hygiène informatique sont bien appliquées, ainsi que des mesures de prévention et de traitement des incidents*. »

Quant à l'OACI, celle-ci vient préciser dans le point 4.1 de la Stratégie de cybersécurité de l'aviation : « 4.*1* ***La cybersécurité doit être incluse dans les systèmes de sûreté et de supervision de la sécurité*** *de l'aviation des États dans le cadre d'une gestion exhaustive du risque*. »

On arrive à la conclusion que les acteurs du transport aérien ont déjà un mis en place depuis des années des systèmes de management en matière de sécurité et de sûreté. Ces systèmes fonctionnent que ce soit dans les compagnies ou dans les aéroports de manière distincte. Souvent, dans les organigrammes, nous avons une

direction de la sûreté, une direction de la sécurité et une direction des systèmes d'information.

Ainsi, le risque cyber comme nous l'avons défini devrait être intégré dans un système de management transversal à la sûreté, la sécurité et l'informatique. L'on pourrait aussi, au vu de l'actualité, s'interroger sur le risque sanitaire et son intégration dans le système de management du risque dans le transport aérien.

Cette citation de l'intervention « Le conseil cyber pour le transport aérien CCTA, une instance partenariale pour adapter le transport aérien aux menaces cyber » de Guillaume Counio, chargé de Mission Cybersécurité à la Direction du Transport Aérien de la DGAC nous résume les travaux entrepris par le CT3 du CTTA :

« D'abord on a mis au point une **méthodologie partagée pour l'évaluation des risques cyber pour toute la filière ; c'est assez important parce que ça permet d'avoir ensemble la vision de ce qu'il est urgent de faire** (…).

Ensuite, on a mis au point une cartographie des flux d'information qui traverse le système du transport aérien : c'est quelque chose qui n'existait pas. On a étudié différents cas incluant des usagers d'exploitation en vol et au sol, la maintenance, le cargo etc.. On a réussi à en déduire des positions coordonnées et partagées avec nos collègues industriels ».

Le risque cyber va donc être pris par le management du transport aérien. A contrario, la multiplicité des textes juridiques en matière de protection des données personnelles crée un nouveau risque à prendre compte : le risque juridique.

SECTION 2. Le management du risque juridique dans le transport aérien

Le *legal risk management* ou en français le management du risque juridique est un nouveau domaine qui préoccupe de plus en plus les entreprises de manière

générale. Le transport aérien y est particulièrement assujetti. En effet, comme nous l'avons précédemment évoqué, de nombreux textes juridiques viennent imposer des contraintes aux acteurs du transport aérien.

Il y a textes qui gèrent la protection des données et qui concernent toutes les entreprises. Dans le futur, le nouveau règlement PART.AISS, sera spécifique à l'aérien. Enfin, existent également les certifications des objets connectés, que ce soit les règles générales de certification européennes ou celles spécifiques au transport aérien.

Le juriste va donc devoir faire face à de nombreux nouveaux risques que la transformation digitale du transport aérien a engendrées.

Alain Bensoussan, avocat à la cour d'appel de Paris et spécialiste en droit des technologies avancées nous donne la définition précise du risque juridique :

« *Le risque juridique peut être défini comme l'expression et/ou la manifestation du* ***non-respect des dispositions légales ou réglementaires*** *auxquelles l'organisation est soumise pour toutes* ***ces activités****. Le référentiel juridique concerné est naturellement l'ensemble des dispositions légales internationales, européennes si elles ont un effet direct, françaises mais également la jurisprudence qui précise la portée des dispositions précitées, ainsi que les normes professionnelles, sectorielles, déontologiques****. Le risque juridique est étroitement lié aux risques opérationnels de l'organisation***. »

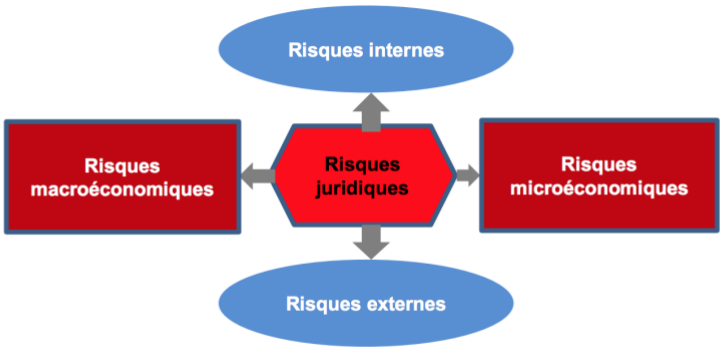
Il est intéressant de noter dans la définition l'aspect opérationnel de l'organisation. Le transport aérien est une activité très opérationnelle, disposant comme on l'a vu d'un véritable système de gestion des risques opérationnels. De manière étrange, cela n'inclut pas encore les risques juridiques dans le transport aérien, malgré la culture prégnante de conformité en matière de sécurité.

La gestion des risques juridiques ainsi que la cartographie semblaient encore « *incongrues et relever d'une prospective fort éloignée des préoccupations et de la réalité des entreprises* »[83]. Mais depuis ces dernières années et la multiplicité des textes en matière de cybersécurité, « *la reconnaissance croissante du concept de risque juridique ainsi que sa prise en compte, en tout cas dans les grandes entreprises, militent pour qu'il soit intégré dans une cartographie générale ou fasse l'objet d'une cartographie spécifique.* »

Le RGPD et la Direction NIS ont des effets considérablement marqués pour l'activité du transport aérien puisque tout l'écosystème est concerné par ces textes. La mise en conformité avec ces textes est un processus dynamique et continu. Les entreprises du transport aérien se doivent d'être constamment en conformité. « *La notion de « conformité » est apparue à l'origine dans les pays de droit anglo-saxon sous le terme de « compliance ». En effet, l'un des premiers instruments juridiques imposant une vérification du risque de conformité résulte de la loi sur la réforme de la comptabilité des sociétés cotées, prise par les Etats-Unis en 2002 (encore appelée loi Sarbanes-Oxley, du nom des deux sénateurs américains à son origine, Paul Sarbanes et Mike Oxley) suite notamment aux affaires Enron, Arthur Andersen… »*

Schéma de l'interdépendance du risque juridique :

83 Collard, Christophe, et Christophe Roquilly. « Les risques juridiques et leur cartographie : proposition de méthodologie », *La Revue des Sciences de Gestion*, vol. 263-264, no. 5, 2013, pp. 45-55.



Ainsi, il est évident que le transport aérien va faire face à des crises multifactorielles. Le transport se doit de répondre à la menace concernant l'intégrité de ces données, tout en respectant de nouvelles règlementations contraignantes. L'on peut citer la crise sanitaire puisqu'il est de plus en plus demandé aux aéroports ainsi qu'aux compagnies de faire des tests de dépistage des passagers.[84] La responsabilité des aéroports et des compagnies peut être mise en cause concernant le recueil et le traitement des données sanitaires sensibles.

Une fois de plus, l'aspect polymorphe de la cybersécurité apparait, celle-ci étant également liée au domaine sanitaire. Qui aimerait voir ses données de santé recueillies par un aéroport voire publiées après un piratage ? Qui aimerait savoir que ses données très sensibles peuvent fuiter ?

Cet été, la Grèce a mis en place un QR code obligatoire pour tous les passagers arrivant sur son territoire. Certaines personnes ont même été empêchées d'embarquer à cause d'un formulaire mal rempli[85]. Ce formulaire (ANNEXE) demande aux passagers de fournir des données personnelles. Or, il n'est fait aucune mention concernant le traitement de ces données personnelles par l'Etat grec ou bien par les compagnies. De plus, à bord de l'aéronef, les compagnies

[84] https://www.francebleu.fr/infos/sante-sciences/premiers-test-covid-19-obligatoires-a-l-aeroport-nice-cote-d-azur-1596286414

[85] https://www.capital.fr/economie-politique/une-famille-empechee-dembarquer-pour-la-grece-a-cause-dun-nouveau-formulaire-mal-rempli-1377517

remettent de nouveau aux passagers un document papier à remplir. Ce long formulaire est encore plus précis que le formulaire de l'Etat grec. D'après une des hôtesses « ce formulaire est obligatoire, il s'agit d'une demande européenne »[86]. Ce sont les compagnies aériennes qui sont chargées de récolter les données personnelles de leurs passagers. Comment seront traitées ces données par la suite ? Quelle est la valeur juridique de ces formulaires dont personnes ne vérifie l'exactitude des informations communiquées ?

