CYBER CERCLE
collection

SÉCURITÉ NUMÉRIQUE & AÉRONAUTIQUE

Regards croisés

Pascal ANDREI | Nathalie FEYT
Anaïs BENSAÏ | Patrick KY
Diane BERTONCINI | Jean-Marc LAURENT
Stéphanie BUSCAYRET | Colonel Forian MANET
Damien CAZÉ | Laurent PIC

Préfaces de Bénédicte PILLIET & Eric VAUTIER

2022

SÉCURITÉ NUMÉRIQUE et AÉRONAUTIQUE

Regards croisés

Ce livre est édité sous la direction de
Bénédicte PILLIET, Présidente du CyberCercle

Préface

BÉNÉDICTE PILLIET
Présidente
CyberCercle

Quand nous avons engagé en 2015 un travail de réflexion sur le secteur maritime, certains acteurs de l'aéronautique étaient venus nous voir en nous demandant « pourquoi les marins et pas nous ? »… De même après la parution fin 2020 dans notre Collection CyberCercle - Regards croisés, du premier ouvrage sur la cybersécurité maritime.

Grâce à l'implication de notre senior advisor, Eric VAUTIER, grand RSSI dans le secteur aéronautique qui a coordonné cet ouvrage, nous pouvons aujourd'hui présenter des contributions éclairantes sur la manière dont ce secteur, secteur stratégique s'il en est, fait face au risque numérique. Comment, au-delà de la prise en compte au sein des entreprises, ce secteur complexe, riche d'organisations très différentes tant dans leurs champs de compétences que dans leurs structures, s'est engagé aux niveaux national, européen et international, dans une démarche collective indispensable.

La dynamique pour une culture et des actions de sécurité numérique partagées entre les acteurs du secteur aéronautique est lancée : le CyberCercle continuera de répondre présent pour y participer.

Je tiens à remercier Eric VAUTIER sans lequel cet ouvrage n'aurait pu être réalisé ; l'ensemble des contributeurs d'avoir accepté de partager ainsi leur expertise et leur vision ; et nos partenaires, Avant de Cliquer et Certitude Numérique, qui ont contribué avec nous au financement de cet ouvrage.

« *Seul on va plus vite, ensemble on va plus loin* ».
Cette maxime que le CyberCercle a fait sienne depuis sa création s'applique également, et ô combien, au secteur aéronautique.

Je vous souhaite une bonne lecture.

Préface

ERIC VAUTIER
Senior Advisor
CyberCercle

Faire décoller, voler et atterrir des avions est une des activités où le génie humain a le mieux trouvé à s'employer : théoriser la navigabilité, concevoir les avions, les fabriquer à la perfection, former les pilotes capables de les maîtriser, toutes ces activités ont nécessité la mise en place de processus rigoureux, testés et affinés au fil des décennies, permettant à l'aviation commerciale de devenir le moyen de transport le plus sûr. Tout naturellement, la réglementation et la certification ont accompagné ce développement afin de garantir le respect de toutes les normes et procédures sur lesquelles reposait la théorie d'un vol en toute sécurité.

Plus tard sont apparus les « acts of unlawful interference » - pour reprendre le vocabulaire de l'Organisation de l'Aviation Civile Internationale - et l'industrie de l'aviation s'est organisée pour les prévenir, sans pouvoir tous les anticiper, hélas. Le domaine de la sûreté est devenu depuis le plus visible du passager en raison des contraintes qu'il subit avant de pouvoir embarquer. Là encore, la réglementation a étroitement encadré ces processus cruciaux pour la sécurité des passagers.

Et aujourd'hui, le risque cyber vient s'ajouter à la longue liste des risques à évaluer et à traiter afin de garantir cette fiabilité mais, et c'est une nouveauté, nécessite une réflexion double : individuelle au niveau de chaque opérateur - constructeur, compagnie aérienne, aéroport, contrôle aérien - mais aussi systémique puisqu'une vulnérabilité chez l'un peut finalement être exploitée chez l'autre.

Vous découvrirez au fil des interventions réunies dans cet ouvrage la variété et la complexité des questions que soulève la prise en compte de ces nouvelles exigences et comment l'industrie de l'aviation coopère pour y répondre à la fois localement et globalement. Nous espérons que vous prendrez autant de plaisir à les lire que nous en avons eu à les rassembler.

De la nécessité d'un continuum de sûreté pour le transport aérien

PASCAL ANDREI
Senior-Vice-president
Chief Security Officer
Airbus

L'évolution de la menace à bouleversé les principes de base des organisations chargées de la sûreté (security) des entreprises. Certaines certitudes, fondées sur des années de routine et emballées sous les voiles du « secret » se sont effondrées.

Dans l'aéronautique comme dans bien d'autres secteurs d'activités, la menace est mondiale, physique ou cyber. Au fil de l'évolution des technologies et des techniques, les frontières entre ces deux mondes se sont estompées. Il est devenu nécessaire de casser les silos, rompre le silence et intégrer les menaces dans une analyse des risques exhaustive, commune et harmonieuse.

Croire que l'on peut encore compartimenter la sûreté par domaine est une erreur à ne plus commettre. L'interpénétration des domaines se matérialise tous les jours : quelques lignes de programme informatique suffisent à priver un pays entier d'électricité, un sabotage physique d'un composant matériel peut déposséder une région entière de connexion internet, ou encore la corruption d'un système vidéo peut nuire à la protection d'un site physique… L'heure du « Phygital » a bien sonné et la transformation numérique de toutes nos activités économiques, parfois réalisée à marche forcée pour cause de pandémie, augmente tous les jours la dépendance de nos entreprises aux ressources numériques et surtout leur surface d'exposition aux attaques cyber.

Les « cybermenaces » en ont certainement été le déclencheur. Elles concernent toutes les ressources connectées. Il nous faut mieux les

comprendre pour les anticiper et s'en protéger. Cela demande un énorme travail d'inventaire et d'analyse. Mais cela implique aussi une campagne de ralliement de toutes les fonctions d'une société qui ne doivent plus « se reposer » sur l'organisation de sûreté mais comprendre qu'elles font pleinement partie de ce continuum de sûreté.
Ces quelques lignes n'ont aucunement l'intention de donner une leçon « d'organisation nominale » de la sûreté d'une entreprise en 2022. L'efficacité d'une organisation est tellement liée à l'entreprise elle-même, qu'il n'existe pas de recette commune. Contentons-nous de partager les schémas directeurs et les nouveaux principes de base de ce changement de paradigme.

Airbus : un risque intégré dans la gouvernance depuis les années 90 grâce à l'avion et plus particulièrement l'A380

Airbus a depuis longtemps intégré cette donnée dans son organisation. Le premier modèle de gouvernance de la sûreté « nouvelle génération » s'est construit dès la fin des années 90 avec le développement de l'A380.

Largement connecté, très disruptif par rapport à ses prédécesseurs, le programme A380 a imposé le changement de paradigme évoqué ci-dessus, en embarquant à son bord et à grande échelle, des équipements COTS[1] et de l'informatique, dite standard. Pour la première fois, l'avion n'est plus uniquement constitué de systèmes propriétaires, connus seuls des ingénieurs chargés de leur conception et dépendant des standards aéronautiques. La conception de l'avion plus ouverte à l'utilisation de logiciels et d'équipements

commerciaux, grand public, largement utilisés et connus mondialement a ainsi conduit Airbus à changer radicalement sa façon de concevoir ses produits,avec une sûreté intégrée dès la conception.

Dès lors, la sûreté n'est plus seulement un sujet qui concerne les outils de conception informatiques de l'avion (maquette numérique, simulateurs, chaînes de fabrication…) mais bien le « produit avion » lui-même et son opération dans son écosystème.

A cette époque, le modèle clair de gouvernance permettant d'englober l'ensemble des aspects de sûreté (physique et cyber) de l'avion n'existait pas : il a donc été vital d'éclater les silos et les périmètres jusque-là isolés, peuplés de spécialistes centrés sur la sécurité des systèmes embarqués avec une vision très « safety » (sécurité), pour élargir la capacité du groupe à prendre en compte toutes les sources de menace issues des environnements de développement et d'opérations, dans une approche à la fois spécialisée et élargie.

Pour le développement et la production de cette 1ère génération des e-enabled aircraft, la « Security By Design » devient alors sine qua none. Pour éprouver l'efficacité de la méthode, Airbus va recruter une quinzaine de « hackers » : initiative osée et disruptive il y a 30 ans… Cette méthode a engendré une évolution du principe fondateur du développement et de l'intégration d'un avion au sein du bureau d'études : la V&V (Validation et Vérification)- en s'élargissant à l'Évaluation (tests de hacking) devient la V&V&E. Le nouveau standard de développement de la sûreté embarquée est ainsi né. Une volonté qui n'a pas été sans susciter d'interrogations et de résistance mais qui s'est révélée payante, dès la phase de conception du programme en cours et pour tous les programmes suivants.

Ce fut un coup de maître car cette nouvelle génération d'avions s'est retrouvée être la cible d'individus sur internet, clamant leur capacité à prendre le contrôle d'un avion à partir d'un ordinateur, voire d'un smartphone. Revendications qui font d'ailleurs régulièrement l'objet de conférences et publications, toutes contredites. Aussi, Airbus a le devoir de démontrer que ses produits sont robustes et protégés contre ce type de scénario. L'avion est le système de transport le plus sûr du monde et il doit le rester malgré des avions de nouvelle génération, plus communicants, plus connectés. Notre préoccupation de toujours, au cœur du métier d'Airbus, est la sécurité des usagers : préserver l'image de marque de l'entreprise et la confiance des clients dans les produits Airbus fait partie des missions de l'équipe sûreté.

Le monde aéronautique est très fortement régulé, essentiellement et par tradition, en matière de sécurité. La sûreté est, depuis cette période,

intégrée dès la conception de nos produits, quels qu'ils soient, et jusqu'à leur fin de vie (démantèlement ou déconstruction). C'est dans l'ADN d'Airbus : le challenge est alors de le démontrer, de le prouver, sans dévoiler ni de secret industriel ni d'information critique aux yeux malintentionnés. Désormais, il faut s'assurer de la sûreté complète de l'avion, sûreté physique et cyber. Travailler en silos, si performants et spécialisés soient-ils, ne fonctionnent plus. La « Safety » et la « Security » démontrent, plus que jamais, leurs synergies à l'heure de l'avion connecté.

Au-delà de l'aspect cyber, il a fallu intégrer la menace physique et ses diverses composantes dans la grande matrice des menaces, qui au final, ont permis d'avoir une vision synthétique et harmonieuse du risque « security » intégré globalement. Une vraie vision de l'ensemble des risques de sûreté et de leurs interrelations !

L'ensemble des produits d'Airbus (avions, hélicoptères, satellites, missiles, drones, lanceurs) se doivent d'être pensés en tenant compte de toutes ces menaces, d'autant que certains d'entre eux ont un double usage civil et militaire, encadrés par des réglementations différentes, de nouvelles attentes des clients ou régulateurs.

Puis vint la sûreté de l'environnement industriel…

Très rapidement, le constat fut que la sûreté des systèmes embarqués n'était plus suffisante pour garantir celle du produit final et de son opération (en service). Les environnements industriels, longtemps laissés à leur propre gestion au sein des programmes avions sont devenus une composante majeure de la chaîne de protection de tous nos produits. Les sites de production, d'assemblage, de tests et essais, de livraison de ses derniers ont dû être challengés et repensés. Des organisations et des comités internes dédiés ont ainsi vu le jour afin de prendre en compte cette dimension nouvelle, ayant la capacité d'assurer la sûreté aussi bien des environnements hérités que celle des chaînes d'assemblage de nouvelle génération (A350 , A320 NEO, A330…). Cette gouvernance couvre à présent l'ensemble de la chaîne d'approvisionnement, devenue dans le même temps, un des vecteurs de menaces les plus importants dans le risque global monitoré par Airbus.

Cette extension du périmètre des activités de sûreté a par la suite été renforcée par une équipe dédiée au Département Service Client, qui assure la continuité de la chaîne de confiance pour garantir une sûreté de bout en bout, allant jusqu'à l'accompagnement des opérateurs finaux.

Gérer les risques aujourd'hui et demain

En tant qu'avionneur, prenons encore un peu plus de hauteur (et ça nous savons le faire…).

Autant d'entrées dans le périmètre de protection nécessite d'englober tous les actifs dans une gouvernance commune pour assurer le continuum de sûreté global pour l'entreprise, ses produits et ses clients. L'enjeu de cette gouvernance est aussi de coordonner la manière dont on gère les risques dès aujourd'hui pour les produits qui voleront demain.

A titre d'exemple, le futur système de combat européen amène à couvrir des champs d'expertises nouveaux, que nous n'avions pas prévus d'établir en interne il y a tout juste 5 ans : interconnexion de « systèmes de systèmes » externes, l'intelligence artificielle pour la sûreté temps réel, l'informatique quantique, la 5G… et tout ceci auprès de différents partenaires, sur terre, dans les airs et dans l'espace.

Pour l'ensemble de nos activités, au service de la stratégie d'entreprise, la Direction Générale du groupe a besoin d'une vue à 360° des risques auxquels notre société est exposée : de la sûreté physique à la sûreté numérique en passant par la sûreté des produits, des usines, des équipements industriels et des lieux de travail, des services commercialisés par Airbus…

Le périmètre en question chez Airbus couvre plus de 23 000 produits « volants », des milliers d'applications critiques, plus de 300 000 voyages professionnels par an, 7 000 systèmes de contrôle industriels, répartis sur plus de 200 sites géographiques dans plus de 60 pays dans le monde dont certains à hauts, voire très hauts risques… Il nous faut connaître, comprendre et appliquer toutes les réglementations qui régissent cet immense périmètre. Pour ce faire, une organisation conséquente est en

place au sein du groupe. C'est cette communauté globale et internationale qui protègent Airbus et ses produits, et qui assurent le continuum nécessaire pour couvrir les risques, sécuriser les actifs critiques et assurer la résilience des opérations associées.

Lors des évènements récents survenus en Ukraine, nous avons dû assurer la sûreté des expatriés pendant leur rapatriement, celle des employés sur place, des installations localisées dans les différents pays concernés tout en surveillant les cyber-attaques liées à l'évènement. Sans coordination entre les équipes, les risques pourraient être mal appréhendés et l'efficacité des actions mise à mal.

Qu'elles soient cyber ou physiques, toutes les menaces doivent être considérées, anticipées et gérées, y compris dans l'organisation de gestion de crise, qui fait d'ailleurs partie de la Sûreté. Mais qu'en est-il de la menace ? Car qui dit menace dit implicitement risque induit. Si le CERT[2] est notre meilleur organe de « Threat Intelligence », il faut lui associer l'anticipation des menaces afin d'assurer une couverture complète des risques présents et à venir. Certains groupes ou institutions intègrent des équipes composées d'écrivains, scénaristes, auteurs de science-fiction voire même de créateurs de jeux vidéo dont le seul objectif est de sortir du contexte classique et des sentiers trop fréquentés par les spécialistes du domaine. Penser « out of the Box » comme ils disent. C'est une direction que nous prenons aussi à notre échelle car l'anticipation reste le maillon fort à la fois de la gestion des risques, des plans de reprise et de continuité d'activité (PRA / PCA)[3] et de la gestion de crise.

Une gestion des ressources humain ré-adaptée aux nouveaux métiers de la sûreté

Dans le domaine de la sûreté et plus particulièrement celui de la cybersécurité, il reste un terrain sur lequel de rudes batailles sont engagées y compris entre alliés : les ressources et le partage des compétences.

Les métiers de la cybersécurité sont en croissance et les flux de ressources sont bien trop faibles face à la demande. Débutants ou expérimentés, les candidats se font rares et se voient offrir des opportunités, en particulier

chez les GAFAM, contre lesquelles il est difficile de lutter. Les salaires ont souvent raison de la passion ou des challenges que nous pouvons proposer. Chez Airbus, les métiers liés à la sûreté ont évolué et nous devons garantir un développement de carrière à l'ensemble de nos métiers de la sûreté, physique ou digitale. Experts ou managers, spécialistes ou généralistes, chacun doit y trouver sa place et pouvoir se développer selon ses aspirations. C'est un véritable bouleversement de la gestion des ressources humaines. Lorsqu'on est un spécialiste cyber, Airbus n'est pas la porte à laquelle on frappe en 1er, car vue comme une entreprise d'ingénieurs passionnés par l'aéronautique et le spatial. Pourtant, il faut écouter ces profils et leur donner ce qui les nourrit, ce qui les motive, ce qui les retient. Leur offrir des possibilités variées de mobilité dans un groupe aux multiples domaines. Il faut témoigner de leur grande utilité dans un environnement qui se doit d'être à l'écoute, réactif et dynamique. Rien n'agace plus un « pentester » que de voir son rapport croupir dans un tiroir, attendant le déluge, ou encore d'entendre de bien mauvaises raisons de ne pas mettre en application leurs recommandations pourtant étayées et abouties. Il faut par-dessus tout leur donner un plan de développement et les moyens de maintenir leurs compétences. Tout cela ressemble plus à la gestion d'une start-up que d'un grand groupe. C'est la règle imposée et il faut jouer le jeu. De ce fait, un autre rôle clé dans nos organisations, méconnu jusqu'à lors, a émergé : le manager d'experts et de spécialistes cyber.

Très peu de personnes ont la compétence pour couvrir tous les domaines et savoir-faire. Aucun à vrai dire. Il faut pouvoir compter sur des spécialistes, des experts et des experts séniors pour adresser tous les niveaux de sûreté et en anticiper les évolutions. Recruter, former et faire évoluer les talents de la sûreté est un challenge permanent pour l'organisation : la stratégie du continuum est là-aussi mise en œuvre afin d'ouvrir les champs d'activité multiples des métiers de la sûreté.

La pénurie de talents touche Airbus comme les autres sociétés et la stratégie choisie par le groupe est d'accompagner ses talents pour développer leurs compétences et leurs savoir-faire au sein d'un parcours encadré et reconnu par l'organisation. Un professionnel de la sûreté pourra soit approfondir ses connaissances dans son domaine de prédilection ou étendre ses compétences plus largement sur des domaines annexes, selon son souhait.

A titre d'exemple, pour pallier au manque de candidats spécialistes en cybersécurité, Airbus crée en 2022 son propre diplôme Cyber, destiné à préparer ses futurs collaborateurs à la multiplicité des spécialités cyber existantes au sein du groupe. Animés par des collaborateurs du groupe volontaires, le cursus permettra aussi aux apprenants d'intégrer en immersion les valeurs du groupe.

La gestion de la variété des métiers de la sûreté, de leurs disparités, de leur complémentarité, de leur interopérabilité, des expertises et spécialités qui les composent… est un véritable challenge tant pour les Ressources Humaines que pour les managers en charge. L'alchimie livre alors tout son sens. Chacun des deux mondes apportant le meilleur de lui-même au service d'un tout.

ONE SECURITY : une pour tous et tous pour une

La sûreté doit s'ouvrir, fédérer et communiquer. Quel changement majeur ! Ce domaine resté si longtemps sous silence doit à présent, pour se défendre, apprendre à communiquer, à collaborer. Jamais les coopérations n'ont été si fructueuses. Devant une menace de plus en plus organisée, maîtrisant les multiples réseaux d'échange, il nous faut user des mêmes armes entre partenaires. Sous-traitants, équipementiers, aéroports, services de la navigation aérienne, fournisseurs de moyens de communication, opérateurs et compagnies aériennes… tous doivent s'entendre, y compris entre concurrents. Cela peut surprendre, mais la collaboration entre Boeing et Airbus a toujours été excellente dans le domaine de la protection de nos produits, dans l'intérêt global de la sûreté de l'aviation commerciale.

Une sûreté pour tous et tous pour la sûreté devrait être notre slogan !

En effet, il est important de comprendre que la sûreté de l'entreprise n'est pas sous la seule responsabilité du Directeur de la sûreté. Il en a le commandement, c'est-à-dire la définition de l'ambition, de la vision et de la stratégie globale, mais il en a certainement pas les responsabilités opérationnelles incombant aux fonctions (métiers) de l'entreprise et à chaque employé.

Les principales fonctions de l'entreprise (Bureau d'étude, Production, Finances, Achats, Ressources Humaines, Service client…) ont la responsabilité de faire l'inventaire de leurs biens et actifs et d'en catégoriser la criticité. Le département de la sûreté, quant à lui, décrit les menaces associées, leur vraisemblance et les moyens de s'en protéger. Ce n'est que la convergence de ces deux responsabilités qui définit les risques globaux et résiduels respectifs.