Les acteurs du transport aérien font face à de nouveaux défis bien différents de ceux qu'ils ont connus auparavant. Ils ont su relever les défis comme le risque terroriste, ou encore la crise économique. Les assureurs ont participé à maintenir cette confiance dans le transport aérien après la crise du 11 septembre[87].

CHAPITRE 2. L'assurance du risque cyber et culture de la sécurité, ciments de la cyber-résilience du transport aérien

A travers ce dernier chapitre, nous verrons que le risque cyber dans le transport aérien a besoin d'être assuré, même si cela semble être un vrai défi pour les assureurs du transport aérien. (Section 1). Nous avons évoqué dans ce mémoire la culture de la sécurité très présente dans le transport aérien. Le problème est que la cybersécurité est un domaine très particulier qui demande une propre culture de la cybersécurité. Nous démontrerons que le transport aérien se doit de fusionner la culture de la sécurité des vols avec la culture de la cybersécurité pour atteindre l'état tant recherché de cyberrésilience (section 2).

[86] D'après l'expérience personnelle de l'auteur ayant effectué un vol Marseille-Heraklion le 1 er aout 2020
[87] https://www.argusdelassurance.com/social/directeur-general-de-la-reunion-aerienne-la-couverture-des-risques-de-guerre-est-du-ressort-des-etats-traumatise-par-les-attentats-du-11-septembre-le-marche-aviation-a-neanmoins-surve.11958

SECTION 1. L'assurance du risque cyber dans le transport aérien

Après avoir démontré que le secteur de l'assurance développe des polices pour assurer le risque cyber en général (A) nous verrons qu'en ce qui concerne le domaine aérien, assurer le risque cyber semble difficile mais pas impossible (B).

A. Le développement d'assurances de police spécialisées en risque cyber

Tout d'abord il est important de définir le terme assurance. La définition de l'assurance la plus communément utilisée est celle de J.hémard : « *l'assurance est une opération par laquelle une partie, l'assuré, se fait promettre, moyennant une rémunération (la prime), pour lui ou pour un tiers, en cas de réalisation d'un risque, une prestation par une autre partie, l'assureur, qui prenant en charge un ensemble de risques, les compense conformément aux lois de la statistique.* »

Ainsi, l'assurance vise à couvrir un risque. L'assurance a permis aux sociétés de couvrir des risques très variés tels que le risque incendie, le risque lié au transport, le risque lié aux intempéries.

Depuis sa création, l'assurance est intimement liée au transport. En effet, d'après les historiens, les premières polices d'assurances seraient celles du transport maritime. Le risque « fortune de mer » était l'un des premiers risques assurés par les marchands depuis les Romains[88].

Il apparait donc que l'assurance a toujours été liée aux activités humaines et à leurs transformations.

Nous avons évoqué la transformation digitale dans la première partie de ce mémoire. Ainsi, nous avons expliqué que la plupart des secteurs de l'économie

[88] Keucheyan, Razmig. « 2. Financiariser la nature : l'assurance des risques climatiques », *La nature est un champ de bataille. Essai d'écologie politique*, sous la direction de Keucheyan Razmig. La Découverte, 2018, pp. 85-154.

entraient dans une phase de transformation digitale. Nous avons ensuite démontré que cette transformation digitale induisait un nouveau risque pour les entreprises à savoir le risque cyber.

Le secteur de l'assurance subit lui aussi cette transformation des activités. Le risque associé aux nouvelles technologies évoluant très vite, le secteur de l'assurance a dû mettre en place des polices pour couvrir ce risque.

Un mémoire de qualité a été réalisé en 2017 par R.Deslande de l'Institut des assurances de Lyon, « Présentation des programmes de cyberassurances et de leurs limites ». L'auteur explique que les polices spécifiques de cyberassurances sont apparues notamment parce que les contrats d'assurance classique n'apportaient qu'une réponse partielle au cyber risque, *« ne couvrant que la responsabilité civile ou les dommages ou n'en couvrant pas les conséquences immatérielles ou de manière sous-limitée. Ces contrats n'apportent pas de prestations de gestion de crise adaptées au risque cyber, ni d'intermédiaire spécialisé*. »

L'auteur affirme la particularité du risque cyber à forcer les assureurs à repenser leurs polices d'assurance. Le risque cyber n'est pas figé dans le temps, il est mouvant. Il faut également travailler en coopération avec les assurés, responsables de la mise à jour de leurs systèmes, ainsi que de l'intégrité de leur data.

B. La difficile mais nécessaire mise en place d'une assurance du risque cyber dans le transport aérien

« *Si les programmes de cyberassurances présentent des garanties adaptées au risque cyber, ils gagneraient à se spécialiser par secteur d'activité car ces derniers ne présentent pas la même exposition au risque cyber. Ils ne sont en effet pas susceptibles de subir les mêmes typologies d'attaque ni les mêmes types de dommage*s ».

Sans pour autant développer son idée, l'auteur conclut que les polices cyber gagneraient en efficacité en étant étudiées de façon sectorielle.

Les professionnels du secteur de l'assurance commencent à mettre en place des polices spécifiques au transport aérien. Ainsi, Willis Towers Watson propose un nouveau produit cyber adapté au secteur de l'aviation, « CyFly ». Il a été développé avec AIG. La police contient une extension des pertes **d'exploitation à des tiers**. La police prend en compte le fait que les entreprises du transport aérien dépendent de services de nombreux tiers pour assurer une continuité d'activité. Les frais de maintenance des avions ou les frais de sécurité de l'aéroport sont aussi couverts.[89]

Les différentes interventions de Sophie Maysan, Directrice juridique et sinistre à la réunion aérienne, seront les sources de notre développement. Sophie Maysan, est intervenue à nombreuses reprises lors de colloques de l'AAE ou bien encore aux Rendez-vous de l'assurance transports de 2018. Ces différentes interventions constituent une mine d'or en matière de cyber assurance du secteur aérien.

Sophie Maysan démontre que le cyber risque en aéronautique concerne surtout les problèmes de bug. Selon ses propos, les assureurs du transport aérien ont dû faire face à de nombreuses reprises à des réclamations qui concernaient des retards, non pas à cause des systèmes d'information, mais bien à cause d'un dysfonctionnement des systèmes.[90]

Sophie Maysan a travaillé au sein d'un groupe de réflexion sur le sujet des clauses en matière de cybersécurité aérienne. Leurs travaux se sont concentrés sur les clauses d'exclusion du risque de la violation du risque de données personnelles, ainsi que sur les pertes d'exploitation liées à la donnée. Le groupe de réflexion composé d'assureurs, de l'autorité de l'aviation anglaise, ainsi que d'industriels en a conclu qu'il était trop tôt pour assurer tout le risque systémique qu'engendrent les problèmes de sécurité.

[89] WILLIS TOWERS WATSON, Willis Towers Watson launches innovative new cyber product for global airlines, Press Release, Avril 2017.

[90] Risques Cyber : Assurance des risques de demain ? Session Plénière animée par M. Frédéric DENEFLE, Directeur Département Relations Extérieures du CESAM et Directeur Général du GAREX

Il est aussi intéressant de noter que dans les polices d'assurance classiques le risque terroriste est souvent exclu. Les cyberattaques sont pour le moment considérées comme un risque terroriste par les assureurs du transport aérien.

En effet, comme nous l'avons vu précédemment, le risque cyber est un risque qui peut entrainer une défaillance de tout le système du transport aérien. Pour le moment, il n'est pas possible d'assurer cet effet domino qu'engendre le risque cyber. [91]

L'autre problème posé par l'assurance du risque cyber sont les nouvelles obligations règlementaires auxquelles sont assujettis les acteurs du transport aérien en matière de gestion du risque cyber.

L'assurance cyber dans le transport est perçue comme le transfert de risque de la part des assureurs. L'assurance cyber est pluridisciplinaire par nature. Par conséquent, elle doit être construite en partenariat avec le management opérationnel. Le risque cyber est à la croisée des chemins.

La question pour les assureurs est de savoir s'ils devront obliger les acteurs du transport à être en conformité avec les nouveaux textes au moment du sinistre pour profiter de la garantie ? L'autre point important est de savoir comment les assureurs pourront faire la différence entre une défaillance des systèmes d'information et une négligence humaine dans l'organisation (compagnies, aéroports, constructeurs) ?

[91] Risques Cyber : Assurance des risques de demain ? Session Plénière animée par M. Frédéric DENEFLE, Directeur Département Relations Extérieures du CESAM et Directeur Général du GAREX

SECTION 2. La nécessité d'une culture cyber dans le transport aérien

A. Définition de la culture cyber

Tel que nous avons pu le voir dans la partie précédente, l'humain est au cœur de la sécurité dans le transport aérien. En effet, le « facteur humain » est souvent responsable de nombreux incidents et/ou accidents, comme nous le précise le commandant de Bord Phillipe Agnès.[92] Le facteur humain est un élément-clé de la sécurité aérienne.

Concernant la cybersécurité, l'humain n'est, en apparence, pas concerné. Pour le commun des mortels, ce sont les gros serveurs qui se doivent d'être sécurisés. En réalité, l'humain, en matière de cybersécurité, constitue la première faille. En effet, « **le fondement de la sécurité de la donnée informatique** dans une organisation dépend de **l'éducation, de la conscience collective** ainsi que de la collaboration permanente de l'ensemble des parties prenantes afin de faire face aux menaces ».[93]

La culture de la cybersécurité n'est pas un concept facile à appréhender car elle fait appel aussi bien au collectif qu'à l'individuel.

Elle fait appel au collectif car la culture de la cybersécurité des systèmes d'information doit être insufflée à tous les niveaux de l'organisation mais aussi de la supply-chain. (Nous pouvons évoquer AirCyber, le programme de cybersécurité de la supply chain des PME de l'aéronautique. Patrick Fanget, président de BoostAerospace depuis 2016, s'est donné pour missions pour augmenter la cybersécurité de la chaîne logistique (supply chain) aéronautique)[94].

[92] Intervention IFURTA « FACTEUR HUMAIN »
[93] Barim, Sofia. « Développer la culture sécurité de l'information numérique de son organisation », *I2D – Information, données & documents*, vol. volume 54, no. 3, 2017, pp. 49-50.

[94] https://www.industrie-techno.com/article/la-filiere-aeronautique-normande-s-associe-a-aircyber-le-dispositif-de-cyber-protection-de-boostaerospace.57030

Mais elle fait également appel à l'individuel car la culture de la cybersécurité concerne tous les individus au sein de l'organisation. Mattieu Garin, Senior Manager chez Wavestone,[95] expert en cybersécurité, dans un article sur le blog Expectra[96] nommé « Le facteur, clé de la cybersécurité » vient appuyer cette idée. Il nous explique que la plupart des cyber-attaques se servent des défaillances humaines pour pénétrer les systèmes d'information des entreprises. Il évoque le perfectionnement des techniques de social engineering.

Franck Decloqument, dans son article « Espionnage, attaques subversives et cyber sécurité : de l'impact des actions de « social engineering » et des vulnérabilités humaines sur la sécurité globale des entreprises », définit la notion de social engineering :

« *Le social engineering est une forme* ***d'acquisition déloyale d'informations*** *par le recours massif à* ***l'art du conditionnement*** *et à la manipulation. Autrement dit, l'escroquerie des personnes à des fins d'obtention de données sous embargo, à très haute valeur ajoutée. Il s'agit* ***d'informations sensibles*** *qui n'auraient jamais été divulguées dans des conditions normales d'interactions sociales.* ***On influence ou abuse généralement de la confiance d'un individu que l'on conditionne****, afin de lui soutirer des renseignements utiles (mot de passe, données sensibles, codes d'accès, agenda interne, options stratégiques, etc.) pour* ***commettre un forfait****. Il s'agit en définitive de conditionner autrui à « répondre positivement » à des attentes ou des injonctions cachées induites par un interlocuteur malveillant, sur la base des* ***fameuses failles humaines*** *qui affectent notre perception* »[97]

L'auteur conclut son article par cette phrase qui résume bien notre démonstration :

« ***Nos individualités*** *sont devenues, en quelque sorte à notre corps défendant, une*

[95] « *Wavestone est un cabinet de conseil français spécialiste de la transformation des entreprises et des organisations* »

[96] Le blog de référence pour les managers, cadres et agents de maîtrise

[97] DeCloquement, Franck. « Espionnage, attaques subversives et cyber sécurité : de l'impact des actions de « social engineering » et des vulnérabilités humaines sur la sécurité globale des entreprises », *Sécurité et stratégie*, vol. 22, no. 2, 2016, pp. 21-29.

trajectoire obligatoire pour les arnaqueurs et les pirates usant des techniques numériques intrusives pour agir, sous l'influence de cette mimésis universelle. »[98]

L'humain, est donc, pour nombre d'experts, la première faille des systèmes d'information. En effet, ces derniers deviennent de plus en plus techniques et complexes. Les piratages ou même les bug sont souvent dus à l'humain qui va entrer un mauvais code ou bien avoir un mot de passe qui n'est pas assez sécurisé.

Certains employés du secteur aérien travaillent avec des données sensibles. Si des personnes mal intentionnées se mettaient à les cibler à travers des faux mails, cela mettrait à mal la sécurité et la sûreté de l'organisation.

B. De l'importance d'une convergence des cultures de sécurité et de cybersécurité

L'OACI en est arrivée à la même conclusion. Le septième point du document « Stratégie de Cybersécurité de l'Aviation », évoqué de nombreuses fois dans notre étude, précise :

« 7. Renforcement des capacités, formation et culture de cybersécurité

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

[98] DeCloquement, Franck. « Espionnage, attaques subversives et cyber sécurité : de l'impact des actions de « social engineering » et des vulnérabilités humaines sur la sécurité globale des entreprises », *Sécurité et stratégie*, vol. 22, no. 2, 2016, pp. 21-29.

l'information et cybernétique soient fusionnés et mis en rapport avec ceux de professionnels pertinents en aviation. »

Ainsi, l'OACI incite les Etats à prendre en compte l'importance du facteur humain dans leurs politiques de cybersécurité du transport aérien.

Les travaux universitaires, à l'instar du mémoire de Lydia GAVRILL, nous ont démontré que la culture de la sécurité était ancrée dans le domaine aérien. Désormais, il faut mettre en place un plan d'action pour essayer de faire converger les deux cultures que sont la culture de la cybersécurité, et la culture de la sécurité aérienne.

Ainsi, nous arrivons à la principale préconisation de ce mémoire. La sécurité aérienne se structure autour de la « culture juste ». « *La « culture juste » est « une culture dans laquelle les agents de première ligne ou d'autres personnes ne sont pas punis pour leurs actions, omissions ou décisions lorsqu'elles sont proportionnées à leur expérience et à leur formation, mais dans laquelle les négligences graves, les manquements délibérés et les dégradations ne sont pas tolérés. » Il s'agit de la définition donnée dans le règlement européen (UE) N° 376/2014 concernant les comptes rendus, l'analyse et le suivi d'événements dans l'aviation civile »*[99].

Dans l'aérien, les opérateurs ont l'obligation de faire remonter les incidents, accidents sans avoir peur d'être sanctionnés. Cette remontée d'information est faite au travers d'un formulaire à savoir le compte rendu d'évènements de sécurité.