Quant aux employées, qui doivent être notre meilleure ligne de défense (en appliquant les principes de base tels décrits dans les directives de sûreté ou au travers de training et campagnes de sensibilisations) ne doivent plus être un vecteur de menaces, comme les statistiques le montrent, notamment dans le cas des ransomware.

Ainsi, la Direction de la sûreté doit définir le modèle de gouvernance et de sensibilisation le plus approprié pour enrôler salariés et fonctions dans une même dynamique et en garantir le résultat.

Le choix fait à Airbus a été de mettre en place un « Council » de haut niveau, appelé « Corporate Security Council » (CSC), couvrant tous les domaines (physique et digital/cyber), toutes divisions (Airbus Commercial, Airbus Helicopters et Airbus Defense & Space), tous les biens (assets).

Ce continuum de sûreté pour protéger tous les actifs du groupe, s'est organisé autour de 4 piliers qui couvrent l'ensemble des périmètres évoqués et reportant au CSC :

1. La sûreté des systèmes industriels et de nos fournisseurs
2. La sûreté des produits (avions, hélicoptères, satellites, drones…) et des services (maintenance prédictive, gestion des flottes…)
3. La sûreté des personnes et de tous les sites de travail (ex : voyageurs, expatriés, pays à risques)
4. La sûreté des systèmes d'information, de l'IoT et des données (ex : notre infrastructure technique, nos architectures mondiales et communications associées, les informations critiques…)

Ces organes de coordination sont composés de membres opérationnels de toutes les entités d'Airbus, tant venant de la sûreté que des fonctions.

Ce Council se réunit régulièrement ou de façon ad hoc et reporte directement au Comité Exécutif et au Conseil d'Administration.

Le Continuum de sûreté : un rôle devenu majeur

La combinaison des rôles dans le continuum de sûreté est nécessaire pour protéger une entité comme Airbus, elle est une force de l'organisation pour assurer la continuité d'activité et le développement des opportunités à venir.

Le 1er rôle de l'organisation sûreté d'Airbus est de protéger le groupe et ses intérêts.
Le 2ème est d'assurer des relations de confiance avec les autorités, clients, régulateurs, actionnaires.
Le 3ème est de développer des opportunités économiques à l'extérieur du groupe, via les activités de services qu'Airbus propose. Au-delà de la contribution au portefeuille commercial du groupe, ce volet permet de voir et de comprendre comment les menaces évoluent dans d'autres secteurs, ce qui apporte de la valeur pour le groupe lui-même.

Parce que personne ne peut combattre le cybercrime seul, réaffirmer les enjeux pour un groupe international comme Airbus, c'est :

- Disposer d'un véritable support, affirmé, de la part de la Direction Générale et des actionnaires, car les moyens d'assurer la protection du groupe ne peuvent pas être attribués sans une compréhension globale des enjeux par la direction.

- Assurer l'engagement global des salariés. Sans un comportement exemplaire des collaborateurs, assurer la sûreté est impossible. La menace rançongiciel illustre bien l'inutilité des protections techniques les plus élaborées si les collaborateurs n'ont pas le comportement responsable et conscient que l'on peut attendre de la 1ère ligne de défense. L'effort est immense en matière de sensibilisation et l'hétérogénéité des métiers et cultures présents dans le groupe ce qui requiert une adaptation fine aux profils et aux contextes d'exercice.

- Disposer d'une expertise de haut niveau, pour développer les programmes de demain, sécuriser les technologies innovantes. Cette expertise en cyber est reconnue à l'international : les équipes sûreté d'Airbus sont régulièrement primées lors de compétitions internationales.

- Se donner les moyens d'attirer et de former les talents dont le groupe a besoin comme avec le diplôme Cyber Airbus

- Rivaliser avec les GAFAM pour retenir ses talents et leur permettre de développer leurs compétences au sein du groupe. Airbus offre une variété incomparable des métiers de la sûreté, au-delà de la cybersécurité, pour proposer des parcours d'évolution de carrière que très peu d'organisations peuvent offrir aujourd'hui.

- Se positionner comme un acteur clé de la cybersécurité du secteur aéronautique, en participant aux conférences mondiales, aux groupes de travail sectoriels, aux projets de recherche, en accompagnant les start-up du secteur aérospatial, en investissant en continu dans la R&D pour contribuer activement à ce que l'avion (et ses successeurs) reste pour longtemps le mode de transport le plus sûr du monde.

Le continuum de sûreté tisse un maillage robuste, efficace et évolutif au sein du groupe pour bâtir une vision et une compréhension globale de la menace, qu'elle soit physique ou cyber, pour mieux gérer tous les risques associés et protéger en temps réel les actifs du groupe dans l'intérêt général de l'entreprise afin que l'avion reste encore et toujours le mode de transport le plus sûr au monde.

[1] Commercial On The Shelf
[2] Computer Emergency and Response Team
[3] Plan de Reprise d'Activité (PRA) et Plan de Continuité d'Activité (PCA)

La cybersécurité vue par les compagnies aériennes

ANAÏS BENSAÏ
Responsable Pôle Technique
Fédération Nationale de l'Aviation et de ses Métiers
&
DIANE BERTONCINI
Chargée de mission Affaires Techniques et Réglementaires
Fédération Nationale de l'Aviation et de ses Métiers

La sécurité du transport aérien est hautement réglementée. En 1944, la convention de Chicago a été signée par 54 pays afin de définir les principes de base permettant le transport aérien international et a conduit à la création de l'OACI (Organisation de l'Aviation Civile Internationale). Aujourd'hui, des annexes ont été ajoutées, et cette convention regroupe plus de 12000 normes, et recommandations adoptées par les 193 États membres de l'OACI.

Au sein de l'Union Européenne, dont en France, la sécurité aérienne se conforme aux exigences de la gestion de la sécurité aérienne élaborées par l'AESA (l'Agence Européenne de la Sécurité Aérienne). Depuis sa création en 2002, l'AESA est le pilier de la stratégie de sécurité aérienne au sein de l'Union Européenne. Sa mission est de promouvoir et d'atteindre le plus haut niveau de sécurité dans l'aviation civile, notamment au travers de l'application du Système de Gestion de la Sécurité (SGS) par les compagnies aériennes. Grâce aux procédures de gestion des risques mises en place chez les exploitants, partie intégrante du SGS, les procédures de sécurité sont donc régulièrement renforcées.

Au travers de la mise en œuvre du système de gestion, l'exploitant démontre qu'il assure une exploitation sûre de ses aéronefs et leur maintien en état de navigabilité.

Par son rôle et l'importance qu'il représente dans le monde, le secteur de l'aérien, et plus particulièrement les compagnies aériennes, est en proie à de nouveaux types de menaces : les cybermenaces.
Le nombre de cyberattaques est en constante augmentation : entre 2020 et 2021, c'est 37% de cyberattaques supplémentaires en France. De plus, en 2020, 61% des cyberattaques en France dans le secteur de l'aéronautique visaient les transporteurs aériens.
Cependant, à niveau égal d'un système de gestion de la sécurité efficace, la perception et l'évaluation des risques liés aux cybermenaces restent hétérogènes en fonction des compagnies aériennes. La majorité des métiers qui composent une compagnie aérienne sont opérationnels. La perception des cybermenaces, et la prise de conscience liée aux risques associés restent alors difficiles s'il n'y pas d'impact opérationnel.

Les différents impacts d'une cyberattaque sont donc variés et peuvent engendrer des conséquences graves pour une compagnie aérienne, indépendamment de sa taille, de son organisation et de son activité.

L'attaque la plus fréquente subie par les compagnies aériennes est la cyberattaque dite « ransomware » (rançongiciel en français). Ici, l'objectif visé par le hacker est lucratif. En fonction de la rançon demandée et de l'importance de l'attaque, l'impact financier pour l'entreprise pourrait être considérable.
Il est à noter que certaines opérations à but lucratif peuvent recourir à un mode opératoire relevant d'autres catégories comme le vol de données. Lufthansa et également British Airways en 2015, ont subi des cyberattaques visant leur programme de fidélité. L'objectif était de dérober des miles aux clients afin d'acheter des billets.

Une autre cyberattaque courante est le vol d'informations des passagers (coordonnées, papiers d'identités, voire coordonnées bancaires). Ce type d'attaques impacte l'image de la compagnie aérienne, et peut entrainer des conséquences commerciales négatives.
La compagnie aérienne British Airways a d'ailleurs été victime d'un vol des données « cartes bleues » de ses passagers pendant quinze jours en 2018.

Une cyberattaque peut également avoir un impact sur la sécurité des vols. Les chemins d'attaques sont de plus en plus nombreux, en effet, les compagnies aériennes renouvellent leur flotte avec des avions de plus en plus récents (A350, A220, Boeing 787 …), avec des connexions sol/air de plus en plus performantes.
Pour exemple, en 2014, Ruben Santamarta, chercheur espagnol, a expliqué lors d'une conférence qu'il était désormais possible d'utiliser le wifi disponible à bord des avions pour pirater les équipements de communication satellite et ainsi interférer avec les systèmes de navigation de l'aéronef.

Enfin, certaines attaques peuvent avoir pour objectif d'entraver le fonctionnement d'une compagnie aérienne. L'idée serait de s'attaquer directement au planning des vols, au planning des personnels navigants ainsi qu'aux logiciels utilisés pour la préparation des vols.
Si ces attaques peuvent avoir un impact très grave sur la sécurité des vols, elles peuvent aussi avoir des conséquences opérationnelles, engendrant des retards ou même des annulations de vols.

Un assistant aéroportuaire de dimension mondiale a d'ailleurs été touché par ce type d'attaque en 2022. L'objectif de l'attaque était lucratif, mais l'impact organisationnel a été très important. En effet, l'attaque subie par l'assistant en escale a entrainé le retard de nombreux vols.

Ces cyberattaques sont effectuées par différents profils d'attaquants, appelés « source de risques ». Ces profils d'attaquants peuvent être divisées en trois catégories :

- les organisations structurées guidées par une logique de gain et de performance disposant de moyens conséquents, voire quasi illimités (États, agences de renseignement, crime organisé) ;
- les organisations guidées par une motivation idéologique disposant de moyens plus ou moins significatifs mis en œuvre de façon relativement coordonnée (terroristes, Cyber-hacktivistes, groupements d'intérêt, sectes) ;
- les attaquants disposant de moyens plus ou moins limités mais spécialisés (individus isolés, amateurs, organisations cybercriminelles).

On retrouve aussi d'autres profils d'attaquants comme le malveillant pathologique (concurrent déloyal, client malhonnête…), et le vengeur (le vengeur est persuadé que son acte est légitime).

Le plus souvent, les compagnies aériennes sont attaquées par des profils du type cybercriminels et/ou amateurs. Des kits d'attaques sont aisément accessibles en ligne, et un amateur peut aujourd'hui facilement entraver le fonctionnement d'une compagnie sans forcément parvenir à l'objectif visé.

C'est ce qu'il s'est produit pour une compagnie long courrier française il y a quelques années, avec un ordinateur portable victime d'un phishing (hameçonnage). L'ordinateur, une fois branché au réseau, est devenu la porte d'entrée d'un rançongiciel. L'objectif du hacker était de compromettre tous les postes du réseau, afin d'arriver au chiffrement de l'intégralité des données du réseau. Ici, seulement quelques postes ont été compromis et les contre-mesures mises en place par la compagnie aérienne ont permis de contrer l'attaque et ainsi de limiter son impact. Les bonnes connaissances informatiques du hacker (amateur ou cybercriminel aux moyens limités) n'ont pas été suffisantes pour atteindre son objectif visé qui était lucratif (la rançon n'a pas eu besoin d'être payée par la compagnie aérienne).

Pour lutter face à ces menaces de plus en plus importantes, l'Union Européenne a décidé de renforcer la réglementation. En effet, l'ensemble des acteurs du transport aérien sera bientôt soumis à deux évolutions réglementaires majeures, propres au secteur aérien :

- L'amendement (UE) n°2019/1583 au règlement (UE) n°2015/1998 fixant les normes de base commune en matière de sûreté, qui vise à sécuriser les systèmes d'information contribuant à la sûreté de l'aviation civile, applicable depuis le 31 décembre 2021 ;
- Le règlement (UE) Part IS, en projet actuellement, qui vise à sécuriser les systèmes d'information contribuant à la sécurité de l'aviation civile qui devrait être adopté en décembre 2022 pour une application prévue fin 2024.

Le but de ces règlements est l'implémentation d'un « management de la cybersécurité » pouvant s'intégrer dans les quatre piliers du système de gestion de la sécurité déjà en vigueur :
- Plan : Politique en matière de cybersécurité et organisation ;
- Do : Gestion des risques (capacité à alimenter sa cartographie) ;
- Check : Assurance du maintien de la cybersécurité (audits, analyses d'événements cyber…) ;
- Act : Promouvoir la cybersécurité (formation, campagnes de communication…).

Actuellement, les compagnies aériennes doivent se mettre en conformité avec ces nouveaux règlements, qui allient opérations aériennes, et gestion de la sécurité du système d'information. L'objectif de la DSAC (Direction de la Sécurité de l'Aviation Civile) et de la FNAM, est d'accompagner les opérateurs dans leur démarche.

En complément de ces réglementations à venir, la Direction Générale de l'Aviation Civile (DGAC) a proposé de mettre en place un CERT (Computer Emergency Response Team) dédié à l'aviation. Le CERT est une structure d'alerte et d'assistance aux acteurs du transport aérien. Ses principales fonctions sont la veille et l'analyse de la menace cyber, ainsi que l'aide à la réponse aux incidents pour les organisations qui en sont membres.

A la FNAM, nous organisons un groupe de travail dédié, se réunissant régulièrement, dont l'objectif principal est de définir une cartographie des risques cyber pour les compagnies aériennes.
Cette cartographie sera alors un outil de prédictivité : elle liste les événements les plus impactant, les dangers et menaces, afin de mettre en place les barrières de protection adéquates pour réduire le risque résiduel. Une fois la cartographie établie, les compagnies aériennes pourront plus facilement se projeter dans l'organisation de leur management de la cybersécurité. L'enjeu étant d'adapter son management cyber à la taille, aux opérations, et à la complexité de l'entreprise, tout en maîtrisant ses dépenses.

Ainsi, certaines compagnies aériennes se réorganisent, en créant un service dédié souvent nommé « Sécurité des Systèmes d'Information (SSI)», dont le responsable devrait être rattaché directement au dirigeant responsable.

Par ailleurs, certaines compagnies aériennes ont déjà mis en place, en amont des nouveaux règlements, un certain nombre d'actions et de bonnes pratiques :
- Sensibilisation de la direction aux risques cyber ;
- Mise en place d'une veille cyber mensuelle (CERT Eurocontrol, SITA, CLUSIF….) ;
- Participation à des événements cyber (salon, symposium…) ;
- Mise en place d'outils de surveillance et d'alerte du système d'information ;
- Audits ;
- Cartographie des risques cyber concentrée sur l'avionique des aéronefs (en particulier l'IFE), et le site web de la compagnie.

Aujourd'hui, il faut continuer de promouvoir la cybersécurité en France, chez des transporteurs aériens.

La promotion de la cybersécurité passe par divers vecteurs :
- Une formation et/ou sensibilisation à la cybersécurité, adaptée à son organisation, et aux parties prenantes. Celle-ci peut être récurrente ;
- La diffusion d'une veille d'événements cyber ;
- La réalisation d'un plan de gestion de crise cyber : l'idée est de créer des procédures visant à limiter les impacts d'une cyberattaque en définissant des rôles clés aux employés concernés, avec des tâches à effectuer. Ces exercices de gestion de crise cyber devraient être organisés régulièrement ;
- Des campagnes de test, comme des campagnes de phishing.

Malgré la conjoncture actuelle du secteur du transport aérien, notamment à cause de la crise du covid, et la guerre Russo-Ukrainienne, il faut que les compagnies aériennes réussissent à préparer leur avenir. Elles doivent rester performantes, assurer la sécurité de leurs appareils et de leurs passagers, tout en continuant d'investir dans deux domaines clés sur le long-terme : le développement durable et la cybersécurité.

La prise de conscience des transporteurs aériens est donc longue face à l'émergence des cybermenaces. En effet, les fonctions opérationnelles sont pour le moment très peu touchées et les cyberattaques ont principalement engendré des impacts financiers mineurs pour les compagnies aériennes.
Les nouveaux règlements, notamment la Part-IS qui entrera en vigueur en 2024, commencent à obliger les dirigeants responsables à se projeter dans l'avenir et à réfléchir à leur stratégie pour anticiper les opportunités des différents attaquants.

La cybersécurité en compagnie aérienne doit alors se traiter globalement, tout son périmètre opérationnel doit être pris en compte dans la cartographie des risques, en collaborant avec les autres acteurs du transport aérien (aéroports, DGAC, constructeurs, sous-traitants …).
L'objectif reste bien d'organiser et d'établir un management de la cybersécurité efficace.

« S'il vous plaît… fabrique-moi un avion »

STÉPHANIE BUSCAYRET
CISO
Latécoère

Demandez aux passagers en attente à l'aéroport[1] de lister des entreprises de l'aéronautique : il y a fort à parier qu'Airbus et Boeing soient largement cités mais que la liste s'éteigne assez vite… Si les grands avionneurs sont des « marques » mondialement connues, la majorité des acteurs nécessaires à la construction d'un avion est inconnue du grand public ! Et pourtant, il faut plus de 1000 entreprises pour faire naître un avion, qu'il soit commercial ou militaire, long ou moyen-courrier…

Il fut un temps où les pionniers de l'aéronautique pouvaient fabriquer un avion de A à Z et même opérer le service de transport associé mais ce temps est depuis longtemps révolu. Les avions « modernes » sont structurellement plus complexes que ne l'étaient leurs glorieux ancêtres, beaucoup plus sûrs, toujours mieux équipés et de plus en plus connectés !

Dans la recherche constante d'innovation pour rendre les avions plus performants et mieux adaptés aux enjeux économiques et écologiques actuels, les avionneurs s'appuient sur le meilleur des compétences disponibles pour chacune des composantes (moteurs, aérostructure, câblage, équipements…) et pour chaque savoir-faire (design, architecture, industrialisation, montage, maintenance…). Cet optimum ne peut exister au sein d'une seule entité, si mondiale et avancée soit-elle : les avionneurs s'appuient sur leur Chaîne d'approvisionnement (*Supply Chain*) pour compléter leurs propres compétences et constituer un écosystème ad hoc.

La stratégie de constitution de la *SupplyChain* est variable selon les avionneurs : Boeing a longtemps privilégié la fabrication « interne » mais s'ouvre à chaque programme un peu plus à la sous-traitance (même à des

acteurs européens !), Airbus a une tradition de *SupplyChain* élargie (en combinant déjà 4 ADN nationaux à l'origine), Dassault différencie les fournisseurs par segment (tout le monde ne peut pas prétendre à un programme militaire), Embraer et Bombardier ajustent les besoins selon le type de programme. Cette réalité combinatoire existe aussi pour les autres productions du secteur aéronautique et spatial : hélicoptères, satellites, drones…

La *SupplyChain* réunit des maillons de tous types (fournisseurs de services, industriels, bureaux d'étude…), de toutes tailles (du géant mondial à la TPE) et de toutes nationalités (pour les avions civils au moins). Pour concevoir et construire les éléments qui composent un avion, les entreprises partagent toujours plus d'informations, toujours plus vite (comprendre : en temps réel) et avec toujours plus d'interlocuteurs à travers le monde. Le système nerveux de cet organisme est numérique : il est partout et nulle part ! C'est ce qui le rend puissant, résilient et paradoxalement vulnérable.

Protéger, c'est l'affaire de tous !

Protéger l'information dans un écosystème de cette envergure est impossible sans responsabiliser chaque acteur, chaque système et chaque organisation. Le mantra du niveau de sécurité d'une chaîne comme n'étant que celui de son maillon le plus faible trouve un écho très concret dans l'organisation en entreprise étendue et dans la *SupplyChain*.

Cette entreprise collective de protection du bien commun s'exécute dans un environnement toujours plus hostile : la menace grandit, se sophistique et se déploie elle-aussi sans contrainte de frontières. Les chiffres le montrent, les autorités alertent, les témoignages se multiplient, les attaquants sortent de l'ombre pour faire publiquement leur « promotion » et recrutent au grand jour ! La tendance s'accélère toujours plus chaque année, c'est un fait.