C'est la raison pour laquelle, si la sécurité du transport aérien passe par ces remontées d'informations, nous préconisons d'introduire le risque cyber dans la fiche d'information de la DGAC. En effet, tous les employés du transport aérien pourraient avoir accès à un formulaire similaire.

Nous pouvons imager, par exemple, le cas d'un employé d'une compagnie

[99] https://www.ecologie.gouv.fr/observatoire-culture-juste-laviation-civile

aérienne chargé de l'opérationnel qui, dans sa boite mail professionnelle, reçoit des mails suspects. Il pourrait alors faire remonter l'information à travers un formulaire.

Autre exemple : le cas d'un pilote qui fait face à un bug des systèmes embarqués, il pourrait alors remplir une fiche dédiée aux cyber-incidents.

Nous pouvons également imaginer le cas d'un aéroport qui découvre une faille de sécurité dans la communication sol/air. L'opérateur pourrait alors avertir l'autorité. Cela permettrait de voir si ce bug qui est apparu dans un aéroport, ne pourrait pas se reproduire chez d'autre aéroports.

Nous préconisons également d'intégrer la cybersécurité dans les programmes des formations à prédominance juridique et managériale, telles que l'IFURTA, destinées aux futurs cadres du transport aérien. Tout comme au sein des formations de l'ENAC, la gestion du risque cyber dans l'aérien doit être intégrée dans tous les programmes.

Concernant les formations juridiques, nous préconisons davantage de droit du numérique et de compliance. En effet, les juristes du transport aérien seront en première ligne face aux nouveaux défis de la cybersécurité du transport aérien.

Enfin, il ne faut pas oublier les formations opérationnelles pour lesquelles nous préconisons un programme de sensibilisation au risque de cybersécurité. Les ateliers de maintenance, par exemple, vont devenir de plus en plus connectés. Leurs opérateurs doivent être formés en amont au risque cyber (par exemple, ne pas brancher son téléphone à un ordinateur des ateliers pour le charger).

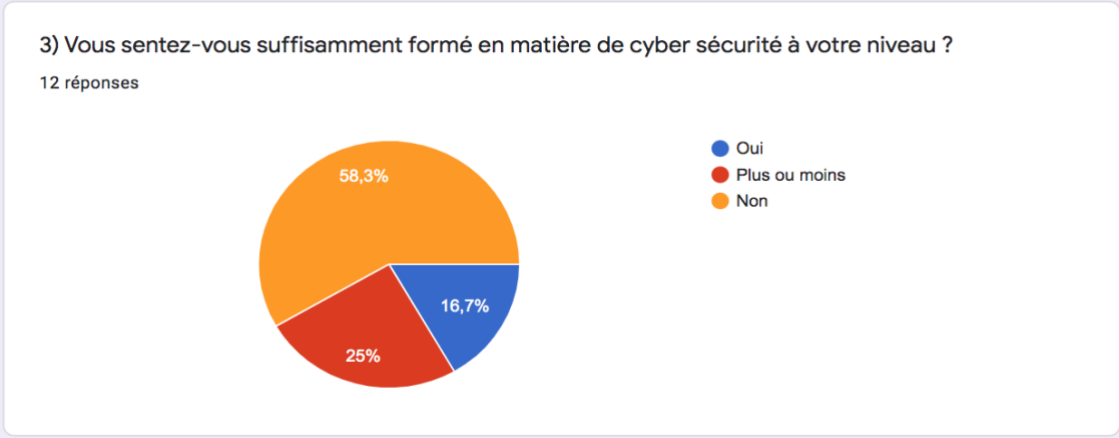
Pour conclure, nous avons lancé un questionnaire à diffusion large afin de pouvoir observer le niveau de connaissances des employés en matière de cybersécurité du transport aérien.

Les résultats sont encourageants même si peu d'employés semble sensibilisés. Un véritable début d'émulation en matière de cybersécurité du transport aérien a eu

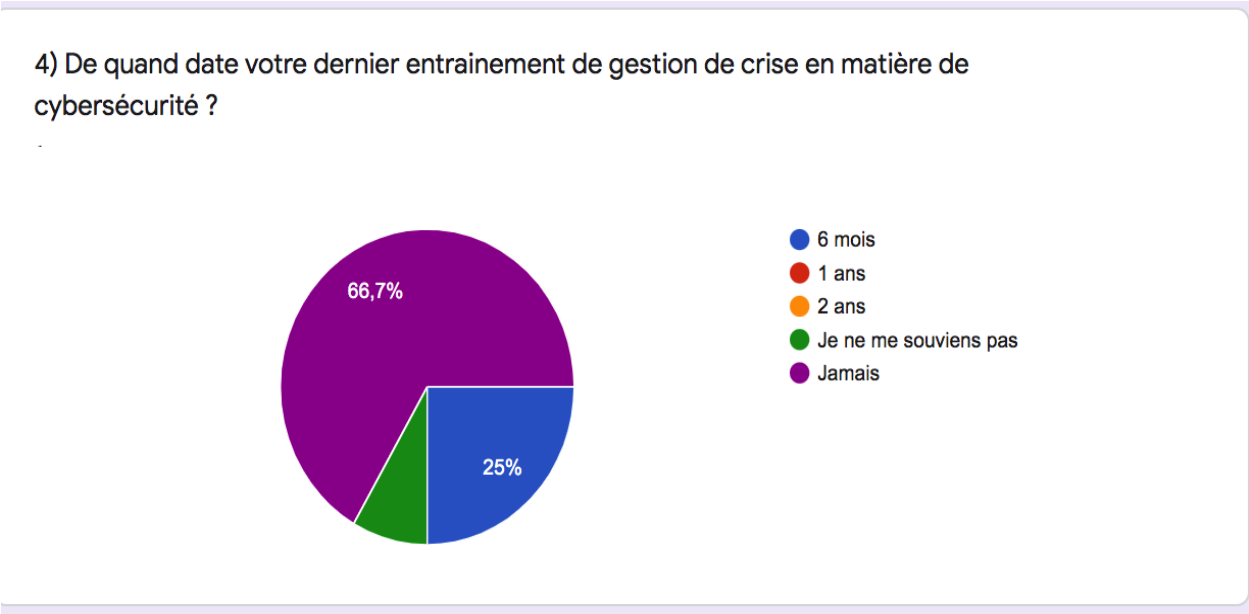
lieu ces dernières années.

Mais la crise du coronavirus est venue freiner les actions entreprise. Il reste encore du chemin à parcourir, comme le prouve ces résultats recueillis. En raison de la crise sanitaire, ce questionnaire en raison de la crise n'a pas pu être développé comme voulu. Il sert à confirmer ou à affirmer les différentes hypothèses mises en avant tout au long de ce mémoire.

Tout d'abord, en matière de formation de cybersécurité, 58,3 pourcent des personnes interrogées ne se sentent pas assez formées. Cela constitue un véritable problème que nous avons voulu mettre en lumière.

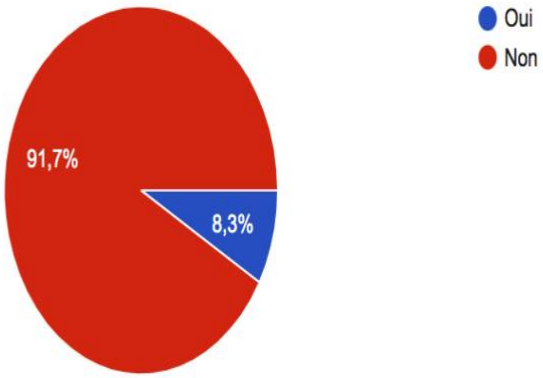


Ensuite, intéressons-nous à la gestion de crise : 66,7 pourcent des sondés n'ont jamais eu d'entrainement en gestion de crises en matière de cybersécurité. Il s'agit là encore d'un réel effort à fournir pour le transport aérien. Le risque cyber étant changeant, des entrainements et formations réguliers doivent avoir lieu. Certains aéroports, ainsi que compagnies, ont déjà mis en place quelques expériences, mais cela reste anecdotique.



Par la suite, nous avons à faire à la réponse la plus inquiétante de ce sondage. En effet, 91,7 pourcents des répondants ne se sentent pas assez formés en techniques de social engineering dont nous avons démontré l'importance d'y être sensibilisé. Les employeurs du transport aérien doivent absolument mettre en place des méthodes de sensibilisation cyber pour tous les employés. Pour ceux qui subissent la transformation numérique dans leur fonction, il faut les reformer. En effet, les compétences de certains opérateurs vont devenir totalement obsolètes. La formation continue à la cybersécurité est une clé essentielle à la cyberrésilience.

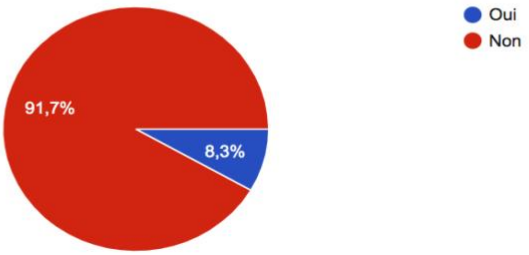
Beaucoup d'attaques cyber utilisent des techniques de social engenering. C'est-à-dire des techniques se servant d'informations d'employés pour arriver à pirater des systèmes. Pensez-vous que votre employeur vous a suffisamment formé à ces techniques ?



Enfin, deux réponses pointent du doigt la méconnaissance de la règlementation de la part des acteurs du transport aérien. Tel que vu précédemment, le règlement PART.AISS va pourtant imposer des obligations au niveau managérial qui vont directement toucher les employés. Pourtant, ces derniers ne semblent pas en avoir entendu parler.

A la douzième question, l'un des sondés avait une parfaite connaissance de la cybersécurité dans le transport aérien. Il a évoqué le fait qu'il fallait clarifier le rôle de l'autorité en charge de la cybersécurité (ENISA où AESA pour l'Europe par exemple.). Il a également parlé de la dualité entre le futur règlement part.AISS et la directive Nis comme évoquée dans ce mémoire. Enfin, l'employé a cité la notion d'harmonisation Européenne qui s'avère être essentielle en matière de cybersécurité.

11) Avez-vous entendu parler du nouveau règlement AESA nommé « PART AISS » qui impose aux compagnies, constructeurs et aéroports d'être pro-actifs en matière de cyber sécurité ?



12) Que pensez-vous de ce règlement ?

Plutôt une bonne idée

Clarifier le rôle de l'autorité en charge (aviation ou cyber).
Clarifier overlap NIS Directive vs Part AISS
Challenge pour autorités pour mettre en place un ISMS.
Durée de la transition pour la conformité au nouveau règlement.
Harmonisation au niveau Européen : même exigences quel que soit le pays.
Applicabilité aux petits acteurs (e.g aéroport).

Ainsi, ces quelques extraits nous prouvent que des efforts sont encore à faire en termes de compréhension du risque cyber par les employés du transport aérien. Les employeurs doivent donc mettre en place des formations de sensibilisation pour tous les employés et de manière régulière, en matière de cybersécurité.

CONCLUSION :

Nous arrivons ainsi au terme de notre étude. Nous pouvons à présent répondre à la question initialement posée : En quoi les cadres juridique, managérial et assurantiel en matière de cybersécurité favorisent-t-ils la cyber-résilience du transport aérien ?

Tout d'abord, nous avons démontré que le transport aérien, dès sa création, a toujours été accompagné par l'informatique. Depuis, le secteur aéronautique est en pleine révolution numérique. Les aéronefs deviennent et vont être de plus en plus connectés, tout comme les aéroports. L'aviation change, et de ce changement apparait le risque cyber.

Le transport aérien dispose déjà de bases nécessaires pour construire un écosystème solide en matière de cybersécurité ; grâce à sa culture de la sécurité, mais aussi grâce au corpus juridique. Ces atouts dont dispose le transport aérien doivent être utilisés pour pallier les nombreuses carences en matière de cybersécurité.

La cybersécurité dans le transport aérien, n'est dont qu'une composante de la cyber résilience de ce dernier. En effet, le juridique, le management, ainsi que les assurances, la culture et la cybersécurité, permettent la cyber résilience du transport aérien. Ces domaines doivent travailler en coopération au sein des organisations pour pouvoir atteindre réellement l'objectif de résilience.

Enfin, la cyber sécurité dans le transport aérien n'en est qu'à des débuts. La crise sanitaire a fait resurgir un risque nouveau pour le transport aérien : le risque sanitaire. Il ne faudrait pas que le risque cyber soit oublié ou mis de côté du fait de cette crise sans précèdent. Aussi, les investissements en matière de cybersécurité ne doivent pas être considérés comme non essentiels pendant cette crise.

Ainsi, dans le futur, le pilote d'aéronef sera de plus en plus en contact avec la machine ou pourrait même se voir supplanté par une machine « intelligente ». La

question des interactions hommes-machine se posent déjà dans le transport aérien. Qu'en sera-t-il de l'interaction homme – Intelligence artificielle ?

Bibliographie

I. Sources Législatives et Règlementaires :

- Le règlement n° 2016/679, dit Règlement Général sur la Protection des Données

- Convention de Montréal du 28 mai 1999 pour l'unification de certaines règles relatives au transport aérien international

- Règlement (UE) 2019/88 de la Commission du 18 janvier 2019, CybersecurityAct

- Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, Directive NIS

- Loi n° 2013-1168 du 18 décembre 2013, Loi de programmation militaire

- Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La loi Informatique et Libertés :

- Arrêté du 18 mai 2018 relatif aux exigences applicables aux télépilotes qui utilisent des aéronefs civils circulant sans personne à bord à des fins autres que le loisir

- Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Transports terrestres » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense

- R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du Code de la Défense

- Protocole additionnel à la convention pour la répression de la capture illicite d'aéronefs fait à Beijing le 10 septembre 2010

- Futur Règlement Part.AISS (20XX,XXX) : Notice of Proposed Amendment (NAPS) , « Management of Information Security Risk l », 2019

II. Ouvrages et Travaux :

- « *Le Livre blanc sur la défense et la sécurité nationale* », Ministère des armées, 2013

- « *Le manuel de Tallinn* », OTAN, Ed.Michael N Schmitt,2013

- E.Petit « *Histoire Mondiale de l'Aviation* » , Hachette, 1967

- F. Gorriez, « *Le Droit de la Cybersécurité* », Nuvis , 2020

- P. Agnes « *Intervention IFURTA : Facteurs humains* », 2019

- S. Maysan, « *Intervention Colloque Académie Air et de l'Espace* », 2019

-F. Denefle, « *Risques Cyber : Assurance des risques de demain ?* » Session Plénière, 2019

- J. Anton, Présentation : « *NPA 2019-07 "Management of Information Security Risks* », EASA Workshop on NPA 2019-*07,* 2019

- L. Archambault, « *Présentation Selene Avocats à l'Institut de Formation Universitaire et de Recherche du Transport Aérien* », 2019

- A. Frisch, DGAC, Présentation Séminaire sécurité des aérodromes, « *Les évolutions réglementaires attendues* », 2019

- J. Guitard, « *Cours de Gestion des Aéroports* », 20 ème édition, 2011

- Académie de l'Air et de l'Espace Actes du colloque : *« Vers des navires et aéronefs sans équipage ? Jusqu'où la machine peut-elle remplacer l'homme* » 2020

-Académie de l'Air et de l'Espace « *Cybermenaces visant le transport aérien* », Les Dossiers, n°45, 2019

- S. Kretzschmar, « *Présentation Séminaire Sécurité* », IFURTA, 2019

-J. Laborde dit Bouriat, « *Introduction au Droit Aérien* », IFURTA, 2020

-V. Brun, « Cours M2 Economie Transport Aérien » IFURTA, ,2020.