Les grands donneurs d'ordre ont bien compris l'accroissement de la menace cyber envers leurs outils numériques et ont considérablement renforcé leur sécurité, rendant plus difficiles et plus coûteuses les attaques

pour les cybercriminels. Ces derniers ont naturellement trouvé un chemin plus simple pour atteindre leur cible : les fournisseurs, connectés mais moins armés et moins préparés à résister à ce type de menaces.

Pour ceux qui conçoivent et réalisent des logiciels embarqués dans les avions, qu'ils soient destinés aux commandes de vol ou au système multimédia pour les passagers, produire un système « non faillible » est une évidence : étant nativement numérique, leur produit ne doit pas ajouter une porte d'entrée dans l'avion dont on ne pourrait pas assurer la robustesse face aux attaques cyber ! C'est une question de responsabilité et de confiance. Pour ceux qui fabriquent des boulons ou de la peinture, l'enjeu de la cybersécurité est peut-être un peu moins évident, et pourtant…

L'enjeu de la cybersécurité, on s'en parle ?

Les assureurs et les cabinets de tendance ont beau afficher le risque cyber dans le top 3 des risques d'entreprise (après la pandémie indétrônable sur les derniers mois, l'Ukraine a remis le risque géopolitique en embuscade), sur le terrain, les entrepreneurs le voient encore bien loin de leurs priorités. Ce n'est pas les blâmer que le dire mais la hausse constante des coûts de l'énergie et des matières premières, l'incertitude économique liée à la pandémie, les difficultés de recrutement s'imposent loin devant les risques cyber dans l'agenda des patrons de PME et d'ETI, où qu'ils soient dans le monde.

Concrètement, comment expliquer à un patron de PME industrielle que sécuriser ses systèmes d'information est un enjeu pour sa société ? Comment le convaincre que le Numérique porte autant de perspectives de croissance que de risques ? Ce même entrepreneur qui vient d'investir plusieurs dizaines ou centaines de milliers d'Euros dans une machine industrielle dernier-cri (forcément connectée mais pas forcément sécurisée), financée par le plan de relance et qui doit lui permettre d'améliorer sa compétitivité pour gagner de nouveaux marchés, cruciaux en cette période incertaine…

On ne manque pas de témoignages de victimes de rançongiciel : collectivités territoriales, hôpitaux et mairies qui sont revenues au fax et aux procédures papier - mais qui ne risquent pas la faillite, elles.

Ce n'est pas un hasard si les autorités ont recruté des auteurs de science-fiction pour imaginer l'avenir cyber : pour comprendre l'impact des menaces cyber sur nos sociétés, nos démocraties et nos vies quotidiennes, rien de mieux que les histoires. Celles dans lesquelles on peut se projeter, s'interroger et réaliser que ce qui était de la fiction il y a seulement 5 ans est devenu la réalité.

Le méchant hacker qui prend le contrôle du système avionique depuis son salon pour prendre en otage un avion commercial et faire du chantage aux autorités, ça fait un bon scenario pour un film catastrophe… seulement pour un blockbuster hollywoodien.

Proposer un scénario « que se passerait-il si… » permet d'engager une réflexion sur les risques en commençant par les impacts potentiels, à condition qu'il s'inscrive dans la réalité de l'entreprise.

Commençons le synopsis :

Que se passerait-il si le projet « usine du futur » lancé pour améliorer la productivité de l'entreprise est déployé sans analyse du risque cyber ?

Que des connexions externes avec le fabriquant sont maintenues ouvertes pour permettre la maintenance prédictive de la machine 4.0 ?

Qu'un attaquant se connecte sur le système d'information par cette liaison exposée peu/mal/pas sécurisée ?

Qu'il parvient à entrer dans le système qui contrôle ladite machine ?

Qu'il modifie les programmes et génère une production non conforme qui serait bonne pour la poubelle (à condition que le contrôle qualité soit efficace et réactif) ?

Qu'il sabote purement et simplement la chaîne de production en modifiant quelques paramètres de contrôle de température ou de rotation des instruments (un classique des attaques sur les systèmes industriels) ?

Que les paramètres de l'imprimante 3D « faussés » par l'attaquant conduisent à une faiblesse structurelle de la pièce fabriquée, à l'origine d'une défaillance critique une fois l'avion en vol ?

Qu'évidemment l'assurance (s'il est assez chanceux pour en avoir une) refuse de couvrir le sinistre puisqu'une négligence de l'assuré est à l'origine des dégâts ?

Qu'à l'issue du sinistre, la ligne de production est arrêtée, les personnels en chômage technique ?

Que ses clients, mécontents de ne pas recevoir leurs commandes dans les délais fixés appliquent les pénalités financières contractuelles qui entameront le peu de trésorerie encore disponible ?

Qu'ils dégradent sa note de confiance, privilégiant la concurrence pour le prochain appel d'offre ?

Que la perte de marchés l'oblige à licencier du personnel ?

Que dans le pire des cas, la situation amène l'entreprise jusqu'à la cessation d'activité, voire la faillite personnelle du dirigeant ?

Pure fiction ? Malheureusement non.

Certes, ce scenario est un peu plus sophistiqué que le simple ransomware (si courant qu'il truste la 1ère place du tableau des sinistres cyber) qui paralyse une production juste parce qu'une personne clique sur le mauvais lien, depuis un PC pas assez bien protégé, connecté à des systèmes pas suffisamment « étanches ». Mais rappelons-nous que la majorité des PME n'a pas d'expert en sécurité informatique ! Si déjà elle a un vrai informaticien…

Il existe autant de scenarii à explorer que de types d'attaques et de cibles :

- L'introduction d'une porte-dérobée à la faveur d'une mise à jour système « non vérifiée » est plus adaptée pour interroger un concepteur de logiciel embarqué ou une start-up qui développe des API,
- Le cyber-espionnage par vol de données hébergées dans le Cloud au détour d'un S3 mal configuré sera plus pertinent pour un bureau d'étude ou un institut de recherche engagé dans la décarbonation de l'avion,
- La mise en défaut des systèmes de production (par déni de services, rançongiciel ou autre joyeuseté) qui bloque la capacité à livrer dans les délais trouvera un écho plus attentif chez un industriel fabriquant des pièces mécaniques,
- La découverte d'un malware dormant qui déclenche une fuite de données programmée juste après l'acquisition d'une société parlera plutôt à des spécialistes des Fusions/acquisitions, en ces temps de consolidation à tout va pour atteindre des tailles critiques…

Pourtant il y 2 hics à cette approche par les scenarii…

Le premier, c'est que les experts qui ont connaissance de ces évènements « de la vraie vie » œuvrent dans les rangs des très grands groupes ou les services de renseignements économiques, avec une probabilité quasi nulle de rencontrer les acteurs économiques de taille modeste aux six coins de l'hexagone… Les autorités, notamment la DGSI, propose des exemples concrets de menaces (pas uniquement cyber) visant les entreprises à travers les « flash ingérence »[2] : combien d'entrepreneurs le savent et les lisent ? Sans doute très peu. Pour les services bleu-blanc-rouge, ce n'est pas faute de sortir de leurs bureaux régulièrement pour évangéliser les entrepreneurs mais plutôt d'avoir l'audience espérée. Si vous avez déjà assisté à des séances de sensibilisation au risque cyber, vous y trouverez les acteurs déjà sensibilisés qui viennent pour une piqûre de rappel mais pas ceux qui n'ont aucune idée de ce dont il s'agit.

Convaincre tous les acteurs économiques de la réalité du risque cyber est une cible que nous n'avons pas encore collectivement réussie à atteindre.

Un espoir est né lors de la grande messe de l'aéronautique du Bourget en 2019 : l'équipementier ASCO est victime d'une cyberattaque qui paralyse

une partie de ses usines pour plusieurs semaines ! Tout ce que l'aéronautique compte d'acteurs internationaux est mis au courant, les téléphones sonnent (« mon Comex me demande d'expliquer ce qui se passe chez ASCO ») et on se prend à espérer qu'enfin la menace cyber va être comprise et intégrée dans les tableaux de Risk Management des acteurs de la filière, suite à cette démonstration par l'exemple. Las, effet « salon » sans doute, tout est bien vite oublié pour célébrer les visites de VIP sur les stands et les signatures de contrats…On apprendra plus tard que la société belge est en cours de M&A avec Spirit Aerosytems qui en a profité pour revoir le montant de l'acquisition sensiblement à la baisse[3] et qu'aucune des usines Asco servant Boeing n'a été touchée par le rançongiciel…

Le second hic de cette approche par les scenarii de risque, c'est qu'elle oblige l'entrepreneur à formuler des hypothèses qui font peur ! Comme le FUD[4], même si ici l'influence vise à mettre en lumière un risque qui peut mettre à mal la viabilité d'une entreprise (admettez que ça part d'une bonne intention !). Le concept de FUD, théorisé dans les années 70 en informatique (un hasard ?) est encore utilisé par certains vendeurs de solutions, pour convaincre leurs clients novices qu'empiler des « solutions techniques de cybersécurité » les rend inattaquables (sic).

Pourtant, c'est bien en déroulant le « WIF - What If » que le chef d'entreprise peut se projeter dans un « possible » qu'il n'a jamais rencontré, sans doute jamais envisagé, encore moins préparé. Envisager le pire est un exercice de mise à nu, qui fait surgir des craintes et révèle des vulnérabilités. Pour certains, l'exercice est intellectuellement insupportable ; le déni devient alors une forme de protection, qui bloque toute tentative d'un tiers de rassurer, d'accompagner vers la prise conscience nécessaire pour passer à l'étape suivante (NDLR : situation vécue !).

Pour éviter que ce premier pas ne soit traumatique, il faut un peu de courage et un environnement de confiance : savoir que révéler des vulnérabilités ne sera pas exploité ni divulgué mais qu'au contraire, permettra de trouver une écoute attentive.

C'est là que l'écosystème de la SupplyChain doit jouer son rôle : parce

que d'autres avant vous ont fait cet exercice, dans le même environnement, face aux mêmes risques et aux mêmes menaces, ils ont su tirer profit de l'expérience pour construire une démarche d'amélioration de la protection de leur activité, de leurs intérêts économiques et de leur réputation. De ceux-là, on peut apprendre beaucoup et bien plus vite que tout seul ! C'est le rôle d'une communauté de pairs.

« Comment font les autres ? »

C'est une question souvent posée par les directions d'entreprise au RSSI (s'il y en a un/une), au DSI à défaut (s'il y en a un/une !) ou à « l'expert informatique » (qu'il soit interne ou externe, celui qu'on appelle quand son PC est planté). Pour l'expert, il est contre-productif de citer l'organisation et les moyens de son client (souvent plus gros, mieux armé et plus mature que vous) pour établir une cible… irréaliste pour la plupart des PME de se comparer ne serait-ce qu'à une ETI, encore moins à un grand groupe…

En revanche, appeler son confrère dans une société du secteur, de taille équivalente, permet souvent d'obtenir un début de réponse à la question. Pouvoir en consulter plusieurs, échanger sur leurs problématiques du moment et sur les réponses qu'ils ont trouvé, dans un cadre de confidentialité et de bienveillance garanties permet d'établir un panel des possibles, à portée de budget et réalisables avec des compétences équivalentes.

Disposer d'un référentiel commun de maturité cybersécurité, adapté au secteur, permet de répondre à la seconde question « ils en sont où les autres ? » qui arrive souvent en suivant…

Être accompagné dans la structuration des possibles, par des acteurs de confiance, facilite le passage de la réflexion théorique à la pratique. C'est le premier pas dans un monde qu'on imagine complexe et hautement technique alors qu'il est d'abord bâti sur :

- Des pratiques organisationnelles financièrement peu coûteuses,
- L'enrôlement des collaborateurs dans une démarche collective de protection des intérêts communs, fédératrice à plusieurs niveaux,

- L'adoption de quelques outils simples qui peuvent amener, contrairement à l'idée reçue, des gains de productivité mesurables.

La structuration « administrative » de la cybersécurité de l'entreprise - construite à base de politiques, chartes et autres procédures- est également plus simple quand on peut partager des modèles documentaires éprouvés, des guides et méthodes 'labellisés ' au sein de la communauté.

Les opérations de communication et de sensibilisation sont aussi grandement facilitées par la mise en commun de ressources déjà élaborées par ceux qui nous ont précédés dans la démarche et qui partagent leurs outils !

Pour les étapes suivantes, le choix de technologies et d'outils de cybersécurité peut apparaître complexe tant la panoplie des offres marketées à grand renfort d'acronymes barbares et de concepts sibyllins laisserait étourdi plus d'un béotien. Là encore, le conseil de ses pairs et leurs retours d'expérience sont précieux tant pour le choix des solutions que pour éviter les écueils d'implémentation.

Si en plus d'une meilleure protection de son patrimoine informationnel et de sa résilience numérique, l'entreprise y trouve la reconnaissance de ses efforts, de la part de ses clients et de ses pairs, la cybersécurité devient un avantage différenciant par rapport à des concurrents qui n'ont pas démontré leur maturité cyber.

Cette reconnaissance bâtit la confiance, celle qui conditionne le partage de l'information pour un programme de partenariat, un contrat commercial ou un rapprochement économique…

Cette communauté dédiée à la cybersécurité du secteur aéronautique existe et ce sont maintenant plus de 200 acteurs de la *SupplyChain* qui ont choisi de la rejoindre. Voilà 5 ans que quelques croyants de la 1ère heure ont décidé de constituer, autour de BoostAeroSpace, sous l'égide des 4 grands donneurs d'ordre aéronautique européens, le programme AirCyber[5] pour lancer un grand élan de montée en maturité Cybersécurité du secteur tout entier.

« Il s'agit avant tout d'un programme de soutien mutuel et d'évaluation de la maturité initié par les équipementiers du secteur. Ils partagent leurs matériels et leur expertise afin de permettre à leurs fournisseurs d'accéder au même niveau de sécurité que le leur. L'objectif final est de standardiser et d'harmoniser le niveau de cyber-protection de l'industrie mondiale. »

Ils sont encore nombreux ceux qu'il nous faut enrôler dans la bataille contre les menaces cyber et pour la résilience de notre industrie…et tous y ont une place ! Plus la SupplyChain sera impliquée dans la démarche, plus large sera la base de partage et plus grands seront les bénéfices de ce programme, tant pour les fournisseurs que pour les clients, surtout pour ceux qui jouent les deux rôles à la fois.

Notez que l'on peut espérer aussi, à terme, en partageant un référentiel commun, porté par un Tiers de confiance, ne plus avoir à remplir de multiples évaluations de maturité cyber au long de l'année, au fil des contrats, des appels d'offres et des partenariats (chacune spécifique dans son format mais semblable aux autres dans l'objectif) : on y gagnera en productivité !

Protéger nos activités d'une autre menace ?

Et parce que l'industrie aéronautique n'est pas une exclusivité européenne, le chemin est encore long pour nos chercheurs, nos industriels, nos bureaux d'études, nos commerciaux qui doivent répondre aux exigences des clients à travers le monde. Des clients qui n'ont pas tous les mêmes référentiels pour appréhender le risque cyber et délivrer un label de confiance. Les donneurs d'ordre étrangers, américains en particulier, évaluent le domaine avec des bases NIST/ CMMC (que le marché soit dépendant du *Department of Defense* ou pas).

Les évaluations demandées aux sociétés européennes pour candidater sur des marchés étrangers ne sont pas sans danger pour la confidentialité de nos pratiques, la nature de nos outils de sécurité et les vulnérabilités qui pourraient être déduites des non conformités. Les tiers chargés d'établir cette conformité sont presque tous de nationalité américaine, ou soumis à sa réglementation…

Nos industriels, en particulier les industries de défense, doivent-ils s'exposer à des risques d'espionnage et de déstabilisation en échange du droit de candidater à un marché ? Si les acteurs aéronautiques américains collaborent étroitement avec leurs homologues européens au sujet de la menace globale, dans le cadre de l'A-ISAC[6] notamment, les acteurs étrangers ne sont pas pour autant exemptés de tout soupçon d'intérêt pour nos savoir-faire, dans le secteur de la défense, sur des technologies souveraines existantes et à venir. L'évolution de la loi de blocage par le décret de février 2022[7] va dans ce sens[8] mais combien de dirigeants d'entreprise en connaissent le contenu ?

Pourquoi s'interdire d'aller jusqu'au bout de l'ambition de protection de nos intérêts économiques et d'imaginer une normalisation volontaire des pratiques de cybersécurité spécifiques à l'aéronautique ? Une norme ISO 27AERO, de portée mondiale, auditable depuis tous les pays, reconnue par tous les organismes publics et privés qui œuvrent à la protection des intérêts de la filière… une norme pivot reconnue en équivalence aux réglementations locales, à l'instar de l'OEA[9] qui permet d'obtenir une équivalence du CT-PAT. Plus besoin d'exposer nos savoir-faire mais au contraire les valoriser et gagner en influence. S'il y a une centaine de normes en projet sur la thématique cybersécurité[10] , pas encore de proposition pour l'aéronautique…

A vous tous qui êtes impliqués, concernés, engagés et motivés : qui est partant ?

[1] (sauf celui de Toulouse-Blagnac évidement…)
[2] DGSI-flash-ingerence
[3] De 650 millions à 420 millions de dollars mais Spirit Aerosystems, en difficulté suite aux crises du 737MAX et du Covid-19, se retirera totalement du deal.
[4] FUD -Wikipedia
[5] AirCyber - BoostAeroSpace
[6] Aviation ISAC
[7] Loi « de blocage » - entreprises.gouv.fr
[8] Décret n° 2022-207
[9] l'autorisation OEA
[10] Normes Cybersécurité (afnor.org)

Du Conseil pour la Cybersécurité du Transport Aérien au CERT Aviation : développer et renforcer la résilience du transport aérien face à la cybermenace

DAMIEN CAZÉ
Directeur général
Direction Générale de l'Aviation Civile

L'histoire de l'aéronautique dans notre pays est une histoire ancienne, riche. Une histoire de passion et d'excellence qui font de la France le deuxième pays aéronautique au monde. Le secteur aérien français compte de nombreux leaders mondiaux dans l'industrie, la formation et le transport aérien. Il s'appuie sur un maillage aéroportuaire unique en Europe et compte une importante population de pilotes privés regroupés dans de nombreux aéroclubs. Ce secteur, fragilisé par deux années de pandémie est essentiel à l'économie nationale et contribue fortement à l'attractivité économique et touristique de la France. Il doit cependant poursuivre sa mue pour relever les défis de la transition écologique, des nouvelles générations d'avions bas carbone, de la mobilité aérienne urbaine et ses nouveaux aéronefs électriques à décollage et atterrissage verticaux (VTOL), des drones, dans le maintien d'un très haut niveau de sécurité et de sûreté.

Le secteur aérien s'est engagé dans une transformation numérique sans précédent afin d'accroitre ses performances, sa compétitivité et sa sûreté. Pour être interopérables dans le dispositif aérien actuel, ces futurs systèmes devront être en capacité à la fois d'exploiter les standards techniques existants (dont certains nous viennent de l'après-guerre) mais aussi de tirer profit des technologies du 21ème siècle avec ce qu'elles offrent de performance, de flexibilité et de robustesse. Or si cette numérisation offre de nouvelles opportunités, elle crée également de nouvelles vulnérabilités pouvant être exploitées par des acteurs malveillants. Les aéronefs pilotés

ou télépilotés ne pourront plus envisager d'être isolés le temps du vol. Ils devront être connectés, autonomes et cyberrésilients[1]. Cette résilience devra être appréhendée de façon globale sous les prismes technique, organisationnel et humain.

Une menace réelle, concrète et protéiforme

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) confirme dans son Panorama de la menace informatique 2021[2] une hausse continue du niveau des attaques informatiques en volume et en sophistication. Cette menace revêt de multiples visages derrière lesquels se cachent bien souvent des acteurs de natures très différentes (cybercriminels, acteurs étatiques et *hacktivistes*[3]) aux motivations diverses (gains lucratifs, espionnage et déstabilisation).

Outre le contexte géopolitique actuel dans l'est de l'Europe, l'actualité récente nous confirme que non seulement le transport aérien n'échappe pas à cette tendance de fond mais qu'il peut même représenter une cible stratégique au regard des enjeux politiques, économiques, environnementaux et sociétaux qu'il porte. En atteste la cartographie[4] des incidents de cyber sécurité qu'élabore et maintient le *European Air Traffic Management CERT d'EurocontroI* (EATM-CERT) : toutes les typologies d'acteurs sont touchées (aéroports, compagnies aériennes, avionneurs, équipementiers, prestataires de services de navigation aérienne, organismes de formation, sociétés de maintenance, autorités de surveillances) et ce à l'échelle mondiale.