II. Thèses et Mémoires

- **Mémoire** :

W.Daoudi « *L'évolution du transport aérien de 1903 à 1995 : Les compagnies de pavillon aux alliances stratégiques* », Ecole des Hautes Etudes Commerciales Affiliée à l'Université de Montreal, Science de la gestion, 1996

R .Deslande « Présentation des programmes de cyberassurances et de leurs limites », Institut des Assurances Lyon, Mémoire de fin d'étude , 2017

L. GAVRILL, « Accident de Germanwings : Symptomatologie d'un métier en évolution et intégration des risques », IFURTA 2017

A. Brillaud, « Les NTIC dans le parcours passager : Quel futur pour l'expérience client en aéroport », Institut de Formation Universitaire et de Recherche du Transport Aérien (IFURTA), 2017

- **Thèse** :

M. Benejean, « *Informatisation des productions d'information et des activités de communication dans les relations pilotes-contrôleurs : Contradictions et reconfigurations entre technologies en projet et mises en pratiques* », Université de Toulouse, Ecole doctorale Aéronautique, 2013

III. Articles

J. Duriez-Mise « Un hacker aurait réussi à pirater un avion de ligne », Europe 1, Rubri. Technologie, 2016

J. Lago, « EasyJet : piratage des données de 9 millions de clients, un cabinet d'avocat réclame 20 milliards d'euros », France soir, 2020

H. Vernet, « Coronavirus : qu'est-ce-que l'opération Résilience", lancée par Emmanuel Macron ? », Le Parisien, Rubr. Politique, 2020

M. Simantov « L'aérien, un modèle pour la cybersécurité », Blog Medium, 2018

A. Naab « La cybersécurité, ou l'épée de Damoclès du secteur aéronautique. » Centre de ressources et d'information sur l'intelligence économique et stratégique ,2018

L. Guezo « Cybersécurité du nucléaire ? Où en est-on ? » Tribune, CyberCercle, 2015

B., Oriane. « Existe-t-il un droit international du cyberespace ? », Hérodote, vol. 152-153, no. 1, pp. 201-220, 2014

K. Poireault, « La filière aéronautique normande s'associe à AirCyber, le dispositif de cyber-protection de BoostAérospace », Industrie & Technologie, 2020

M. Garrin, « Le facteur, clé de la cybersécurité », Le Net Expert Informatique Cybersécurité & Conformité, 2017

F. DeCloquement « Espionnage, attaques subversives et cyber sécurité : de l'impact des actions de « social engineering » et des vulnérabilités humaines sur

la sécurité globale des entreprises », Sécurité et stratégie, vol. 22, no. 2, pp. 21-29, 2016

S. Barim, « Développer la culture sécurité de l'information numérique de son organisation », I2D – Information, données & documents, vol. volume 54, no. 3, pp. 49-50, 2017

Willis Tower Watson, « Willis Towers Watson launches innovative new cyber product for global airlines», Press Release, Avril 2017

Argus de l'Assurance, « Directeur Général de la Réunion Aérienne : " la couverture des risques de guerre est du ressort des états " », 2002

C. Domenech, « Une famille empêchée d'embarquer pour la Grèce à cause d'un nouveau formulaire mal rempli », 2020

S. Ghobri, « Premiers tests covid-19 obligatoires à l'aéroport de Nice Côte d'Azur »,2020

Collard, Christophe, C. Roquilly. « Les risques juridiques et leur cartographie : Proposition de méthodologie », La Revue des Sciences de Gestion, vol. 263-264, pp. 45-55, no. 5, 2013

L. Archambault, « Le concept de « privacy by design » à la rescousse des drones civils européens », Aérobuzz, 2017

Tiffany, « Le Cybersecurity Act la sentinelle contre les Cybermenaces », Blog Datanaos, 2019

C. Cimpanu, « Ransomware : black-out des écrans à l'aéroport de Bristol », ZDNet, 2020

M. Simantov, « Cyber sécurité dans l'aéronautique : sécurité où sureté ? », Blog Medium, 2019

M. Betus, « Innovation : ce que nous préparent les compagnies aériennes », Vol Retardé, 2017

X. Biseul, « Le voyage aérien plus fluide grâce au digital », Voyages d'Affaires, 2019

H. Pellegrin, « Comment Air France exploite-t-elle le digital en interne et en externe ? », Tom Travel, 2019

H. Meddah, « Être compétent en cybersécurité sera bientôt aussi important que de parler anglais », L'Usine Digital, Rubr.Cybersécurité, 2015

M. Angel, « A Toulouse, Thales dévoile son cockpit du futur », Industrie et Technologies, Rubr.Aéronautique, 2019

B. Trévidic, « Thales ouvre la voie au cockpit connecté et sans copilote », Les

Echos, Rubr. Tourisme Transport, 2017

Groupe ADP « dévoile « Play Your Airport », concours mondial d'innovation », Site internet parisaeroport.fr, 2020

M. Lardiray, " SITA : l'aéroport du future sera autant connecté que ses passagers", Tom Travel, 2019

Rédaction du Figaro, « Record d'affluence pour l'aéroport Paris-CDG », Le Firago, 2014

Communication Thales, Site internet Thales.fr, « De la sécurité à la cybersécurité aérienne », 2017

U.Roux, « La transforme digitale des entreprise », La Découverte, Repères, p.128, 2018

J. Jolu, « Pour ses mises à jour, Boeing utilise des disquettes des années 90 », Capital, 2020

S. Ghernaouti, & C. Aghroum, Cyberrésilience, risques et dépendances : pour une nouvelle approche de la cybersécurité. *Sécurité et stratégie*, 74-83, 2012

B. Cyrulnik. « Plongée dans l'univers de la résilience », Conférence, 2017

Question internationale, « Le transport aérien : une mondialisation réussie », Question internationales, n° 78 Mars-Avril, 2016

IV. Rapports publics

- Publication du site des assises du transport aérien, « Le transport aérien à l'air du numérique », 2018

- Club de la sécurité de l'information français (CLUSIF), « Rapport, Menaces informatiques et pratiques de sécurité en France », 2018

- Discours sur l'état de l'Union 2017, Bruxelles, J. JUNCKER, le 13 septembre 2017

- Conseil européen, Conseil de l'Union européenne, « La cybersécurité en Europe : des règles plus strictes et une meilleure protection », 2020

- Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), Rapport annuel 2019, 2019

- Rapport, assemblée OACI 39e session Montréal, 27 septembre – 6 octobre 2016

- Extrait de la Résolution A40-10 : Cybersécurité dans l'aviation civile, 2019

- Publication Ministère écologie ; Observatoire de la culture juste de l'aviation civile, 2020

- Rapport OACI SMM , « Safety In Aviation» , 2006

- E. Borne, « Conclusion des Assises nationales du transport aérien – Présentation de la stratégie nationale du transport aérien », 2019

- Rapport du Sénat J. Bockel: « La cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information n°681, 2012

- Le Programme National de Sûreté de l'Aviation Civile, OACI

VI. Sites Internet

- Site ENISA :

https://www.enisa.europa.eu/media/enisa-en-francais/

- Site CERT-UE :

https://www.cert.europa.eu/

- IATA :

https://www.iata.org/en/publications/store/aviation-cyber-security-toolkit/

- OACI:

https://www.icao.int/about-icao/pages/fr/default_fr.aspx

- Les Assise du Transport Aérien :

https://www.assisesdutransportaerien.gouv.fr/

ANNEXES

Table des annexes :

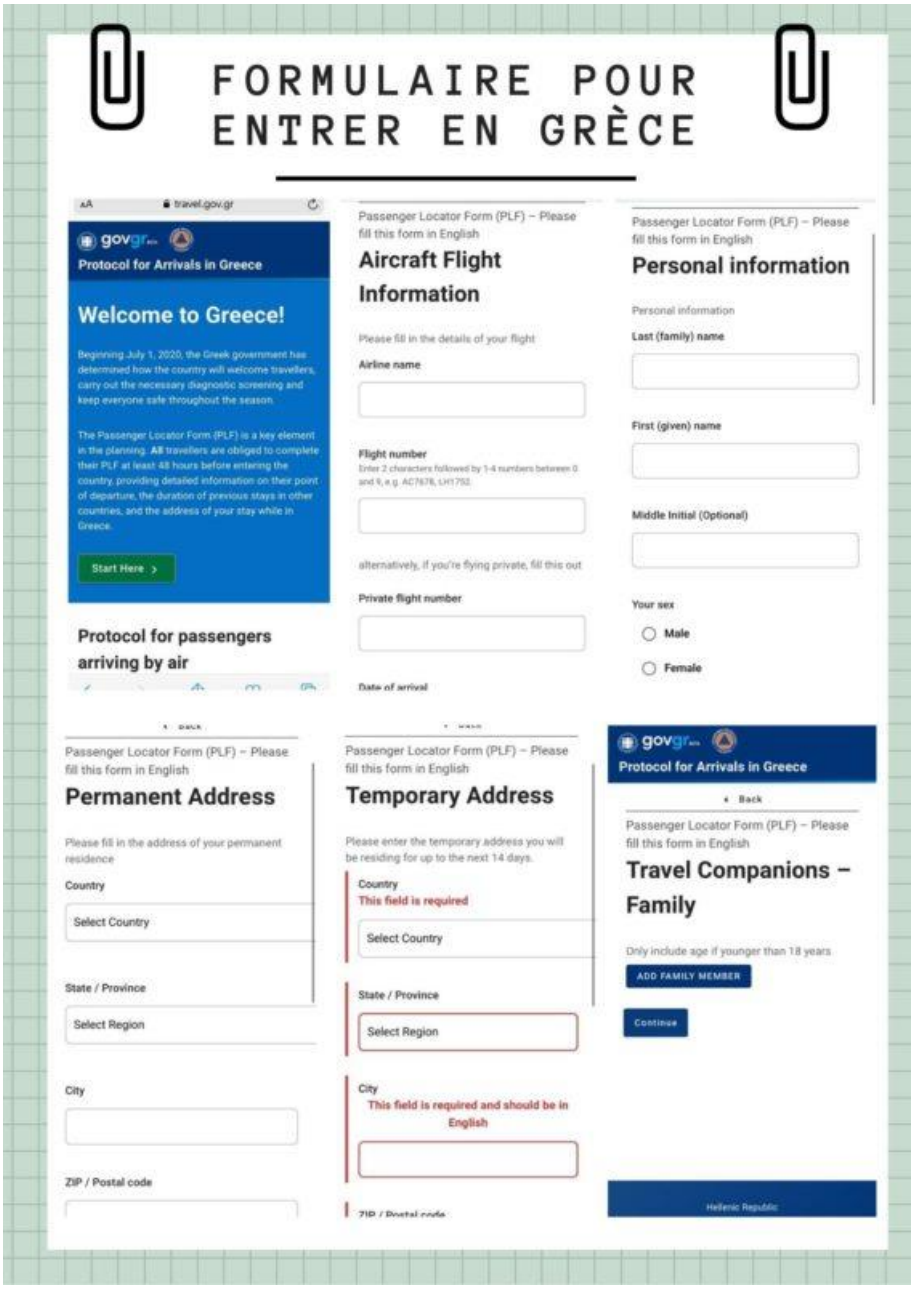
ANNEXE

ANNEXE I : LES RISQUES CYBER D'ORIGINE ACCIDENTELLE

5.1.6. Les risques cyber d'origine accidentelle

Incidents accidentels	Nature de l'évènement	Conséquences	Impacts financiers
Erreur humaine 	• Erreur de programmation, • Erreur d'implémentation, • Erreur d'utilisation, • Erreur de maintenance	▶ Arrêt des systèmes d'informations ▶ Responsabilité en cas d'erreur opération client, délivrance de bien ou services, ▶ Perte ou altération de données client, de données confidentielles, ou de données d'exploitation ▶ Procédure réglementaire	▶ Frais supplémentaires d'exploitation ▶ Frais de défense / Dommages et intérêts ▶ Frais de reconstitution de données ▶ Pertes d'exploitation ▶ Cout du matériel de remplacement ▶ Frais et sanction administrative
Panne/problèmes techniques 	• Défaut de maintenance • Problème de mise en production d'un logiciel • Problème d'interopérabilité des systèmes avec fournisseurs, tiers, client • D'origine industrielle électrique : commutation de contacts, fonctionnement de thyristors, etc. • Electronique : réseau de distribution, problème de relais,		
Evènement naturel 	• Incendie, • Inondation, • Dégât des eaux • Tempête • Foudre et surtension électriques liées		

ANNEXE II : FORMULAIRE COVID GRECE

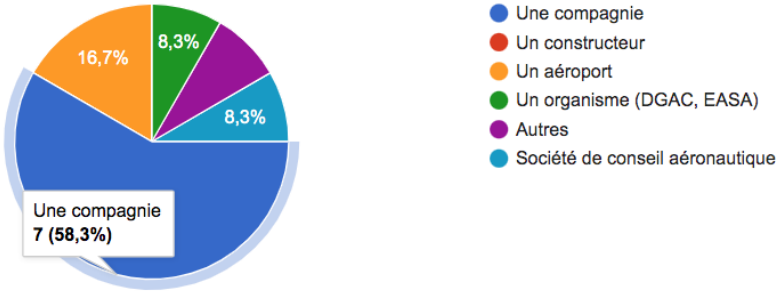


ANNEXE III : QUESTIONNAIRE VISION DES ACTEURS DU TRANSPORT AERIEN :

Résumé | Question | Individuel

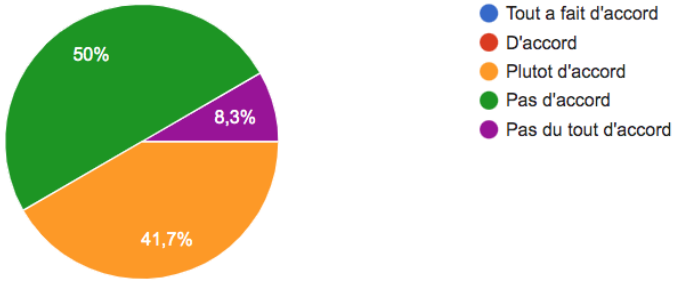
Vous travaillez pour :

12 réponses



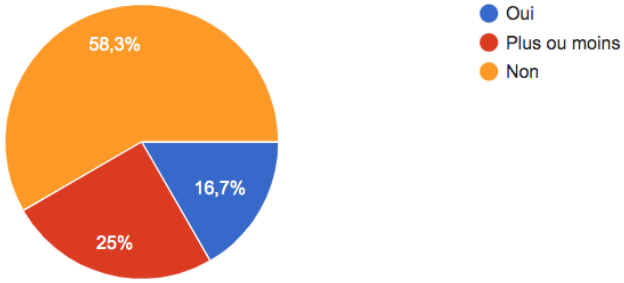
Le secteur aérien est bien préparé au risque cyber

12 réponses



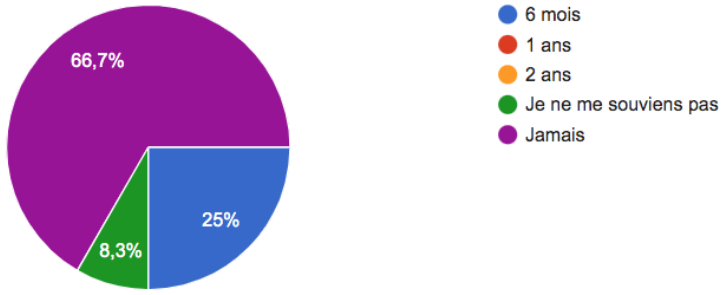
3) Vous sentez-vous suffisamment formé en matière de cyber sécurité à votre niveau ?

12 réponses



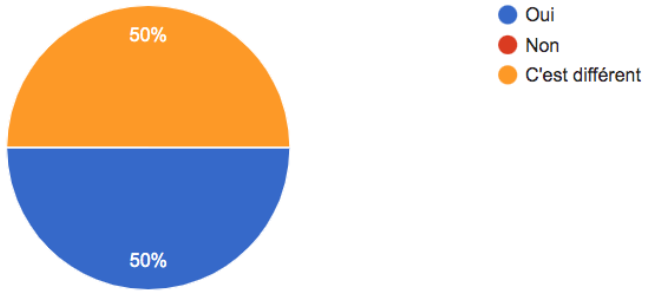
4) De quand date votre dernier entrainement de gestion de crise en matière de cybersécurité ?