Le Conseil pour la Cybersécurité du Transport Aérien : Plier mais ne pas rompre

Les grands acteurs du transport aérien français et les pouvoirs publics ont pris la mesure de ces enjeux. En avril 2018 sous l'impulsion de la ministre déléguée aux transports, le gouvernement a installé le Conseil pour la Cybersécurité du Transport Aérien (CCTA). Présidé par le directeur général de l'Aviation Civile avec le soutien de ses trois vice-présidents (le directeur général de l'ANSSI pour le secteur de l'Etat, la direction d'Airbus pour le secteur Industriels et la direction du Groupe ADP pour le secteur

Opérateurs), il vise à appréhender de façon globale le cyber-risque français.

Le CCTA s'appuie sur 14 membres répartis en 3 collèges :
Collège Opérateurs
• ADP
• Air France
• La Direction des Services de la Navigation Aérienne (DSNA)
• La Fédération Nationale de l'Aviation et des Métiers (FNAM)
• L'Union des Aéroports Français (UAF)

Collège Industrie
• Airbus
• Dassault Aviation,
• Safran
• Thales
• Le Groupement des Industries Françaises Aéronautiques et Spatiales (GIFAS)

Collège Etat
• L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
• Le ministère des Armées
• Le ministère de l'Intérieur
• Le ministère des Transports (DGAC)

Cette instance est pour les acteurs de l'aviation civile un lieu de référence pour encadrer, structurer et coordonner les initiatives en matière de cybersécurité du transport aérien. Deux groupes de travail œuvrent au sein du CCTA :

• Le premier comité technique s'attache à déployer une stratégie d'influence auprès des instances internationales en particulier en coordonnant des positions nationales relatives à la réglementation européenne et aux projets d'échelle mondiale portés par l'OACI (Organisation de l'Aviation Civile Internationale). Il est également le forum de discussion pour optimiser la mise en œuvre de la réglementation cyber et accompagner l'évolution de l'aviation civile dans ce domaine.

- Le second comité technique travaille à l'identification et à l'évaluation des menaces, de leurs impacts potentiels et des cyberrisques qui pèsent sur le transport aérien.

Ces deux axes de travail visent essentiellement à cartographier l'écosystème du transport aérien et à orienter les travaux réglementaires ou leurs déclinaisons, en cohérence avec les spécificités de la filière. S'appuyant notamment sur des recommandations[5] formulées en 2019 par le groupe de travail Cybersécurité de l'Académie de l'air et de l'espace (AAE), les acteurs du CCTA ont souhaité aller plus loin en cherchant à développer la résilience opérationnelle du secteur. Dans ce contexte, l'idée d'un *Computer Emergency Response Team* (CERT) dédié au monde de l'aviation a germé.

Le CERT Aviation France : Souveraineté et confiance

Un CERT est un dispositif opérationnel reposant sur une équipe de professionnels de la sécurité des systèmes d'information et dont les missions consistent à anticiper et répondre aux incidents survenant sur le périmètre qui lui a été confié. Le futur CERT Aviation sera ainsi un CERT sectoriel au bénéfice de l'ensemble des acteurs de l'écosystème du transport aérien français. Des organisations les plus matures aux acteurs les moins sensibilisés et potentiellement les plus fragiles. A l'instar de la *safety* la robustesse d'une chaîne de cybersécurité se mesure à la solidité de ses maillons les plus faibles. Il est donc essentiel d'associer progressivement l'ensemble des acteurs dans cette dynamique.

Un CERT est avant un outil structuré autour de 3 axes essentiels :
- L'anticipation
- Le partage
- Le soutien

Anticiper

Identifier les menaces émergeantes, qualifier et évaluer leurs impacts, sont évidemment des enjeux cruciaux dans notre capacité à anticiper les attaques qui cibleront le transport aérien dans les années à venir. C'est la

mission première d'un CERT que d'assurer cette veille et cette analyse préalable des menaces. Le CERT Aviation France pourra en cela s'appuyer sur les travaux du CCTA, notamment ceux du comité technique « menaces et impacts » pour identifier les points névralgiques de l'écosystème et y focaliser son attention. De la capacité du CERT Aviation à connaître et à prendre en compte les spécificités de la filière aéronautique, dépendra son efficience dans ses missions de veille.

Partager

Un CERT ne travaille pas seul. Il a vocation à tisser des liens avec ses pairs et à s'insérer dans une communauté. Le CERT Aviation France a pour objectif de développer ses relations avec les autres CERTs nationaux (régionaux, sectoriels, industriels, étatiques) mais également avec ses homologues internationaux (Aviation-ISAC[6], EATM-CERT[7], FIRST[8]). Au niveau français l'ambition pour le CERT Aviation est d'intégrer courant 2023 le réseau *InterCERT France* communauté de référence qui regroupe et fédère les CERTs majeurs au niveau national.
Au-delà de ses liens externes, l'efficience d'un CERT se mesure également à la qualité et à la pertinence des informations qu'il diffuse à ses bénéficiaires. Elles doivent être ciblées, pertinentes, compréhensibles et exploitables. Or pour percevoir les tendances, les signaux faibles et orienter ses capacités d'analyse vers les bons sujets, le CERT Aviation aura besoin d'être alimenté et notifié par les acteurs du transport aérien. Cet objectif nécessitera de la pédagogie et de la confiance.

De la pédagogie, car il faudra savoir expliquer aux différents cercles de bénéficiaires, les enjeux de cette démarche. Savoir mettre en lumière les interdépendances au sein de l'écosystème. Faire comprendre les chaînes de propagations et les impacts directs et indirects des cyberattaques. Si les grands acteurs de la communauté aérienne française ont déjà fait l'objet d'attaques avérées, il reste certainement à renforcer le partage d'expérience et l'acculturation de la *supply chain* notamment. Le transport aérien est riche d'une multitude d'acteurs qu'il faudra savoir accompagner dans cette prise de conscience et dans cette montée en maturité progressive.

De la confiance enfin, car sans elle il n'y aura pas de partage. Cette confiance ne se décrètera pas elle se construira au fur et à mesure et le CERT Aviation devra en être le garant.

Pour que puissent être librement remontées les informations, il faudra savoir démontrer d'un point de vue technique et organisationnel que les questions de souveraineté et de confidentialité sont assurées. Cette confiance s'est installée entre les organisations membres du CCTA. Elle est notamment à l'œuvre aujourd'hui dans la coordination et le partage d'information qu'anime la DGAC en lien avec la crise Russo-Ukrainienne. Il faut continuer à renforcer cette confiance et il faudra l'étendre progressivement aux différents cercles de bénéficiaires, selon les enjeux et selon le besoin d'en connaître. Les principes fondamentaux de la *culture juste* « 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[9] » devront utilement être étendus aux questions de cybersécurité.

Soutenir

Soutenir enfin, car nous le savons, au-delà de notre capacité d'anticipation et de notre niveau de préparation, il nous faudra savoir gérer des crises locales, transverses ou sectorielles. Les attaques brutales subies par les services hospitaliers ces 12 derniers mois en pleine pandémie de COVID 19, nous rappellent la nécessité de structurer notre secteur d'activité afin d'anticiper ces attaques et de nous préparer à gérer collectivement des crises touchant un ou plusieurs acteurs de l'écosystème.

La DGAC en lien avec les services de l'Etat et les membres du CCTA, anime et structure une réflexion pour un dispositif de gestion de crise cyber sectorielle. Si les acteurs du transport aérien ont une habitude certaine de la gestion de crise en général, les crises d'origine cyber par leurs spécificités et l'intention manifestement malveillante qui les animent, nécessitent une organisation adaptée. Le CERT Aviation aura toute sa place dans ce dispositif sectoriel afin d'alimenter les cellules de crise

stratégiques et décisionnelles. S'appuyant sur la connaissance qu'il aura acquise des différents écosystèmes et via les liens qu'il aura tissés avec les bénéficiaires, le CERT Aviation sera le point de synthèse, d'analyse et de pivot de l'information technique. A ce titre il pourra dans les crises les plus limitées comme dans les crises globales être un relai efficace entre les différentes parties prenantes lors des phases de qualification, d'investigation et de remédiation des incidents de cybersécurité.
Pour que cette ambition puisse se concrétiser, le dispositif de gestion de crise sectorielle porté par la DGAC, prévoit la réalisation d'exercices de crise. Ils permettront de consolider régulièrement le dispositif lui-même et la contribution que pourra avoir le CERT Aviation au fur et à mesure de sa montée en puissance dans les mois et les années à venir.

Le CERT Aviation est un prolongement naturel de cet esprit qui anime depuis toujours le monde aéronautique : collaborer, partager, analyser les événements et en tirer tous les enseignements afin d'améliorer sans cesse la sécurité et la sûreté des vols. La très forte culture sécurité qui imprègne depuis l'origine la communauté du transport aérien sera un atout indéniable dans mise en œuvre de ce projet. Le CERT Aviation porte l'ambition de venir enrichir et renforcer les dispositifs existants dans le transport aérien, en liens avec ses pairs aux niveaux national et international.

Comme le rappelait Guillaume POUPARD le directeur général de l'ANSSI « *étant donné ceux contre qui nous luttons, la disproportion des moyens rend essentiel le bon emploi de nos ressources. […] L'inefficacité n'est pas concevable. Cette approche vaut en interne comme avec tous nos partenaires publics et privés au niveau national et à l'échelle européenne.* »

Le CERT Aviation s'inscrit pleinement dans cette démarche d'efficience et de complémentarité. Ce sera, sous l'impulsion de la DGAC, un outil coconstruit par le transport aérien pour le transport aérien.

[1] https://academieairespace.com/publications/les-dossiers/dossier-n-45-cybermenaces-visantle-transport-aerien/
[2] https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf
[3] Activistes exploitant le champ cyber pour défendre leur idéologie
[4] EATM-CERT Aviation Cyber Events Map - https://www.eurocontrol.int/cybersecurity
[5] https://academieairespace.com/publications/les-dossiers/dossier-n-45-cybermenaces-visantle-transport-aerien/
[6] ISAC Information Sharing Analysis Centers - Centres de partage et d'analyse d'informations relatives aux cyber menaces
[7] European Air Traffic Management CERT - CERT d'Eurocontrol
[8] FIRST - Forum of Incident Response and Security Teams - Association de CERTs internationaux
[9] Définition de la culture juste selon le règlement européen (UE) N° 376/2014 concernant les comptes-rendus, l'analyse et le suivi d'événements dans l'aviation civile

Cybersécurité et aviation : quels enjeux pour l'innovation ?

NATHALIE FEYT
Chief Information and Product Security
Thales

Le transport aérien est le moyen le plus sûr de se déplacer et profite des spécificités technologiques de sûreté de fonctionnement du domaine aéronautique pour être, jusqu'à présent à l'abri des impacts d'une cyber-attaques.

Eurocontrol dans son rapport de Juillet 2021 « Think Paper #12 EATM CERT Services » (www.eurocontrol.int) mentionne une hausse des attaques reportées dans le secteur de 530% entre 2019 et 2020, essentiellement sur des vols de données. Cette tendance s'est malheureusement confirmée dans la période COVID. Cependant, l'attaque Ransomware de Garmin en Juillet 2020 (reference www.bbc.com/news/technology-53553576), qui a empêché la livraison des bases de données de navigation à plusieurs compagnies de business jets, les clouant au sol, est un des premier signes d'évolution de paradigme de la menace sur notre secteur. Les impacts étaient initialement sur des données personnelles des passagers éventuellement sur des systèmes de billetterie ou systèmes d'information d'entreprise. Le cas les bases de données de navigation de Garmin illustre l'évolution vers des impacts beaucoup plus opérationnels.

Comment faire en sorte qu'à l'avenir, le transport aérien soit, au moins aussi sûr et disponible que de nos jours ? Quels enjeux court terme pour augmenter la cyber-résilience du transport aérien ? En quoi les technologies de cybersécurité existantes doivent évoluer pour prendre en compte les spécificités du transport aérien ? Quelles propositions pour une aviation future augmentée de fonctions de sécurité dédiées ? Quelle place pour l'innovation cybersécurité dans notre secteur qui doit trouver

prioritairement des solutions pour une aviation verte ? Autant de questions auxquelles nous devons répondre pour doter le secteur des bonnes armes et de moyens à la hauteur de l'enjeu, sur un secteur où la cybersécurité est une des clefs de notre souveraineté.

Pour renforcer la sécurité du contrôle aérien sur les systèmes opérationnels existants, et les infrastructures associées des compagnies aériennes et aéroports, nous pouvons agir pour protéger leur fonctionnement nominal et prévenir de cyber-attaques.

Bien-sûr, partout où c'est possible, les technologies existantes de sécurité et les bonnes pratiques associées seront mises en œuvre.
Mais le challenge est d'améliorer notre posture sans pour autant pouvoir faire évoluer par exemple des protocoles de communication vulnérables ou des outils opérationnels certifiés, mis au point pendant des années pour amener une interopérabilité mondiale et une fiabilité plus grande. Pas de possibilités d'usage des dernières technologies cybersécurité dans ce contexte !

Inspirée des regards croisés des acteurs de l'écosystème de l'aviation française opérateurs (compagnies aériennes et aéroports), avionneurs, et équipementiers et autorités, rencontrés dans le cadre du conseil cyber sécurité du transport aérien visant à mettre la cybersécurité au cœur des préoccupations du transport aérien cette réflexion s'articule sur trois axes.

Garantir la résilience de nos infrastructures, et des opérations aériennes

L'innovation est nécessaire si nous voulons des améliorations court terme ! Les technologies numériques vont être la solution. Le principe fondamental de ces innovations est la redondance dissimilaire. Il s'agit de doubler le processus outillé opérationnel critique existant, souvent réalisé in-fine par un opérateur, avec un équivalent numérique. Nous pouvons ainsi ajouter des vérifications croisées automatisée via des systèmes portables numériques (tablette, téléphone et leurs applications associées) augmentant ainsi l'intégrité des opérations critiques. Ajouter une application numérique de sécurité permettant une consolidation de

l'opération menée : pour les pilotes et personnels cabines via leurs EFBs enrichis de filtres métiers permettant de les alerter sur des données anormales, pour les contrôleurs jusqu'aux opérateurs de maintenance qui opèrent sur le tarmac pour leur permettre de faire des vérifications au plus près de l'aéronef, amènera une meilleure continuité de service. Avec ce principe, ce complément numérique devient un allié du quotidien. Facile à réaliser et peu coûteux à mettre en place, l'innovation réside surtout dans sa mise en œuvre où facteur humains et UX -User eXpérience- seront la clef de la réussite pour un usage accepté et efficace rendu possible par les nouveaux moyens de connectivité sol-sol et sol-bord.

Détecter et réagir rapidement à une attaque ciblée impactant les opérations aériennes

Pour organiser une réponse collective, il faut doter les parties prenantes - les opérateurs et leur supply chain- de capacités additionnelles de type cyber surveillance et de moyens de communications réseaux et téléphonie qualifiés pour véhiculer des informations sensibles. Mais comment se doter de la capacité d'interconnecter les centres d'opérations des différents acteurs clefs avec des centres de supervision de la cybersécurité (SOC) spécialisés dans la détection de cyber-attaques ciblées sur notre secteur aviation ? Le but est d'organiser une réaction rapide pour éviter des effets dominos dans notre écosystème.
La complexité vient de la variabilité de maturité et du nombre conséquent d'acteurs du domaine. L'innovation consiste à modéliser cette complexité et les scénarios « dominos » redoutés pour en déduire les effets « papillon » et les signaux faibles à surveiller et l'outillage des réactions associées, jusqu'à la formation des opérateurs

Maitriser une trajectoire technologique cyber dédiée à l'aéronautique

Le sujet est la protection « en profondeur » qui consiste à doter les systèmes critiques (au sens de la sûreté de fonctionnement) de détections, voire de capacités de réaction si jamais une attaque parvenait à contourner les protections périmétriques aujourd'hui définies. Un minimum serait de disposer de boïtes noires cyber pour ces systèmes critiques (contrôle du

trafic aérien, opérations de maintenance, systèmes de gestion des vols..). Cette nouvelle fonction permettrait d'enregistrer les évènements (dit « logs de sécurité »). Capturant les signaux faibles, ces boites noires permettraient de comprendre les tentatives de mise au point d'attaques et de comprendre les incidents éventuels par anticipation pour mieux appréhender les réactions à mettre en œuvre dans le futur. Mais, très vite nous rêvons à un assistant qui permettrait non seulement de détecter mais aussi de proposer des réponses de manière non équivoque. Le grand principe de ces innovations cyber est le développement de capacités de détection, de réaction locale, rapide, voire autonome permettant de maintenir la sûreté de fonctionnement et la continuité de service

L'ambition pourrait être plus grande encore en imaginant des « D2R2 cyber », compagnon numérique tactique, à base d'IA (Intelligence artificielle de confiance qui pourrait venir en aide aux opérateurs des systèmes critiques, pour identifier les situations anormales et proposer des actions tactiques en cas de risques, par exemple pour aider un pilote, un contrôleur aérien ou n'importe quel opérateur qui se trouverait dans une situation imprévue et qui aurait besoin d'aide. Avec l'apparition des drones dans l'espace aérien, des réactions autonomes seront aussi envisageables ! La traduction du concept de « zéro trust » (référence www.ssi.gouv.fr/agence/piblication/le-modelel-zero-trust/) pour l'aviation naÎtra de la connaissance absolue des fonctionnements nominaux des systèmes critiques et de l'identification en temps réel de tous les comportements anormaux observés qu'ils soient la conséquence d'une cyberattaque que nous ne connaissons pas encore ou d'un aléa de fonctionnement afin de permettre des réactions simples, locales et rapides de mise en sécurité du système critique.

AXE 1 : GARANTIR LA RÉSILIENCE DES OPÉRATIONS AÉRIENNES

Innover pour l'intégrité - au sens cybersécurité - des données « métier » des opérations aériennes

Sur quel processus et sur quelles données pouvons-nous augmenter la résilience via un compagnon numérique redondant le processus et

amenant une vérification dissimilaire des données critiques métier, ou par tout autre moyen de sécurisation de bout en bout de ces données ?
Les données « métier » représentent une masse conséquente de données brassées quotidiennement pour permettre les opérations aériennes. Quelques exemples :

- Les bagages avec leurs données associées : leur poids, leur localisation, leur appartenance, leur destination, leur contenu amènent des processus de gestion complexes pour bien des acteurs de l'écosystème. Les aéroports redoutent les erreurs d'aiguillage ou de vérification de sûreté, les compagnies aériennes veulent garantir leur destination et leur appartenance pour leurs passagers et les pilotes doivent connaitre les plus précisément possible la masse de leur cargaison pour calculer et régler au plus juste leurs paramètres de vol.
- Les plans de vol résultant de nombreux processus de la préparation du vol pour les compagnies aériennes et du contrôle du trafic aérien prennent en compte les routes autorisées, les données météo, le trafic, les états des pistes des aéroports, l'état du terrain, la gestion de la trajectoire pour respecter des objectifs de consommation modérée de kérosène, et utilisent des gigaoctets de données qui sont toutes « véhiculées » numériquement par des « chemins » différents. La fiabilité de ces données, leur intégrité numérique et la possibilité de les vérifier est essentielle
- Les données opérationnelles pour le maintien en condition de fonctionnement des logiciels métier associés aux processus critiques (données de maintenance, données de configurations, cartographie des états de fonctionnement ou d'usure ou d'obsolescence, mise à jour logicielles) sont une autre dimension des données métier dont l'intégrité doit être garantie sans pour autant changer leur format ou les outils/équipements qui les manipulent.

Autant d'exemples de processus outillés et de données métier auxquels nous pouvons associer des compagnons numériques apportant la cyber-résilience nécessaire. L'enjeu d'innovation court terme est de garantir l'intégrité de ces données, leur authenticité et leur innocuité, c'est à dire la preuve qu'elles n'ont pas été modifiées de manière malveillante, et ce à chaque étape des processus et si possible de bout en bout sur la chaine de traitement. Aussi nous avons besoin d'adapter les technologies cyber

existantes à ces spécificités métier : stations blanches adaptées aux supports amovibles parfois anciens- floppy disk, CD-ROM ..- et aux connectiques spécifiques aux équipements aéronautiques , compagnon numérique de vérification d'empreinte numérique de données critiques, filtres sécurité dédiés aux applicatifs métier, mise en œuvre d'un TrustFramework, tel que poussé par l'OACI, (Organisation de l'Aviation Civile Internationale) pour sécuriser les échanges des données métier de bout en bout (référence : www.icao.int/annual-report-2019/Pages/emerging-aviation-issues-cybersecurity_fr.aspx)

AXE 2 : DÉTECTER UNE MENACE CYBER CIBLÉE ET RÉAGIR RAPIDEMENT

Détecter l'accroissement réel de la menace cyber

Comment organiser une réponse collective, si nous ne nous dotons pas des capacités de cyber surveillance en focalisant sur les scénarios qui impacteraient les opérations aériennes ? Là encore, l'innovation va consister :

- d'une part à adapter des solutions cybersécurité de détection type firewall, détection d'intrusion/réaction réseau spécifiques à nos protocoles métiers, comme par exemple les protocoles aéronautique ADS-B pour les communications Sol-bord, ou Sol-sol par exemple avec des outils comme Asterix (reference : www.eurocontrol.int/asterix) développé et coordonné par Eurocontrol, capable d'interpréter les protocoles d'échanges des données Radar utilisées pour la surveillance du trafic aérien
- d'autre part à mettre en place les infrastructures permettant d'échanger de manière sûre ces éléments de surveillance, qui seront la source des indicateurs de compromission des attaques de demain. Bien-sûr à développer les capacités de « Threat Intelligence » - enquêtes sur les menaces visibles et cachées- et de « Hunting » - recherche d'indicateurs de compromission par rapport à des modes actuelles d'attaquants actifs sur un domaine ciblé.

Et s'entrainer à réagir pour soutenir les acteurs opérationnels du secteur

Pour soutenir les initiatives sectorielles dans le domaine type CERT - Computer Emergency Response Team- dédié à la réponse à incident, et les cellules de gestions de crise sectorielles, des moyens d'entrainement spécifiques pourront être développés pour entrainer les opérateurs à réagir dans le cadre d'une « breach attack » exercée sur des simulateurs ou des jumeaux numériques dits « cyber range ». Deux populations sont à former les « pompiers » et les opérateurs.

Les « pompiers » dans notre domaine doivent être capables de maitriser à la fois leurs techniques cybersécurité, mais aussi les technologies spécifiques du transport aérien, et avoir à leur disposition une bonne cartographie des flux de données critiques et de la modélisation des processus associés

Les opérateurs, chacun dans leurs domaines, de la maintenance en passant par l'organisation des vols d'une compagnie aérienne, ou le contrôle du trafic aérien ont besoin de savoir identifier une situation anormale sans chercher à l'analyser, mais pour en fournir un niveau de description suffisant pour alerter et appeler les « pompiers » et centre d'alerte de notre domaine.

L'innovation sur ce domaine consiste à faire évoluer les simulateurs existants utilisés à des fins de formation et d'entrainement pour qu'ils puissent inclure des modules orientés réaction à des situations anormales qui risquent d'être provoquées avec une plus grande probabilité que des défaillances par des cyberattaques.

AXE 3 : MAITRISER UNE TRAJECTOIRE TECHNOLOGIQUE DEDIÉE A L'AÉRONAUTIQUE DE DEMAIN

Accélérer des projets d'innovation cybersécurité spécifiques aux systèmes critiques de l'aviation pour la défense en profondeur

Nous avons besoin de développer nos technologies de défense en profondeur, c'est-à-dire à nous doter de moyens de détections, voire de réactions, si jamais une attaque parvenait à contourner les protections périmétriques aujourd'hui définies. Pourquoi ces technologies doivent-elles être spécifiques au secteur aéronautique ? La particularité des systèmes critiques de l'aviation est que leurs dysfonctionnements pourraient amener une désorganisation partielle ou globale des opérations aériennes, voire un risque de sûreté de fonctionnement. La force actuelle de nos systèmes critiques est la démonstration que leur comportement correspond strictement à leur modèle et spécification, D'un autre côté, nous ne pouvons pas prévoir les modalités des attaques cyber sécurité des dix prochaines années. Utilisons cette force initiale pour engager des stratégies de cybersécurité comportementales, c'est-à-dire une capacité de détecter les comportements anormaux et de réagir en revenant dans une enveloppe de fonctionnement autorisée. Utilisons cette force pour développer des capacités de réaction locales garantissant les temps de réponse nécessaires pour éviter des effets domino impactant au final les opérations aériennes.

L'innovation commencera certainement dans un premier temps par des capacités de détection locales et globales, puis par des capacités de réactions beaucoup plus complexes à modéliser.

- Pour se donner des moyens de détection spécifiques à certains systèmes critiques, nous pouvons travailler par étapes, d'abord bénéficier d'une « boîte noire » d'abord locale au système critique puis connectable à un SOC (« Security Operation Center »). Puis, nous pouvons envisager la mise en œuvre de sondes capables de corréler les évènements collectés localement pour lever les alertes non équivoques

- Pour se donner des moyens de réaction, nous ne pouvons pas « attendre » des incidents ou évènements réels pour avancer. Nous avons besoin pour concevoir ces solutions, de tester les effets d'attaques sur des systèmes représentatifs des chaines fonctionnelles critiques du transport aérien : ce sont des « CyberTWIN » . Enfin nous pourrons construire des capacités de réaction d'abord guidées puis autonomes, d'abord locales puis globales.

Il est à noter que pour les moyens de réaction, nous aurons besoin de travailler sur la problématique de la sécurité pour la sûreté, et la mise en place des moyens de certification vers nos autorités sectorielles permettant de donner la flexibilité nécessaire pour suivre les évolutions nécessaires pour « suivre » les évolutions des menaces et permettre un maintien en condition opérationnelle. Les lois de la physique n'évoluent pas là où les paradigmes de sécurité évoluent constamment. Résoudre cette dualité fait partie des challenges.

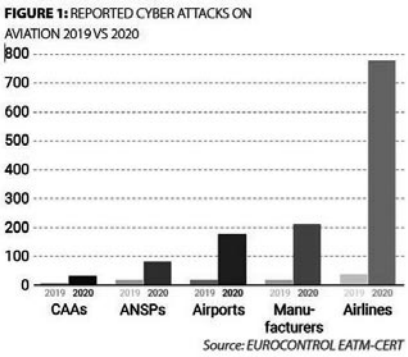
Malgré ces avancées technologiques, le risque zéro n'existera pas. Et il n'a jamais existé et ce, bien avant les problématiques de cyber sécurité. Mais en innovant sur des moyens de détection, de cyber surveillance et de réaction locale ou globale, nous concevrons, non pas des systèmes infaillibles mais nous concevrons des systèmes dont les risques redoutés ont peu de chance de rompre la continuité de service. La défense en profondeur de l'aéronautique doit passer par le développement de ces capacités.

Une défense en profondeur pour une aviation européenne résiliente aux attaques cyber

PATRICK KY
Président
Agence européenne de la sécurité aérienne

Contexte

La cybersécurité de l'aviation comporte deux facettes : la première concerne l'existence d'un nombre majoritaire de systèmes anciens, peu ou pas sécurisés, évoluant dans un cyberespace de plus en plus complexe. La seconde observe l'augmentation très rapide de la numérisation par l'intégration d'outils, systèmes et protocoles issus des technologies de l'information dans l'écosystème aéronautique. Nous avons d'un côté des systèmes aéronautiques conçus pour fonctionner en circuit fermé, avec une ouverture très limitée sur le monde numérique, dont l'internet, et qui ne sont pas capable de répondre à des cyber-attaques. Les risques que font peser ces menaces sur les systèmes aéronautiques hérités du passé ne sont pas complètement évalués. D'un autre côté, la rationalisation et la centralisation de l'infrastructure informatique de l'aviation et la multiplication des connexions réseau introduisent de nouvelles vulnérabilités susceptibles d'ajouter de nouveaux risques sur la sécurité des vols. Les nouveaux systèmes embarqués dans les aéronefs ou utilisés par le contrôle aérien s'appuient de plus en plus sur des technologies de l'information « grand public » ce qui introduit de nouvelles vulnérabilités susceptibles d'ajouter de nouveaux risques. Or, selon les observations fournies par des entités d'analyse et d'échange d'informations comme ECCSA[1], l'A-ISAC[2] ou encore l'EATM-CERT[3], les incidents de cybersécurité impactant l'aéronautique augmentent en fréquence, en ampleur et en complexité.



Il était donc urgent d'agir et l'Agence de Sécurité Aérienne de l'Union Européenne (AESA) avait anticipé la menace cyber dès 2015. Quelles ont été la vision, la stratégie et les moyens mis en œuvre pour répondre à cette nouvelle menace ?

Première étape : protéger les aéronefs

Dès l'apparition de nouveaux types d'aéronefs connectés, la réaction fut d'imposer aux fabricants l'implémentation de moyens de protection directement dans les systèmes embarqués avec une exigence d'efficacité proportionnelle aux risques sur la sécurité. Cela a été fait dans un premier temps grâce à l'utilisation de moyens règlementaires spécifiques, adaptés au type d'aéronef, au cas par cas. Depuis le 1er janvier 2021, ces solutions au cas par cas ont été rationalisées et intégrées dans les exigences de navigabilités. Aujourd'hui tout nouveau type d'aéronef doit intégrer le risque cyber dans son analyse de sécurité. Les opérateurs de ces aéronefs sont également instruits d'assurer le maintien de la protection des systèmes. Nous reviendrons plus loin sur les limites de cette ultime ligne de défense axée sur les aéronefs, mais elles impliquent de rajouter des lignes de défense autour des systèmes de bords. Celles-ci devant être implémentées de manière rationnelle, efficace et coordonnée, il apparut très rapidement qu'une stratégie globale était nécessaire et qu'elle devait impliquer l'ensemble des organisations de l'aviation.

Mise en place d'une stratégie globale

En raison du nombre croissant d'interconnexions, il est improbable qu'une organisation ait une vision complète des vulnérabilités de l'ensemble de l'architecture des systèmes qui supporte ses opérations. Le manque de moyens, de processus, ou de volonté pour échanger des informations liées aux risques cyber crée des barrières qui empêchent une gestion efficace du risque cyber dans l'aéronautique. Ne pas tenir compte de ces interconnections entre les différents acteurs de l'aviation peut au final résulter en une vulnérabilité, présente dans un système d'une organisation, se matérialisant en une menace qui affecte d'autres organisations.

Pour ce faire, l'AESA a très rapidement organisé des consultations stratégiques, au travers de conférences de haut niveau ralliant les décideurs du monde aéronautique européen autour de la volonté d'adresser ce défi. Il fut décidé de créer une structure de coordination stratégique. Cette initiative phare de l'AESA, l'ECSP[4] a pour but principal de rendre le système aéronautique européen résilient contre la menace cyber, en adoptant une cyberdéfense en profondeur dans les produits aéronautiques. Pour permettre la réalisation de cette vision, des objectifs ont été fixés concernant la coordination entre les acteurs du secteur, le partage d'information, la règlementation, l'évaluation du risque, mais également la promotion, la sensibilisation et l'engagement managérial ainsi que la mise en place des ressources nécessaires.

Pour concrétiser cette vision, la communauté aéronautique civile et militaire se sont jointes à ce partenariat coopératif, ont accepté l'objectif principal de définir et de coordonner la mise en œuvre d'une stratégie européenne pour la cybersécurité dans l'aviation.

Cette stratégie tient compte du contexte mondial et inclut une coordination internationale en tenant compte de toutes les normes et initiatives d'organisations internationales de l'aviation, des réglementations européennes applicables que ce soit en cybersécurité ou en sûreté aérienne, ainsi que des normes de l'industrie. Le succès de l'ESCP repose sur un travail collaboratif impliquant toutes les composantes de l'aéronautique,

venant aussi bien de l'industrie que des autorités nationales ou européennes. Les discussions et décisions prises ont abouti à la définition d'une stratégie et un plan d'actions pour la défense de l'aviation européenne. Ce plan d'actions a pour objectif de développer les capacités d'identifier, prévenir, détecter et répondre aux cyberattaques. Cela implique d'évaluer les impacts potentiels, en particulier sur la sécurité des vols de menaces cyber mais également d'établir une continuité opérationnelle dans un environnement dégradé par une cyberattaque. Ce besoin d'une continuité opérationnelle est une des caractéristiques de l'aviation car il n'est pas souhaitable d'arrêter des systèmes qui assurent la sécurité des vols en temps réel. La continuité doit être assurée avec des moyens de réponse appropriés permettant le rétablissement dès que possible des opérations normales.

Cette stratégie a été mise en place afin que le futur environnement aéronautique soit un environnement digne de confiance et fiable, et que toutes les parties prenantes de l'aviation européenne puissent compter sur les services et les informations fournies par d'autres pour la réalisation de leurs objectifs opérationnels. Elle concentre les ressources et les actions dans la réalisation d'une approche systémique de la cybersécurité dans l'aviation dans le but de développer un système de systèmes capable de résister à la menace cyber sans perturbations importantes. Ceci se fait sur deux axes principaux : une résilience évolutive, et une approche de sécurité intégrée.

Résilience évolutive

Un système aéronautique cyber-résilient est un système qui, en cas d'attaque, peut maintenir les fonctionnalités essentielles, c'est-à-dire continuer à assurer la sécurité des vols. Il atténue les effets néfastes des cyberattaques aussi rapidement que possible grâce à une protection à la fois holistique et en profondeur de sorte qu'une attaque réussie sur une couche, par exemple une usurpation d'authentification, ne puisse fournir une autorité suffisante pour compromettre les services critiques du système. Il doit suivre en plus un processus évolutif pour assurer une amélioration continue, c'est-à-dire apprendre des attaques et aborder les changements organisationnels nécessaires pour soutenir la coopération et

le partage d'informations entre l'aviation et les organisations liées à l'aviation, y compris civiles et militaires.

Cybersécurité intégrée

L'adoption d'une approche intégrée de la cybersécurité dans l'aviation signifie qu'il faille intégrer les objectifs de sécurité dès la conception des systèmes en même temps que les objectifs opérationnels et de sécurité traditionnels. Le secteur de l'aviation, dont les produits, les services et les processus ont une durée de vie de plusieurs décennies, doit asseoir son développement futur sur des bases stables en faisant des considérations de sécurité un élément important et une phase incontournable de la conception et de l'architecture des systèmes. Avec cette approche, la sécurité est intégrée des composants matériels jusqu'au au logiciel d'interfaçage avec l'utilisateur. Sécuriser tous les éléments des systèmes impliqués dans la réalisation d'un service critique aéronautique dès la conception permet d'effectuer la transition d'un environnement utilisant des actions correctives et réactives vers un environnement proactif et potentiellement évolutif. L'objectif est d'introduire la possibilité pour les systèmes d'être auto-renforçant, leur permettant ainsi d'évoluer et d'améliorer leur résilience de manière quasi automatique.

Première étape, faire le bilan

Comparer l'état initial du cyberespace aéronautique avec un système idéal ayant les capacités qu'on envisage de trouver dans un système résilient permet d'analyser les lacunes à combler pour mettre en œuvre le changement requis, ainsi que les difficultés, techniques et sociétales qui sont susceptibles d'être rencontrées. L'analyse a été menée en deux étapes : une première identification des obstacles globaux, voire des déficiences systémiques de l'aviation, suivie par l'identification et la spécification des propriétés que le futur système devrait être capable de déployer pour satisfaire les objectifs.

Le panorama des menaces

L'élaboration de la stratégie globale prend en compte le fait que

l'environnement des menaces cyber évolue sans cesse, en fonction de la situation politique internationale, du nombre et de la capacité des groupes malveillants, de leurs motivations et de la disponibilité d'un arsenal cyber de plus en plus efficace et accessible. Il est de plus à noter que ces évolutions échappent pour la plupart à l'influence des acteurs de l'aviation, ce qui fait que toute hypothèse utilisée dans l'élaboration du risque concernant une attaque cyber doit être réévaluée dès que cet environnement évolue. Par exemple, si le coût et la difficulté de développement d'un outil d'attaque est pris en compte dans le calcul du risque, le résultat de ce calcul fait obligatoirement évoluer avec le temps, à l'issue d'un temps certes variable mais très court au regard de la durée de vie des systèmes aéronautiques, la plupart des outils utilisés dans des attaques complexes et coûteuses se trouvent un jour sur le « dark web » et à partir de ce moment finissent très rapidement accessible en source ouvert sur internet. Ceci constitue un défi majeur dans le monde aéronautique car l'application de correctifs est plus long que dans le monde des technologies de l'information principalement à cause de la certification des systèmes.

Deux communautés, des objectifs divergents

Un autre défi général qui doit être pris en compte est la coexistence dans l'aviation de deux communautés, l'une dans le domaine de la sécurité et l'autre dans la sûreté, ayant des objectifs et des perspectives différents. Alors que les experts en sûreté de l'aviation entretiennent souvent des liens directs avec des sources d'intelligence concernant des attaques potentielles et sont habitués à faire face aux menaces intentionnelles et aux méthodes d'attaques, les experts en sécurité de l'aviation ont une connaissance approfondie des conséquences sur la sécurité des vols en cas de défaillance du système et ont une bonne connaissance de la conception et l'utilisation de ces systèmes, ainsi que les mesures de réduction des risques. Du point de vue sûreté, la cybermenace est un autre agent potentiel d'acte illicite, comme une bombe en vol, contre lequel l'aviation doit être protégée, alors que du point de vue sécurité aérienne, une interaction électronique non autorisée est une cause potentielle de dysfonctionnement des systèmes de bord, pouvant compromettre la navigabilité et réduire les marges de sécurité. La stratégie cyber de l'ESCP doit absolument réussir à intégrer

ces deux composantes afin de tirer parti de leurs capacités respectives, en particulier que l'intelligence concernant les cybermenaces soit intégrée dans les prises de décision concernant la sécurité.

Contexte règlementaire

Dernier obstacle, mais non des moindres, le contexte règlementaire dans lequel le système aéronautique évolue n'est pas des plus simples en ce qui concerne la cybersécurité et la mise en œuvre de la stratégie de l'aviation européenne. Sans trop rentrer dans les détails, la « cybersécurité aéronautique » se trouve à l'intersection de plusieurs environnements règlementaires : la sécurité aérienne et la sûreté aérienne comme cela a été introduit plus haut, mais aussi les règlements spécifiques cyber développés au niveau des états et de l'Union Européenne, comme la directive NIS (sécurité des réseaux et des systèmes d'information) dont l'objectif est de protéger les infrastructures critiques de l'Union Européenne, y compris le transport aérien.

Deuxième étape, développer la résilience

Pour atteindre un niveau de cyber-résilience suffisant pour l'aviation, il a été nécessaire d'identifier les éléments fondamentaux qui y contribuent d'un point de vue systémique : Premièrement, identifier les chaines fonctionnelles de l'aviation et ainsi prendre connaissance des systèmes critiques qui les longent, ceux qui assurent la sécurité des vols et la continuité du service. Il faut ensuite comprendre le niveau de protection requis par les attributs de sécurité (confidentialité, disponibilité et intégrité) de ces systèmes. Finalement, et ce n'est pas le plus facile, il a fallu obtenir l'adhésion et l'engagement complet des décideurs des organisations aéronautiques pour les décisions concernant la gestion des risques cyber afin de donner la priorité à la protection des éléments critiques identifiés dans la première étape.

Alors qu'une approche de cyber défense classique a pour but de protéger les systèmes, sans échec acceptable, en assurant une protection périmétrique autour d'un système ou d'une organisation, la cyber-résilience doit assurer la continuité des opérations, assurer la sécurité même

en cas de défaillance locale, doit avoir une architecture de défense en profondeur, multi couches, et avoir une portée trans-organisationnelle. En effet, le principal composant de la résilience est de partager le risque cyber et de s'appuyer sur plusieurs composants de l'aviation pour réaliser une fonction, de manière similaire à un système redondant et dissimilaire. Pour cela, la cyber-résilience doit exploiter toutes les connexions qui peuvent favoriser la collaboration entre les organisations pour assurer une fonction critique afin qu'en retour le niveau de protection global augmente au bénéfice de tous les acteurs de l'aviation. Pour développer de telles connexions, ces entités doivent prioritairement échanger de l'information sur les nouvelles menaces et vulnérabilités, l'analyse, la réponse et la gestion des incidents mais surtout établir les éléments de confiance entre les organisations.