12 réponses



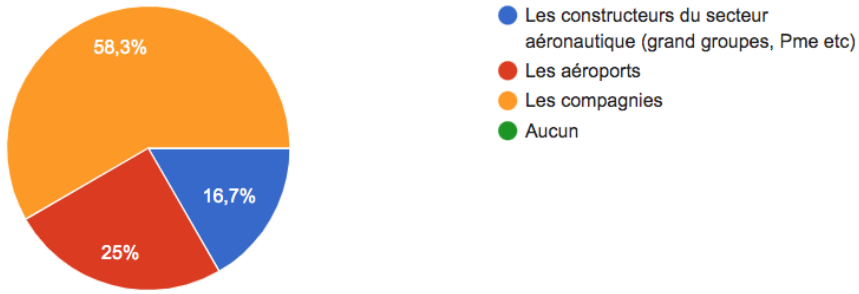
5) Pensez-vous que le risque cyber est aussi grave que le risque terroriste pour le transport aérien ?

12 réponses



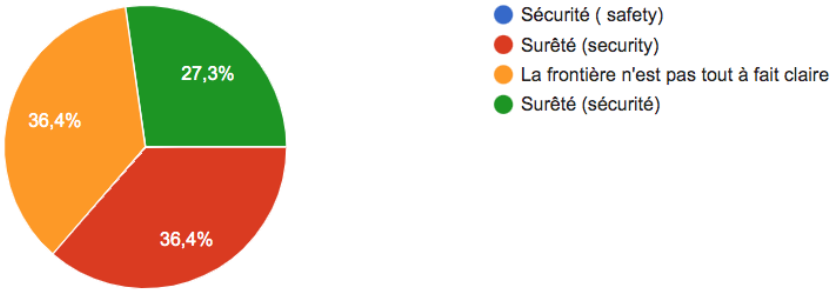
6) Pour vous, le risque cyber est plus prégnant pour :

12 réponses



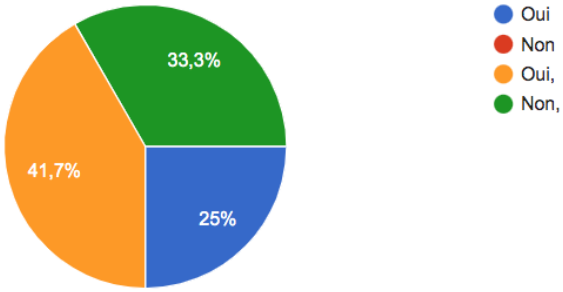
Vous considérez le risque cyber comme un risque de ?

11 réponses



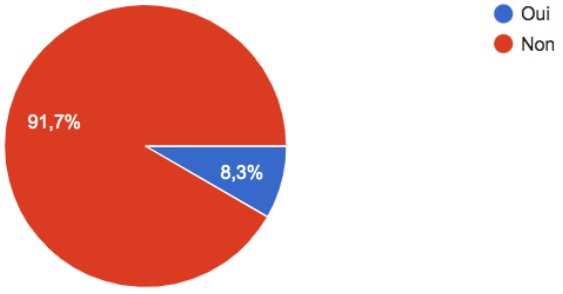
8) La culture de sécurité est cruciale pour le transport aérien. Chaque incident de sécurité des vols doit être remonté à la Dgac via un formulaire. Pensez-vous que les incidents cyber doivent être signalés de la même façon ?

12 réponses



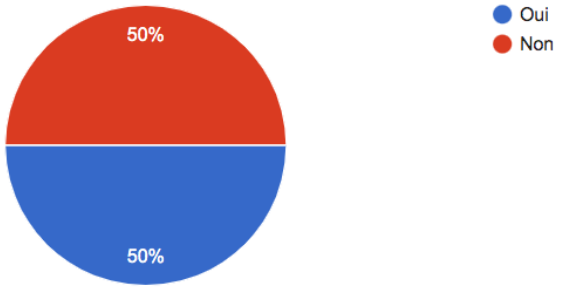
Beaucoup d'attaques cyber utilisent des techniques de social engenering. C'est-à-dire des techniques se servant d'informations d'employés pour arriver à pirater des systèmes. Pensez-vous que votre employeur vous a suffisamment formé à ces techniques ?

12 réponses



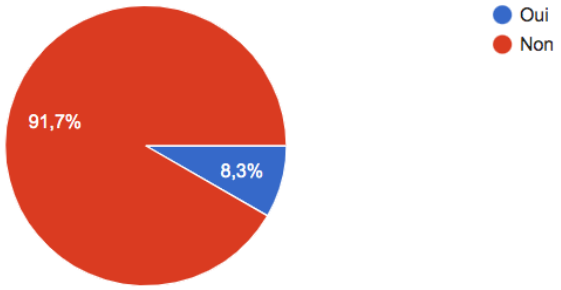
10) Pensez-vous que la focalisation sur la crise sanitaire fait oublier le risque cyber ?

12 réponses



11) Avez-vous entendu parler du nouveau règlement AESA nommé « PART AISS » qui impose aux compagnies, constructeurs et aéroports d'être pro-actifs en matière de cyber sécurité ?

12 réponses



12) Que pensez-vous de ce règlement ?

2 réponses

Plutôt une bonne idée

Clarifier le rôle de l'autorité en charge (aviation ou cyber).
Clarifier overlap NIS Directive vs Part AISS
Challenge pour autorités pour mettre en place un ISMS.
Durée de la transition pour la conformité au nouveau règlement.
Harmonisation au niveau Européen : même exigences quel que soit le pays.
Applicabilité aux petits acteurs (e.g aéroport).

ANNEXE IV : STRATEGIE CYBERSÉCURITÉ OACI

STRATÉGIE DE CYBERSÉCURITÉ DE L'AVIATION

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

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

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

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

Cette vision peut être réalisée comme suit :

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

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

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

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

1. Coopération internationale
2. Gouvernance
3. Législation et règlements efficaces
4. Politique de cybersécurité
5. Partage de l'information
6. Gestion des incidents et planification d'urgence
7. Renforcement des capacités, formation et culture de cybersécurité

Table des matières :

[100] « *Dans la mythologie **grecque**, Cerbère (en **grec** ancien Κέρβερος / Kérberos) est le chien à trois têtes gardant l'entrée des **Enfers**, empêchant les morts de s'échapper de l'antre d'Hadès et des vivants de venir récupérer certains morts* ».

RESUME

Du fait de la révolution numérique, le transport aérien vit une véritable transformation digitale. Cela fait apparaitre un nouveau risque, jusque là peu présent dans le transport aérien, le risque cyber. Depuis ces dernières années, le terme cybersécurité fait son apparition dans le monde aéronautique. C'est moins le cas pour le terme cyber résilience. Pourtant, le transport aérien est par nature une industrie résiliente. Néanmoins, est-elle cyber résiliente **?** Quelles sont les caractéristiques de cette cyberrésilience ? Nous étudierons l'apparition du risque cyber dans le transport aérien, ainsi que toutes les mesures mises en place pour atténuer ce risque en matière de droit, management et d'assurances.

MOTS CLES

Cybersécurité du transport aérien ; Cyber résilience ; Digitalisation ; Facteurs humains

SUMMARY

Faced with the digital revolution, air transport must take the cyber threat seriously. In recent years, the term cybersecurity has appeared in the aeronautical world. Air transport is a resilient industry that resists crises. But is it cyber resilient? What are the characteristics of this cyber resilience? We will study the emergence of cyber risk in air transport, as well as all the measures put in place to mitigate this risk in terms of law, management and insurance.

KEYWORDS

Cybersecurity of air transport; Cyber resilient; Digitalization; Human factors