Eléments mis en œuvre à ce jour

Cinq ans après la création de l'ECSP, des éléments concrets ont vu le jour qui ont contribuéss très rapidement à la sécurisation de l'aviation européenne. Le partage d'information a commencé à s'établir entre les membres de l'ECCSA. Dans le domaine de l'analyse, un groupe d'échange entre les Etats Membres, le Réseau d'Analystes en Cybersécurité (NoCA) a été également établi[5]. Dans le domaine règlementaire les évolutions nécessaires concernant les aéronefs, moteurs et systèmes aéronautiques sont applicables depuis le premier janvier 2021. En ce qui concerne les organisations contribuant à la sûreté de l'information dans l'aviation, l'opinion de l'Agence sur les exigences pour un système de management de la sûreté de l'information (ISMS) concernant ces organisations a également été publiée en 2021, et est susceptible d'être adoptée par la Commission Européenne cette année.

Mais l'impact le plus notable est le changement de point de vue de l'industrie envers la menace cyber. Alors qu'il y a cinq ans, toute nouvelle instruction concernant l'application d'une norme ou d'un règlement cyber pour la navigabilité des aéronefs était perçue encore comme une charge, un changement s'est produit durant cette période. La majorité des acteurs de l'aviation a pris la mesure du défi cyber et est maintenant pro-active, participe aux groupes de régulation de l'ESCP ainsi qu'aux plateformes

d'échange d'informations. Ce changement de perception est peut-être un des succès les plus visibles de la stratégie cyber européenne, peut-être grâce à sa nature collaborative.

Être prêt à affronter le futur

Le paysage aéronautique est en constante évolution. Cela est particulièrement remarquable dans cette dernière décennie qui a vue l'émergence de nouveau concepts d'opération, comme le transport aérien urbain quoiqu'encore embryonnaire, mais également de nouveaux défis, comme la cybersécurité, le risque pandémique ou l'effort à mettre en œuvre pour assurer la transition vers une aviation encore plus respectueuse de l'environnement. Ces défis s'influencent parfois les uns-les autres, lorsque par exemple la dématérialisation numérique de certains systèmes embarqués pour réduire la masse et du coup l'impact carbone entraine une augmentation de la surface d'exposition au risque cyber. L'impact de la pandémie de COVID-19 sur les équipes chargées de la sûreté des systèmes d'information a été également notable l'année précédente. L'émergence des opérations aériennes urbaines conjuguée avec une augmentation de l'automatisation des systèmes de pilotage, de navigation, de communication et de surveillance, voire d'une autonomie partielle ou totale, pose des défis auxquels il faut se préparer dès aujourd'hui. La stratégie cyber de l'ESCP, ayant été conçue pour être adaptative, permet déjà de préparer la cyberdéfense de l'espace aérien européen à ces défis du futur. Il faudra cependant veiller à ce que, de manière similaire au système de management de la sûreté de l'information, les éléments assurant la résilience du transport aérien européen contiennent également une composante « amélioration continue » afin de se corriger, se perfectionner et s'adapter aux menaces encore inconnues que le futur nous réserve.

[1] European Centre or Cyber Security in Aviation: L'ECCSA est un partenariat volontaire et coopératif au sein de la communauté aéronautique ayant pour objectif de mieux comprendre les risques émergents de cybersécurité dans l'aviation et de fournir un soutien collectif dans la gestion des incidents de cybersécurité et des des vulnérabilités qui pourraient potentiellement affecter la résilience et la sécurité du secteur aéronautique. https://www.easa.europa.eu/eccsa

[2] Un centre de partage et d'analyse d'informations ou (ISAC) est une organisation à but non lucratif qui fournit une ressource centrale pour la collecte d'informations sur les cybermenaces contre les infrastructures critiques et le partage bidirectionnel d'informations entre les secteurs privé et public. L'Aviation-ISAC est une entité basée au Etats Unis d'Amérique donc le secteur d'activité couvre l'aviation. https://www.a-isac.com/

[3] Un CERT pour la gestion du trafic aérien (EATM-CERT). https://www.eurocontrol.int/service/european-air-traffic-management-computer-emergency-response-team

[4] ESCP (European Strategic Coordination Platform) est une plateforme de coordination sur les questions stratégiques concernant la menace cyber dans l'écosystème aéronautique Européen. https://www.easa.europa.eu/community/content/european-strategic-coordination-platform-escp

[5] NoCA est une plateforme opérationnelle et technique pour l'AESA et les Etats Membres pour partager et analyser, dans un contexte confidentiel, des incidents d'origine cyber afin d'améliorer la robustesse de l'écosystème aéronautique. https://www.easa.europa.eu/community/content/network-cybersecurity-analysts-noca

Le risque cyber dans l'aviation de combat

JEAN-MARC LAURENT
Général de corps aérien (2S)
Responsable exécutif de la Chaire Défence & Aérospatial
Sciences Po Bordeaux

Parce qu'Internet a révélé au plus grand nombre les risques inhérents au transport de l'information numérique, il s'est répandu le sentiment que ce type d'insécurité serait exclusivement lié à ce réseau mondial et à son protocole d'échange de données. On oublie toutefois que, bien avant son avènement, la question de la fiabilité des informations se posait et qu'elle persiste toujours pour des modes de diffusion et d'échange autres qu'Internet. Ils concernent, pour la plupart, des domaines d'activité spécialisés et réservés comme l'aéronautique, en général, et l'aviation de combat, en particulier.

Certes, le risque porté par Internet touche l'aérien militaire par le biais, entre autres, de ses activités technico-industrielles qui sont largement digitalisées. Mais l'aviation des armées est aussi confrontée, dans sa dimension opérationnelle, à des menaces dématérialisées qui s'appuient sur des réseaux plus confidentiels. En outre, l'usage, à des fins offensives ou défensives, du spectre électromagnétique a, depuis longtemps et antérieurement à Internet, soumis les équipages de combat à des menaces dont les effets sont assez comparables à celles que le réseau mondial a générées. Ainsi, les agressions de ce qu'on appelle communément la guerre électronique (GE) affectent depuis longtemps les systèmes d'armes aériens et les missions de combat dans la 3ème dimension. On peut noter qu'elle le fait d'une façon assez analogue à ce qu'on observe dans la cyberguerre et le passage, pour la GE, de l'analogique au numérique a accru cette ressemblance. En outre, la connectivité croissante des réseaux (on parle désormais d'hyperconnectivité) combine de plus en plus les risques émanant de l'usage du spectre électromagnétique et ceux des réseaux numériques.

Cet article entend présenter quelques aspects de ce milieu impalpable mais bien réel auquel l'aviation militaire est confrontée. Mais il ne s'agit pas d'un rapport d'expert de l'électromagnétique ou des réseaux, mais seulement du témoignage d'un opérationnel du combat aérien.

D'une façon générale, les dangers cyber qui touchent l'aviation de combat peuvent se regrouper en deux familles d'effets : soit ils sont dirigés contre les aéronefs, en tant que machines volantes, et en perturbent le fonctionnement mécanique ; soit ils visent les opérations aériennes et affectent le déroulement opérationnel des missions de combat ou les dispositifs de commandement aériens (*Command & Control*[1]). Nous nous proposons d'évoquer ces différents aspects.

La menace cyber dirigée contre les aéronefs de combat

Commençons par le volet mécanique ou pseudo-mécanique[2] des plateformes aériennes, et par la fragilité numérique dont chacune d'entre elles peut être victime. Je ne vise ici aucun type d'aéronef en particulier, car si vanter un niveau de robustesse numérique d'un aéronef a du sens, vanter une robustesse absolue n'en a pas.

La numérisation des fonctions techniques d'un vecteur aérien lui confère assurément des capacités opérationnelles que les pilotes des générations d'aéronefs antérieures, et j'en suis, ne pouvaient imaginer. Elle permet d'apporter une agilité, une performance technico-opérationnelle et une survivabilité de l'aéronef par une capacité de gestion avancée de ses organes fonctionnels, une optimisation de son domaine de vol ou, encore, une assistance au pilotage ou à la résolution des pannes. C'est le cas, par exemple, des commandes de vol électriques ou des moteurs dont le fonctionnement est « piloté » par des calculateurs numériques. Cette digitalisation permet aux équipages de compter sur des aéronefs pouvant supporter des engagements agressifs tout en limitant le stress technique de leurs systèmes fonctionnels. C'est, par exemple, la capacité de réguler l'inévitable « brutalité » du pilotage humain dans les phases critiques des combats aériens. C'est aussi la capacité de limiter certaines conséquences de pannes en vol.

Mais, en contrepartie, cette digitalisation technique soumet les aéronefs à un risque lié à la qualité et la fiabilité des données numériques qui permettent la gestion de leurs organes vitaux. Or, le propre d'un avion de combat est d'œuvrer dans des environnements électromagnétiques et cyber potentiellement dangereux pour les systèmes mécaniques. Si, en la matière, la résilience des aéronefs occidentaux a toujours pu être préservée (je ne me prononce pas sur les autres), on peut penser que le développement d'une connectivité technique « élargie » pourrait changer la donne si elle ne se double pas d'une « armure » informationnelle.

Par exemple, des menaces pourraient pénétrer les appareils lors du chargement ou déchargement de données techniques avant ou après vol, la mise à jour de logiciels embarqués ou lors d'opérations de maintien en condition opérationnelle (MCO) faisant appel à des bancs de maintenance connectés. Les effets, potentiellement « pilotés » à distance par des agresseurs, pourraient affecter fonctionnellement les aéronefs, c'est-à-dire générer des pannes ou agir sur les qualités de vol et, dans un scénario extrême, conduire à leur perte. La sécurité cyber des outils techniques est donc essentielle et, à cet égard, le paramètre humain doit être prioritairement maitrisé car ce sont la discipline des opérateurs techniques et le bon suivi des règles de cybersécurité qui garantissent en grande partie l'intégrité des appareils et leur hygiène numérique.

La menace cyber dirigée contre des parcs d'aéronefs de combat

Une autre menace à caractère technico-logistique peut affecter l'aviation de combat. Elle ne joue pas forcément sur les paramètres fonctionnels d'un seul appareil mais a vocation à toucher des flottes entières en affectant les paramètres de gestion de leur potentiel opérationnel. Le risque encouru, s'il n'est pas jugulé, est bien plus stratégique que le précédent car il est en mesure de toucher un large pan capacitaire de la puissance aérienne de l'Etat victime. Expliquons-nous.

Depuis deux à trois décennies (cela dépend des générations d'aéronefs et de leurs opérateurs), la gestion des flottes aériennes est assurée par des systèmes digitalisés qui permettent de suivre la santé technique et les

besoins de maintenance[3] de chaque appareil, mais aussi de piloter la disponibilité et la pérennité technico-industrielles de toute une classe de vecteurs aériens. Ainsi, selon l'ambition de leurs concepteurs, ces Systèmes d'Informations Logistiques (SIL) assurent le suivi individuel des aéronefs mais aussi celui des stocks et des flux de pièces de rechanges nécessaires au respect permanent du contrat opérationnel[4] voulu par l'autorité politique. Ils permettent aussi une actualisation en temps réel de la documentation technique, particulièrement dense dans l'aéronautique. Ils peuvent enfin s'étendre à des fonctions « commerciales » comme la passation des contrats de service externalisés qui lient les opérateurs aériens à leurs fournisseurs[5]. Ces SIL ont été perfectionnés et élargis au fur et à mesure du temps et de leur déploiement. Ils tendent, de plus en plus, à s'enrichir de fonctionnalités qui permettent de coupler les informations à caractères technique et opérationnel. On comprend bien entendu l'intérêt de ces systèmes fédérateurs et concentrateurs de la connaissance. Ils permettent une gestion agile, coordonnée et corrélative des aéronefs de combat dont la complexité technico-opérationnelle est particulièrement ardue. Cette complexité est accentuée, selon les Etats, par leur dispersion stratégique sur les bases nationales ou sur les théâtres d'opérations. La France est, en la matière, un exemple marquant de cet éparpillement sur ses territoires métropolitains ou ultramarins, ses zones de pré-positionnement ou celles de ses engagements guerriers. La complexité de gestion est enfin liée aux missions de combat aussi hétérogènes que peu prévisibles et génératrices de faits techniques par principe inattendus.

A terme, ces systèmes de gestion numérisés offrent la promesse, grâce à l'utilisation d'intelligence artificielle et à l'exploitation du *Big Data Analytics*, de faire de l'anticipation technique et de gérer de façon encore plus efficiente[6] les flottes aériennes (on parle, par exemple, de maintenance prédictive). Ils permettront ainsi de maximiser encore plus la disponibilité opérationnelle et de réduire les aléas « matériels ».

En même temps, l'interconnexion des systèmes d'information doit être parfaitement maitrisée pour éviter toute fragilisation de l'ensemble d'un parc aérien. En effet, la cyber-santé de l'ensemble s'aligne sur le dispositif le plus cyber-faible. C'est le cas du système ALIS (*Autonomic Logistics Information System*) de l'avion américain F-35, qui agrège données

opérationnelles et techniques de l'appareil. Après que des failles cyber y aient été détectées et que des possibilités d'intrusion aient été démontrées, le *F-35 Joint Program Office*[7] décida de revoir l'outil (devenu depuis ODIN[8]) considérant, à juste titre, que « *La cybersécurité, la résilience et la capacité de survie du système aérien F-35 sont essentielles à la sécurité nationale et nécessaires pour maintenir la domination aérienne dans tout conflit futur*[9] ».

Les menaces, qu'un système insuffisamment cyber-étanche peut propager, revêtent de nombreuses formes et il serait vain de vouloir les décrire toutes. A titre d'exemple, je souhaite en citer une dont les effets peuvent s'avérer majeurs. Imaginons ainsi qu'un virus pénètre le réseau de gestion technique d'une flotte d'aéronefs et qu'il permette d'altérer la mesure de leur vieillissement[10], alors les conséquences seraient opérationnelles, économiques mais aussi stratégiques. En effet, il pourrait obliger la force aérienne victime à accroitre artificiellement les besoins (technique et économique) de maintenance, à faire face à une indisponibilité décroissante de ses appareils voire à ne plus pouvoir les faire voler si le doute concernant leur intégrité s'installait.

La menace cyber dirigée contre les effets opérationnels

Si la menace cyber peut affecter techniquement les systèmes d'armes aériens ou réduire leur potentiel « mécanique », elle peut aussi toucher la qualité de leurs engagements opérationnels en les empêchant d'obtenir les effets militaires désirés (exemple : brouillage), en les incitant à des actions contraires (exemple : leurrage) ou en détournant des données opérationnelles qu'ils produisent (exemple : piratage d'images ou de flux vidéo émanant des capteurs de reconnaissance des aéronefs).

En la matière, l'aéronautique de défense est depuis longtemps confrontée à ce qui se nomme militairement la « déception ». En effet, avec l'avènement du radar, lors de la seconde Guerre mondiale, l'aviation militaire dut immédiatement faire face aux intrusions dans le spectre électromagnétique et développa ce qui constitue encore aujourd'hui le domaine de la Guerre électronique (GE).

Pour les combattants, amis ou ennemis, il s'agissait d'émettre un signal ou de générer du bruit dans le spectre électromagnétique pour gêner les communications ou saturer les radars adverses. Cela pouvait aussi se traduire par la création de cibles aériennes fictives ou le déplacement irréel de menaces réelles. Certes, on ne parlait pas encore de guerre digitale, les matériels travaillant en analogique, mais la logique du cyber-combat était là.

Les grandes heures de la GE coïncident avec la Guerre froide et ses conflits périphériques, comme la Guerre du Vietnam, où des avions dédiés à la lutte contre les défenses anti-aériennes furent développés pour détecter les menaces électroniques, les brouiller mais aussi les neutraliser : une logique assez identique à la cyberdéfense d'aujourd'hui.

Lorsque le traitement des signaux électromagnétiques passa de l'analogique au numérique, la convergence GE-Cyber s'accentua et, aujourd'hui, l'origine GE ou cyber d'une menace peut être équivoque pour le pilote de combat. A l'avenir, les systèmes de défense mélangeront encore plus les deux origines. Mais, d'ores et déjà, les dispositifs A2/AD[11] couplent, à côté des missiles et autres systèmes anti-aériens, des capacités de déception électroniques et des capacités digitales adverses.

Plusieurs exemples me viennent à l'esprit pour caractériser cette menace contre l'action opérationnelle des aéronefs de combat. Nous avons déjà évoqué le leurrage qui oblige le pilote à s'extraire d'une évidence apparente pour éviter dans un piège mortel. Ces techniques, cyber ou GE, constituent des altérations de la donnée existante et non pas des attaques contre la matérialité des systèmes. Un second exemple me renvoie à ma propre expérience. Il s'agit, lors de missions de pénétration en très basse altitude, de la création d'échos « terrestres » qui leurrent les systèmes de suivi de terrain, obligeant les aéronefs agresseurs à épouser un relief inexistant et, perdant le bénéfice d'un relief protecteur, à se jeter inconsciemment dans la gueule du loup des systèmes anti-aériens adverses. Un autre exemple est la prise de contrôle d'un aéronef. A ce stade, on n'a pas de preuve que cela soit possible pour un avion de combat « habité » mais on sait qu'il existe, aux Etats-Unis, des avions de chasse utilisés comme cibles et pilotés à distance. On sait aussi que les plateformes

volantes des systèmes de drones, dont les capacités de contre-GE ou de contre-Cyber sont moins sophistiquées, ont pu faire l'objet de revendications de prise de contrôle[12].

Dans un contexte de numérisation croissante du champ de bataille aérien, le combat dans les Airs ou à partir des Airs s'appuie largement sur la qualité de la connectivité numérique ou, dit autrement, sur la faiblesse digitale de l'adversaire. Mais cette digitalisation transforme progressivement les aéronefs de combat en plateformes informationnelles qui agissent autant comme des capteurs numériques, des producteurs de données tactiques ou des nœuds de réseau d'un *combat cloud*[13]. La convergence voire l'amalgame entre combat aérien et combat cyber ne fait donc que s'amplifier.

La menace cyber sur le système de Command & Control

L'aviation militaire, agissant de jour, de nuit, par toutes les météorologies et sur des échelles de distance considérables, n'a pu se développer et mettre en place des stratégies offensives efficaces que grâce à une interconnexion des aéronefs entre eux mais aussi des aéronefs avec leurs centres de commandement. Cette dépendance informationnelle, née bien avant Internet, traduit ce qu'on appelle le C2 (*Command & Control*). Mais ce réseau air-air, air-surface (et aujourd'hui air-espace) se limitait initialement à des communications audio ou des interactions par le biais de données radars. Avec le numérique, il s'est progressivement étoffé et a permis des échanges informationnels de plus en plus denses, intriqués et interactifs, conduisant à une transformation totale de l'action armée dans les Airs : gestion instantanée de l'espace aérien à l'échelle d'un théâtre voire de plusieurs (ce fut le cas lors des opérations concomitantes en Afghanistan et en Irak) ; échanges de données tactiques automatisés entre aéronefs ou avec les forces terrestres et navales ; capacité stratégique de suivi des opérations aériennes à grande distance, etc. Ce partage de l'information entre centres de gestion des opérations (*Air Operation Centre*) et aéronefs se fait via des liaisons de données tactiques sécurisées, autres qu'Internet bien que pouvant être compatibles avec son protocole IP (comme la Liaison standardisée OTAN dite Liaison 16).

Les deux dernières décennies ont vu les échanges de données opérationnelles se développer à grande vitesse, au gré des capacités informatiques embarquées et des nouveaux aéronefs comme le F-22 aux USA ou le Rafale en France. Aujourd'hui, les avions de combat modernes mais aussi les avions spéciaux (comme les avions de commandement ou de gestion de l'espace aérien) sont avant tout des machines numériques volantes qui opèrent au sein d'un large réseau informationnel. Ils agissent comme producteurs et receveurs de data, comme outils de traitement et d'enrichissement des données tactiques ou comme relais d'informations numériques (ordres d'engagement, situation radar de l'espace aérien, flux vidéo d'activités terrestres, etc.).

L'augmentation mais aussi la fulgurance des échanges, dans un contexte soumis à une compression du temps opérationnel qui est la marque de l'aviation de combat (il se mesure souvent en secondes), a conduit à la création d'un véritable « *combat cloud* » c'est-à-dire, selon la définition de l'OTAN, d'un « réseau maillé global pour la distribution des données et le partage de l'information dans l'espace de combat, où chaque utilisateur, plate-forme ou nœud autorisé contribue et reçoit en toute transparence l'information essentielle et est en mesure de l'utiliser dans toute la gamme des opérations militaires ».

Le combat aérien est donc de plus en plus immergé dans un *Big data* opérationnel où le pilote reste, sans aucun doute, le décideur dans le cockpit mais où il doit combiner son intelligence avec une intelligence artificielle qui irrigue son aéronef. Il en est de même pour les opérateurs sol dans les centres de gestion des opérations (*Air Operations Center*). C'est ce qu'on appelle le *Man Machine Teaming*. Les différents projets européens ou américains de SCAF (Système de Combat Aérien Futur) verront encore grandir, d'ici une à deux décennies, cette connivence entre le tangible (l'équipage) et le virtuel (la connectivité informationnelle). Le développement du cyber de l'aviation militaire a donc révolutionné le combat aérien. Il permet aussi d'envisager la guerre aérienne, non plus à un niveau local ou régional, mais, sans rupture temporelle, à un niveau mondial. Cela autorise les aéronefs de combat à agir dans des zones de conflit à partir de des sites aussi dispersés qu'éloignés (Etats-Unis ou Golfe pour l'Asie centrale, Europe pour l'Afrique) tout en restant interconnectés entre eux et avec leurs centres de commandement.

Toutefois, si cette digitalisation du combat aérien porte en elle un évident facteur de puissance, elle est aussi la source de risques avec une possible intrusion dans le *combat cloud*. Une telle situation permettrait d'y inoculer des data erronées ou évolutives (générer une fausse situation tactique, créer de faux mouvements ennemis, déformer le champ de bataille numérique, etc.). Elle serait aussi à même de ralentir le cycle décisionnel des opérations aériennes représenté par ce que le monde militaire a l'habitude de nommer la boucle OODA[14]. Or, dans la guerre aérienne collective, comme dans le combat aérien individuel, le vainqueur est celui dont la boucle OODA est la plus rapide.

C'est la raison pour laquelle les dispositifs de *Command & Control* (C2) doivent préserver des modes de résilience non numériques et que les équipages et les opérateurs sol des batailles aériennes s'entrainent à travailler en ambiance cyber dégradée. Ainsi, des exercices sont conduits régulièrement, comme le fameux *Red Flag* américain, où pilotes de combat et opérateurs sont confrontés à des *Cyber Aggressors*.

En la matière, la présence d'humains dans les cockpits ou dans les *Air Operations Centers* demeure, encore aujourd'hui, la seule garantie viable pour faire face aux cyber-pièges. En effet, aucune machine ne sait vraiment modéliser cette forme d'irrationnalité pertinente qui fait la force de la nature humaine et qui permet, par ce qu'on nomme l'intuition[15], de décider face au doute, à l'ambiguïté ou à l'incertitude.

En conclusion

Depuis un siècle, l'aviation de combat élargit, décennies après décennies, ses espaces d'engagement. Il y eut d'abord l'exploration technologique et opérationnelle de la 3ème dimension, qui lui a donné agilité et élongation. Rapidement, elle a fait face à une 4ème dimension, celle du temps, qui lui a conféré fulgurance et précision. Dans le dernier quart du XXème siècle, elle s'est mesurée à une 5ème dimension, celle du spectre électromagnétique qui a fortement accru sa puissance mais lui a aussi opposé des menaces nouvelles devenues immatérielles. Avec l'émergence du digital et des réseaux interconnectés, l'aviation de combat s'est ouverte à un nouveau milieu et s'est « cyber-spatialisée ».

Avec cet environnement digital, elle doit faire face à une agressivité spécifique qui l'oblige et influe assurément ses modes d'action. C'est ce qu'elle fait avec des efforts de maitrise à l'échelle des systèmes d'armes (la robustesse cyber des aéronefs et la capacité des équipages à contrer les menaces virtuelles) ou à une échelle collective (la résilience cyber du C2 des opérations aériennes et la sécurité informatique des SIL).

Pour autant, l'aviation de combat doit aussi tenir compte des contingences propres aux autres dimensions physiques et temporelles où elle exprime sa puissance. C'est là tout le défi du développement des Systèmes de Combat Aérien Futurs qui, bien que fortement digitalisés, demeureront avant tout des objets matériels capables d'action cinétiques et mécaniquement vulnérables.

[1] Le *Command & Control* ou C2 a été défini par l'OTAN comme « L'organisation, le processus, les procédures et les systèmes nécessaires pour permettre une prise de décision politique et militaire en temps opportun et pour permettre aux militaires commandants de diriger et contrôler les forces militaires » (OTAN 1996

[2] Un aéronef moderne comprend des équipements purement mécaniques (comme le moteur ou les gouvernes) et des éléments non mécaniques qui leur sont associés (comme les commandes de vol électriques).

[3] Dans l'aéronautique, la maintenance des aéronefs est préventive et pas seulement curative. Pour chaque appareil, le vieillissement de chacun des milliers de composants est suivi scrupuleusement avec des dates de péremption ou des temps d'activité limites qui conduisent à des opérations de maintenance obligatoires avec dépose des composants concernés.

[4] Le contrat opérationnel des forces, en particulier aériennes, met en relation des ambitions, des capacités et des circonstances. En France, il est agréé par l'autorité politique.

[5] L'ensemble du réseau des fournisseurs de services, de rechanges et de matériels de maintien en condition opérationnelle des aéronefs comme d'autres produits industriels constitue la *Supply Chain*. Pour un avion de combat, on parle de plusieurs centaines d'entreprises qui entrent dans cette chaine logistique.

[6] Le terme « efficient » renvoie à la notion d'efficacité technico-opérationnelle doublée d'une optimisation économique.

[7] Le F-35 *Joint Program Office* est l'agence gouvernementale américaine chargée du management du projet F-35. Il dispose d'une Cyber Team attachée, entre autres, à trouver des « solutions innovantes pour informer et intégrer les capacités de détection et de réponse aux cyber-événements, destinées aux systèmes d'exploitation en temps réel (RTOS) et aux systèmes de technologie de l'information de plate-forme (PIT) ».

[8] ODIN : Operational Data Integrated Network

[9] "*Cyber security, resilience, and survivability of the F-35 air system are critical to national security and necessary to maintain air dominance in any future conflict*", *United States Government Joint Program Office Cybersecurity and Cyberdefense Challenge Notice*, 9 février 2022.

[10] Le vieillissement d'un aéronef est facteur de son activité (heures de fonctionnement, au sol et en vol) mais aussi de son type de vol (la fatigue étant plus ou moins importante selon les manœuvres aériennes).

[11] Les stratégies A2/AD, pour *Anti-Access/Area Denial*, cherchent à empêcher l'accès et la pénétration de zones défendues.

[12] Le 5 décembre 2011, les Iraniens revendiquent la prise de contrôle d'un drone Sentinel par leur unité de cyberguerre. Les Etats-Unis ont contesté cette action évoquant plutôt une destruction par un système sol-air.

[13] *Combat cloud* : réseau d'informations partagé agrégeant les flux d'information produits ou à destination des aéronefs et plateformes terrestres et navales, quels qu'ils soient, et les centres de commandement.

[14] La boucle OODA (*OODA loop*) est un concept inventé en 1960 par John Boyd, pilote de chasse de l'armée de l'Air des Etats-Unis. Fort de son expérience dans la Guerre de Corée, il a décrit le combat aérien par un cycle continu et récurrent de 4 séquences cognitives et opérationnelles (*Observe, Orient, Decide, Act*). L'objectif de l'attaquant est d'assurer une rotation plus rapide de son cycle que celui de son adversaire pour avoir l'ascendant sur lui. Le succès de sa théorie a conduit le principe OODA à être transposé, avec parfois des modifications sémantiques, dans de nombreux autres secteurs d'activité militaires et civils.

[15] L'intuition, présentée aussi comme la connaissance tacite, est définie, en psychologie cognitive, comme étant une forme de savoir issu de l'expérience.

Industrie 4.0, cheval de Troie de la cybersécurité intégrée au sein de l'aéronautique ? Une opportunité historique à saisir

COLONEL FLORIAN MANET
Commandant la Section de Recherches de Bretagne
Gendarmerie Nationale - essayiste

Le terme « Industrie 4.0 » est apparu pour la première fois sous la plume du professeur Wolfgang Wahlster, directeur du Centre allemand pour la Recherche sur l'Intelligence Artificielle[1]. Le 1er avril 2011, il publia un premier article dans les colonne de VDI Nachrichten intitulé « *Industry 4.0 : With the Internet of Things on the Way to Fourth Industrial Revolution* ». D'emblée, ce concept « Industrie 4.0 » fait référence, dans l'esprit de ses théoriciens, à la quatrième révolution industrielle dont la fondation principale repose sur la numérisation. D'où, par ailleurs, la sémantique « 4.0 » empruntée aux sciences de l'information.

Un projet fondateur : SemProM[2]

Le centre allemand de Recherche pour l'Intelligence Artificielle a conduit de 2008 à 2011 un projet d'étude « Mémoire de produit sémantique ».
Il vise à introduire une mémoire numérique de produits pour les objets du quotidien. Dans ce contexte, un robot mobile à deux bras est développé pour la manipulation automatique et le contrôle qualité de produits hétérogènes. La mémoire numérique du produit fournit au robot des informations de manipulation utiles comme le poids, la taille, les points de levage… du produit ciblé. Le projet se concentre sur la combinaison d'un manipulateur mobile hautement flexible avec le placement d'une antenne RFID. Le système de robot ainsi conçu a connu des applications ultérieures dans les domaines de la production et de la distribution de produits.

Dès lors, l'industrie s'est appropriée, avec succès, ce concept novateur qui, aujourd'hui, se répand au niveau international. Un phénomène global de numérisation de l'espace industriel tant au niveau de la production que des process mis en œuvre a redessiné les équilibres globaux. Ainsi, il embrasse toute la chaîne de production :

- conception du produit (usine virtuelle, continuité numérique, modélisation),
- contrôle et pilotage (automatisation des flux et des équipements : usines/ lignes connectées, capteurs/ Internet des Objets, logistique automatisée),
- procédés de fabrication (machine intelligente, fabrication additive, robots collaboratifs ou cobotique),
- maintenance conditionnelle (*big data*, télé-maintenance),
- organisation du travail (opérateur assisté, organisation apprenante).

Cette révolution industrielle s'est emparée de l'industrie aéronautique, notamment, dans les chaînes de production. Elle induit un changement fondamental de paradigme, source d'opportunités mais aussi de risques émergents[3]. La littérature explicitant le concept est, certes, prolifique, pointant les atouts comme les inconvénients. Toutefois, l'évaluation des risques liés aux technologies digitales interconnectées mérite d'être encore approfondie en décortiquant méthodiquement ce changement d'ère. Loin de ne présenter que des impacts environnementaux, qualitatifs ou productifs, l'Industrie 4.0 génère aussi une révolution sociale au cœur des chaînes de production et d'approvisionnement. Décloisonnant l'espace industriel à l'extrême, elle contribue, malgré elle, à le rapprocher d'acteurs malveillants qui exploiteront, sans état d'âme, les opportunités offertes par ce progrès technologique. Au total, cette réorganisation industrielle suscite un nouveau modèle économique global dont le maillon … fort doit demeurer l'Homme, garant de la résilience collective. A ce titre, le développement de l'Industrie 4.0 constitue une formidable opportunité pour renforcer la cybersécurité. Alors, considérons ce concept comme le cheval de Troie d'une cybernétique sécure au cœur de l'aéronautique !

Un ré-enchantement de la production ?

L'industrie 4.0 ouvre pleinement l'usine au monde extérieur.
Elle décloisonne l'ensemble d'une chaîne de production qui, jusqu'à présent, pouvait être perçue comme segmentée et isolée. En effet, autrefois, l'usine était un lieu spécifique qui était dissimulée et qui n'était fréquentée uniquement que par ses employés. Aujourd'hui, le site de production intelligent ou *smart factory* est porteur de valeurs au sein d'une chaîne interdépendante. Ces interconnexions reposent sur des technologies de l'information étroitement mises en réseau. Ainsi, l'Internet des Objets[4] connecte des objets, des équipements industriels et des process de production entre eux. Mais il intègre aussi l'écosystème amont (producteur de matières premières, fournisseurs, *supply chain*) et aval (*supply chain*, commerce de détail et, *in fine*, le client ou le consommateur). Sensible à ces multiples variations, l'objet et le process industriel sont dans une posture d'écoute permanente via un système complexe d'informations interconnecté et « intelligent ».

Enfin, ce mode de production remet définitivement en cause le principe de la production de masse d'articles standardisés. Par ce dialogue constant instauré avec le client, l'enjeu est désormais de produire du sur-mesure répondant aux attentes d'un client placé au centre du système. Avec des coûts de production équivalents voire inférieurs à ceux offerts par l'industrie de masse. En étant, par ailleurs, plus respectueux des ressources naturelles et de l'environnement. Cette proximité numérique établie avec le client vise, aussi, à le rendre acteur de la réalisation de son besoin. A même de suivre pas à pas les différentes étapes de sa fabrication.

La donnée, moteur de performance collective ?

Conçu comme une œuvre collaborative, ce nouveau processus industriel exploite les possibilités infinies qu'offrent les nouvelles technologies de l'information. A ce titre, la donnée devient le centre de gravité d'un système en recherche d'une performance accrue et d'une production centrée sur le client.

La donnée collectée et exploitée pleinement, à bon escient, génère des avantages concurrentiels majeurs. Or, d'une manière générale, il est unanimement reconnue aujourd'hui une trop faible exploitation de la donnée disponible. Les études démontrent en effet qu'elle est principalement employée comme un capteur destiné à détecter une anomalie sur une ligne de production. Victime de cette vision très réductrice, elle est donc, rarement convoquée pour optimiser les process de production et encore moins dans une visée de prédiction. Ainsi, selon un rapport du *Mc Kinsey Global Institute* intitulé *The Internet of Things : mapping the value beyond the hype*[5] publié *en* 2015, seul 1 % des données IoT collectées par les 30 000 capteurs d'une plate-forme pétrolière sont utilement examinées. Par ailleurs, les auteurs insistent sur les atouts d'une valorisation de la donnée au sein du process industriel. Pour ce faire, est pris l'exemple parlant du maintien en condition opérationnelle des lignes de production. La maintenance prédictive faisant appel à l'IoT pourrait, ainsi, réduire les coûts de maintenance des équipements de 10 % à 40 % et les pannes jusqu'à 50 %.

La donnée est bien la clé de voûte du concept d'Industrie 4.0. Elle repose sur trois innovations majeures[6] :
- l'informatique avancée ou décisionnelle avec les machines apprenantes, l'exploitation du *big data* et du *cloud*,
- les objets connectés avec la possibilité de faire le lien avec des objets physiques et des objets numériques,
- la robotique avancée avec des robots collaboratifs.

Au total, le principe d'une entité « *smart* » se fonde sur l'utilisation et l'exploitation des données et des algorithmes afin d'appliquer des processus et des procédures intelligentes qui pourraient, ensuite, être exécutés, évalués et améliorés. Ces entités sont conçues *nativement* pour détenir la capacité d'apprendre et de prendre des décisions en autonomie.

Émergence d'un nouveau modèle économique au sein de la filière aéronautique ?

Cette quatrième révolution industrielle marque une rupture historique dans la production industrielle. Motivée par une recherche permanente

de performances, elle favorise naturellement l'émergence de nouveaux modèles économiques fondés sur la proximité et l'agilité permises par la digitalisation, l'interconnexion des réseaux parties prenantes à l'écosystème de production et la prédiction. En retour, elle facilite une meilleure gestion des stocks et des flux.

Cette démarche de transformation est parfaitement adaptée au modèle économique de l'aéronautique fondé sur une organisation en filières. Ainsi, par exemple, les grands constructeurs commandent les moteurs ou les systèmes embarqués à des sous-traitants. De fait, la pression sur l'approvisionnement de pièces se répercutent tout au long de la chaîne d'approvisionnement composée, notamment, d'une myriade de PME ou ETI. Pour satisfaire la montée en puissance des cadences, les acteurs de la filière constituent des stocks tampons, ce qui peut être *in fine* source de fragilités selon l'évolution du carnet de commande. Enfin, l'aéronautique ne se caractérise pas par une production de masse mais par une réponse individualisée à une commande précise patiemment élaborée. La flexibilité de la filière conditionne son efficacité opérationnelle.

Par construction, la production aéronautique repose structurellement sur trois silos distincts :

- L'*Entreprise Resource Planning* (ERP) ou système de planification des ressources liées aux activités commerciales telles que la comptabilité, l'approvisionnement, la gestion de projet, des risques ou de la conformité et les opérations de la chaîne d'approvisionnement. Les systèmes ERP relient donc une multitude de processus métier et visent à faciliter le flux de données entre eux.
- *Manufacturing Executing System* (MES) ou système d'ordonnancement de la production. Le MES permet de croiser les données de la production avec celles d'autres domaines telles que la qualité, la maintenance, la traçabilité… L'objectif principal du MES est de garantir l'exécution effective des opérations de fabrication et d'améliorer le rendement de la production.
- L'atelier, le cœur nucléaire de la production aéronautique.

L'ambition de l'Industrie du futur appliquée à l'aéronautique est de casser ces 3 silos distincts en favorisant une interconnexion des données de

gestion de l'entreprise avec celle des opérations de l'usine. En d'autres termes, il s'agit de synchroniser le système de planification et d'exécution MES avec les ordres de production délivrée par l'ERP. L'avènement d'une intégration verticale aura pour effet de favoriser l'émergence d'un *smart manufacturing*. La mise en réseau de capteurs insérés sur l'ensemble des lignes de production facilitera ainsi une prise de décision au cœur de l'atelier, en temps réel, embrassant dans sa globalité les enjeux de production. Cela suppose néanmoins un ou des centre (s) de contrôle, point de convergence des données ainsi collectées à minima sur une ligne de production. De plus, il est envisageable d'y faire converger les données issues de plusieurs usines implantées dans plusieurs pays. Dans ce contexte, le rôle de ces *control rooms* sera aussi d'offrir une capacité d'anticipation et de modélisation de scénarii de production ou de crises en fonction d'événements (panne électrique, rupture de la chaîne d'approvisionnement, mouvements sociaux,..). Des applications mobiles sont aussi disponibles pour les opérateurs comme pour les décisionnaires désormais en mesure d'accéder en tout temps / tout lieu à la vie de l'usine en direct.

Ce nouveau paradigme est sujet à des risques singuliers dont l'ampleur est proportionnelle à la puissance de ses interconnexions.

Des risques 4.0, corollaires de l'interconnexion digitale ? Une révolution managériale en marche ?

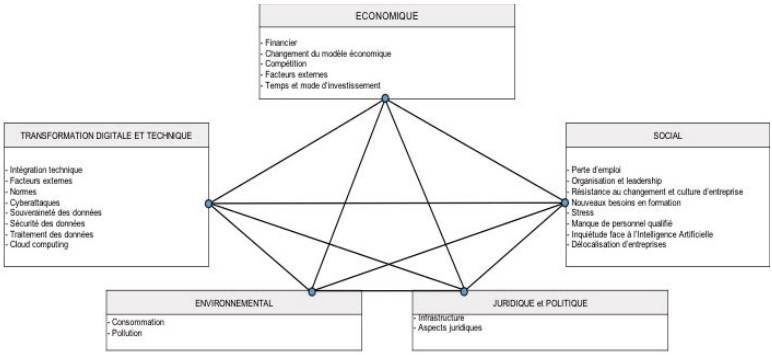
L'Industrie 4.0 engendre une révolution managériale au sein des organisations industrielles. Au cœur du dispositif se trouve le directeur du site de production. Pièce maîtresse, il est à la croisée des chemins de la traditionnelle verticalité qui donne du sens à l'action et d'une horizontalité de plus en plus prégnante qui souligne la dimension collaborative de la chaîne de production intelligente. Ce contexte technologique singulier exige de sa part un niveau élevé de compréhension des mécanismes digitaux et de leurs impacts en terme de production industrielle. Pour mieux appréhender cette nouvelle complexité, le dirigeant s'appuie, de plus en plus, sur des fonctions supports ou expertes. Aussi en est-il d'une figure emblématique, le *Chief Digital Officier* (CDO). Responsable de la transformation numérique, le directeur du digital conseille la direction, en produisant, notamment, des études d'impact sur les nouvelles

technologies et sur leur adaptation aux besoins de la production. Il supervise la bonne mise en œuvre de la stratégie numérique et de sa nécessaire coordination avec la stratégie globale de l'organisation. Par ailleurs, il veille à la cohérence des interconnexions établies par les acteurs du site avec l'ensemble de l'écosystème de production. Il s'efforce d'anticiper les risques et de construire des plans de continuité d'activité adaptés à chaque scénario de crise et aux sinistres. Dans les faits, il s'en suit un partage du pouvoir entre le directeur et le CDO. La complémentarité et la qualité des relations entre ces deux figures essentielles conditionnent la réussite globale de l'entreprise. Cette révolution transforme aussi les relations managériales. Elle s'accompagne corrélativement d'un effort essentiel de communication et de partage avec l'ensemble des collaborateurs qu'il faut embarquer dans ce tout numérique.

De plus, de telles organisations intelligentes supposent une très forte agilité de la part des salariés, acteurs essentiels du dialogue Homme - Machine et Machine-Machine. L'enjeu majeur de cette révolution industrielle est, aussi, la constitution d'une ressource humaine hautement qualifiée et de la qualité d'une formation continue à délivrer, incluant une forte dimension de cybersécurité. L'effort de formation est capital pour la bonne conduite des projets industriels. En effet, l'homme reste au cœur d'un système complexe : il donne du sens et de la cohérence aux données collectées. Son esprit d'analyse facilite la prise de décision. Mais, avouons le, il demeure un maillon fragile susceptible de contribuer, bien souvent malgré lui, à la compromission des systèmes numériques.

Cartographie des risques 4.0

Les différentes études relatives à l'Industrie 4.0 font apparaître une cartographie globale des risques spécifiques présentés dans le schéma ci-après.



Évaluation des risques propres à l'Industrie 4.0[7]

Dans ce contexte, et sans minimiser les autre items de cette étude, nous concentrerons notre attention sur la malveillance génératrice de risques technologiques, cyber et juridiques.

La cybercriminalité, valeur dominante du porte-feuille risque

A l'avenir, les gestionnaires de risque auront un porte-feuille où le volet cyber prédominera. Au-delà même des atteintes physiques sur les collaborateurs et les infrastructures de production. En retour, cette tendance est susceptible d'impacter les solutions d'assurance face à des événements de sûreté caractérisés par un préjudice exceptionnel. Cristallisant les enjeux de souveraineté, la valeur de la donnée épouse le contour de la nécessaire maîtrise de son identité personnelle, de la propriété intellectuelle et du savoir-faire sans négliger la réputation de l'entreprise. Le montant des rançons exigées par des cybercriminels est

illustratif des réalités d'un capitalisme criminel dont l'enjeu contemporain semble être la souveraineté de la donnée quelle qu'elle soit. Ce système illicite parasite le licite dans la mesure où, y puisant ses ressources, il dévoie ses finalités légitimes.

La Data, eldorado contemporain intangible

Centre de gravité de l'Industrie 4.0, la *data* est, alors, considérée comme le synonyme de l'eldorado, cette contrée mythique d'Amérique du sud supposée regorger d'or. La conquête de la donnée est minutieusement conçue par des organisations criminelles déterminées, astucieuses et agiles. Dans ce monde obscur, tout s'échange et tout se monnaye. Audace, disponibilité, compétences et réseau. Les préceptes du professeur Wolfgang Wahlster ont parfaitement été entendus. Innovation digitale, équipes apprenantes, interconnexion au sein de l'écosystème et monde ouvert constituent autant de caractéristiques partagées avec les organisations cyber-criminelles. La technologie numérique facilite l'identification préalable de cibles vulnérables susceptibles d'« accueillir », malgré elles, une infection ou *malware* qui se développera, ensuite, incognito, jusqu'à maturité. Une « porte ouverte ou un trou dans la muraille » au sein des systèmes suffit à déterminer le contour de sa proie, à visiter le « domaine » jusque dans ses moindres détails et, ce, en toute confidentialité. Il s'agit là d'un véritable audit externe (et …malveillant), nourrissant une fine évaluation du potentiel de nuisance qu'une attaque portée sur les systèmes de traitement automatisé de données signifiera *in fine*. C'est aussi une étape clé dans l'évaluation future de la rançon qui sera, ensuite, exigée. La question de la solvabilité de la victime est l'une des explications de la localisation des attaques ciblées au sein des pays développés. Précisons que le moteur principal de l'action criminel demeure l'appât du gain.

Quel que soit le mode opératoire de l'attaquant, l'effet produit se traduit immanquablement sous la forme d'un déni de service. La ligne de production est arrêtée, les serveurs de *control and command* ne sont plus opérants, le fichier clients a disparu tout comme les fichiers de paye voire la dernière innovation de l'entreprise. Fruit d'une interconnexion recherchée à dessein, cela peut être l'ensemble d'un écosystème interdépendant par construction qui se trouve amputé et perturbé.

L'exemple du rançongiciel NOT PETYA est illustratif des effets produits et du caractère irrémédiable d'un tel déni de service opéré sur 50 000 terminaux portuaires. Cette attaque a visé MAERSK, l'opérateur majeur de la logistique maritime mondiale. Le 27 juin 2017, suite aux chiffrements de ses serveurs, MAERSK a été contraint à une reprise manuelle de la gestion et de la manutention de ses terminaux à conteneurs sur 600 sites répartis dans 130 pays. Les pertes directes supportées par l'opérateur s'élèvent à plus de 300 millions de dollars. Quel est le montant global de la facture pour l'ensemble des victimes collatérales de ce dérèglement logistique ?

Le principe fondateur de l'Industrie 4.0 est bien de garantir un continuum numérique fluide entre les multiples acteurs membres d'un même écosystème solidaire. La force de l'ensemble du système repose sur la résistance du .. plus faible des maillons constitutifs de cette chaîne d'intérêts. Les impacts collatéraux sont importants et ne sont guère circonscrits à un secteur d'activité ou à une aire géographique. D'autant plus que des événements physiques peuvent se sur-ajouter à cette évaluation du risque. L'incendie involontaire d'un serveur ou bien une avarie dans les chaînes logistiques[8] sont autant de scénarii perturbateurs mais réalistes. Cet état de fait hors norme ouvre des perspectives de questionnement sur la prise en charge des risques par les compagnies d'assurance et sur l'identification des responsabilités. Des recherches actives sur des solutions d'atténuation du risque intangible[9], notamment en matière de risques immatériels stimuleront l'innovation et garantiront la pérennité du système.

Le commerce de la donnée est devenu un corollaire de ce progrès technologique. Stockées dans le *cloud* ou dans des serveurs physiques, ces *data* ainsi dérobées font l'objet de multiples transactions sur le *darknet* : rançon contre souveraineté de la *data,* revente des données à d'autres opérateurs criminels, usurpation des données à des fins illicites telles que la commission d'autres délits (atteintes à la propriété intellectuelle, ouverture frauduleuse de comptes de rebond ou de sociétés facilitant la réalisation d'escroqueries financières, chantage de toute nature, ..). De plus, le cadre légal unifié à l'échelle européenne relatif à la protection des données influe sur le comportement des acteurs victimes. En effet, le

Règlement Général de Protection des Données[10] impose des obligations aux personnes morales et physiques dès lors qu'un traitement automatisé des données est effectif. Ainsi, l'article 33 subordonne la notification à l'autorité nationale de protection en cas de violation de données mais aussi l'information des personnes concernées par cette violation en cas de risque affectant les libertés et les droits des personnes. De plus, les régulateurs nationaux peuvent, en cas de non-respect, infliger des sanctions financières allant jusqu'à 4 % du chiffre d'affaire global annuel. Dans un tel contexte, on peut comprendre aisément la posture d'opérateurs victimes d'une manœuvre frauduleuse de chiffrement peu enclins à s'exposer, en sus des dommages directs liés au sinistre, à des sanctions financières.

Les Machines, point de vulnérabilité majeur ?

Les équipements industriels constituent des points d'entrée dans les lignes de production. A ce titre, ils sont susceptibles d'offrir des vulnérabilités potentielles pour des violations de données et des dénis de service. La multiplication des appareils connectés présente des interfaces pour des attaquants et génère immanquablement un accroissement du risque. De plus, les failles de sécurité intégrées aux codes logiciels embarqués sont souvent difficiles à détecter et à circonscrire. D'autant plus que cette révolution industrielle exploite pleinement les atouts des systèmes cyber-physiques[11], de la cobotique[12], de la communication entre machines[13], de l'Intelligence Artificielle et des imprimantes 3 D.

Dans ce domaine, l'inter-connectivité forte entre réseaux est susceptible de répartir, d'amplifier les dommages rapidement et de manière significative au sein d'un éco-système complexe. Ainsi, les scénarii de fermeture d'infrastructures complètes contaminées telles qu'une chaîne de production aéronautique ou d'assemblage auraient un impact majeur dans le cadre de sinistres futurs. Sans négliger la perte de production d'un sous-traitant fournissant une pièce clé dans le process industriel. Ces scenarii s'intègrent dans la perspective d'un cyber-chaos redouté.

L'Homme, clé de voûte du système digital ?

Dans ce contexte qui, rapidement, peut devenir anxiogène, il convient de s'assurer de la prise en compte du risque par des mesures de prévention élémentaires.

Au cœur du système réside et résidera l'homme. Le salarié. L'opérateur. Mais aussi le *Chief Digital Officer.* Et le directeur. Chacun a son niveau de responsabilité et d'implication. La clé de voûte du réseau repose dans la nécessaire confiance entre membres de cette même chaîne d'intérêts. Celle-ci s'entretient quotidiennement par la formation et par la sensibilisation aux menaces cyber. Il s'agit d'effectuer des exercices sur table ou grandeur nature pour s'assurer de la pertinence des consignes à appliquer et de leur maîtrise par les équipes. Ces pratiques méritent d'être complétées par des rappels incessants au personnel sur les mesures de sécurité et d'hygiène informatique. L'exploitation pédagogique de retours d'expérience internes ou externes contribue, par ailleurs, à maintenir vive l'attention et la détermination.

Enfin, la conception globale du système de protection des réseaux est l'acte fondateur de la sécurité numérique. Des questions simples permettent d'évaluer la souveraineté de son patrimoine informationnel et de son étanchéité. Qui contrôle les accès ? Combien sont ouverts en permanence ? Y-a-t-il des restrictions d'accès ? Qui détient les clés ? Qui régit la liste des accédants et des détenteurs de privilèges ? Etc.. En filant utilement la métaphore guerrière, il s'agit de concevoir un système de défense digne des forteresses de Vauban, célèbre ingénieur et architecte militaire du Roi Soleil. Ses constructions en étoile, érigées sur des points stratégiques du Royaume, ne présentaient aucun angle mort et prenaient en compte toutes sortes de menaces. A l'intérieur des casernements, l'organisation comme la répartition des tâches entre corps constitués était minutieusement réglée. Sa philosophie d'ingénieur- architecte conserve aujourd'hui toute sa pertinence, notamment en matière de cybersécurité : « l'art de fortifier ne consiste pas dans des règles et dans des systèmes, mais uniquement dans le bon sens et l'expérience ». Gageons que le bon sens soit répandu et que l'expérience soit partagée !

Ainsi, ces nouvelles méthodes de gestion des processus de production industrielle interconnectés et collaboratifs font apparaître des risques émergents relatifs aux connexions entre les opérateurs humains, les systèmes et les objets connectés. Elles offrent un cadre de réflexion utile sur la gestion des risques issus de systèmes complexes. Cette démarche s'inscrit aussi dans les projets plus généraux de *smart port* et *smart city*. Ces environnements urbains et logistiques interconnectant un nombre sans cesse croissant d'acteurs et d'objets connectés viendront interagir avec les *smart factories*.

Une Sagesse 4.0 ?

Cette quatrième révolution industrielle revêt des impacts socio-économiques, organisationnels, juridiques et sécuritaires. Elle suscite, en la matière, des innovations dans tous ces aspects. Elle invite, avant tout, à promouvoir une approche intégrée au sein des organisations interconnectées. Dans ce contexte de complexification des chaînes de production, les capacités humaines peuvent être dépassées et inaptes à saisir les facteurs pertinents dans l'action ainsi que dans la prise de décision. De fait, le recours aux solutions « uniquement » technologiques apportées aux risques émergents peut être trompeur et même accroître les fragilités. Notamment si l'on écarte le facteur humain et organisationnel. Ainsi, le danger majeur peut provenir d'une confiance absolue dans la technologie sans pour autant en identifier ses limites et vulnérabilités. Cette situation - non exclusive de la filière aéronautique - invite à un partage d'expérience avec d'autres secteurs d'activité complexe tels le nucléaire, la pétrochimie ou la construction automobile. Eux aussi sont confrontés aux problèmes liés à la performance humaine. Au fil des expériences, ils ont développé des méthodes d'analyse et des protocoles de prise de décision raisonnée dans le cadre d'une gestion intégrée des risques. L'homme y a toute sa place.

Finalement, l'Industrie 4.0 est en soi une Sagesse.

[1] Ou *Deutsches Forschungszentrum für künstliche Intelligenz* (DFKI)

[2] https://robotik-dfki—bremen-de.translate.goog/en/research/projects/semprom..html_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=nui,sc

[3] Un risque émergent résulte d'un danger nouvellement identifié auquel une exposition significative pourrait se produire. C'est aussi un risque résultant d'une exposition et/ou d'une sensibilité nouvelle ou accrue et inattendue à un danger déjà connu. Cité par l'EFSA (*Européen Food Safety Authority*), disponible sur https://www.efsa.europa.eu/fr/topics/topic/emerging-risks, consulté le 20/10/21.

[4] Ou Internet of Things (IoT).

[5] Disponible sur https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%2520Media%2520and%2520Telecommunications/High%2520Tech/Our%2520Insights/The%2520Internet%2520of%2520Things%2520The%2520value%2520of%2520digitizing%2520the%2520physical%2520world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.pdf&ved=2ahUKEwjj5r2Un9LzAhUM8BoKHceZBkUQFnoECC0QAQ&usg=AOvVaw2CyXg-vrA4I-y6-opbmAmG, consulté le 19/10/21.

[6] Max BLANCHER, *Industrie 4.0 Nouvelle donne industrielle, nouveau modèle économique*, Lignes de repères 2016.

[7] https://www.google.com/url sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi_wfnQgd7zAhXNN8AKHd9fAnsQFnoECBYQAQ&url=https%3A%2F%2Fwww.mdpi.com%2F2071-1050%2F11%2F2%2F384%2Fpdf&usg=AOvVaw0GeJW-F8NCSMPEYxQXp_Rp, consulté le 19/10/21

[8] Le transport maritime supporte 90 % du commerce international. Le blocage d'une artère mondiale de communication telle le canal de Suez, trait d'union entre la mer Méditerranée et l'océan Indien, est un scénario réaliste de perturbation grave des approvisionnements internationaux. D'une capacité d'emport de 20 000 EVP, le porte-conteneurs EVERGIVEN a échoué accidentellement lors de sa navigation dans le canal de Suez le 23 mars 2021 au matin. Son immobilisation a duré 100 jours. Selon Lloyd's List, le coût horaire de l'obstruction serait de 400 millions de dollars eu égard à la valeur des marchandises en transit sur le canal de Suez.

[9] « Le capital intangible est une promesse de bénéfices futurs qui n'apparaît pas au bilan et qui est difficile à contrôler. Un risque intangible est son pendant : une exposition à des pertes futures qui n'est pas quantifiable par les méthodes classiques d'analyse de risque basé sur des études statistiques à cause de la nature rare et aléatoire des événements créant ce risque. » Michel Philippart, 13 juin 2020, disponible sur https://www.place-escange.fr/comment-integrer-les-risques-intangibles-des-longues-chaines-dapprovisionnement/ consulté le 20/10/21.

[10] Règlement UE 2016/679 du Parlement européen et du Conseil du 27/04/2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[11] Un système Cyber-physique (CPS ou *Cyber-Physical-System*) est un système industriel où des éléments informatiques collaborent pour le contrôle et la commande d'entités physiques. Il repose sur la robotique et les réseaux de capteurs. Les CPS sont très présents dans l'industrie aéronautique, automobile, chimique ou dans les transports.

[12] La cobotique est un néologisme apparu en 1999 formé à partir du concept de « *Cooperative Robotics* » et des mots « coopération « et « robotique ». Il désigne un dispositif robotique conçu, fabriqué et utilisé pour interagir et coopérer avec un humain. Contrairement à un robot classique qui fonctionne de manière autonome.

[13] Ou *Machine to Machine* (M2M). Il utilise les télécommunications et l'informatique pour permettre des communications entre machines, sans intervention humaine.

L'OACI engagée pour la cybersécurité et la cyber-résilience de l'aviation civile internationale

LAURENT PIC
Ambassadeur de France
Représentant permanent de la France
Conseil de l'Organisation de l'aviation civile internationale

Comme la plupart des pans de l'activité humaine, l'aviation civile internationale a engagé une transition vers le numérique. Le déploiement des nouvelles technologies de l'information engendre une vague sans précédent d'innovation qui accroît sans cesse davantage sa connectivité. De plus en plus, toute la chaîne des acteurs qui permet à un avion de voler d'un point A vers un point B utilise les réseaux pour communiquer plus vite et mieux, des constructeurs aux services de navigation aérienne, en passant par les compagnies aériennes et les aéroports. En soi, cette évolution devrait accroître l'efficacité des opérations et aider l'aviation à être à la hauteur des enjeux de notre temps, y compris la réduction de ses émissions de CO2.

Mais, il ne faut pas se tromper : à nouveau saut technologique, nouvelles menaces ! De longue date, l'aviation civile internationale a été une cible de choix pour tous ceux qui veulent l'instrumentaliser à d'autres fins, en la perturbant au détriment de l'exigence fondamentale de sécurité qui a, depuis l'origine, accompagné son essor. L'émergence d'acteurs extérieurs à l'aviation dans toute la chaîne du transport aérien contribue à augmenter les risques. La lucidité s'impose : le déploiement des technologies de pointe peut devenir une source de nouvelles formes d'interventions illicites. Dans un monde numérisé, de telles menaces peuvent avoir des conséquences catastrophiques pour l'aviation et constituer un immense défi, d'abord pour sa sécurité.

Conformément à son mandat qui consiste à fournir à l'aviation civile internationale des règles communes allant de pair avec la nature globale de ses activités, l'OACI doit être au rendez-vous de la cybersécurité. Tout comme cette organisation du système des Nations Unies, instituée par la convention de Chicago, l'a été tout récemment, en réponse à l'impact de la pandémie de COVID-19 sur le transport aérien.

Dès 2019, l'OACI s'est dotée d'une stratégie en matière de cybersécurité et d'un plan d'action. Ces instruments, amenés à être régulièrement mis à jour, ont été approuvés par le conseil, l'instance de gouvernance à composition restreinte qui assure la gestion de l'organisation entre deux sessions de l'assemblée qui, forte de ses 193 États contractants, fixe tous les trois ans les grandes orientations.

La stratégie de l'OACI part de plusieurs postulats : reconnaissance par les Etats des obligations que leur impose la convention de Chicago d'assurer la sécurité, la sûreté et la continuité de l'aviation civile en tenant compte de la cybersécurité ; coordination de cette dernière entre les autorités des Etats afin de garantir l'efficience de la gestion mondiale des risques ; engagement de toutes les parties prenantes à développer la cyber-résilience, en assurant la protection contre les cyberattaques. Comme dans de nombreux domaines, sont mobilisés de nombreux instruments, tels que la coopération, le partage de l'information, un cadre normatif efficace, la gestion des incidents et la planification d'urgence, le renforcement des capacités et la formation. Mais, à bien des égards, c'est la dimension humaine qui est la plus importante, dans une approche où la cybersécurité doit relever, à part entière, de la culture de sûreté que l'organisation s'efforce de promouvoir.

Au-delà, l'OACI a aussi pour ambition de mettre à la disposition de tous les acteurs de l'aviation un outil efficace pour sécuriser leurs échanges dans le cadre d'un réseau garantissant les identités numériques. C'est de cette volonté qu'est partie l'idée de mettre en place un cadre de confiance pour l'aviation internationale (International Aviation Trust Framework ou IATF). Dans cette perspective, le travail se poursuit sur un concept d'opération et la gouvernance d'un tel instrument, qui doit donner aux Etats toute la place qui leur revient dans la gestion de problématiques qui relèvent aussi de leur souveraineté.

Pour avancer, il conviendra de trancher des questions fondamentales : est-il réaliste d'imaginer un réseau unique ou préférable de faire le choix de l'interopérabilité entre des réseaux développés à l'échelle nationale ou régionale, comme l'Union européenne s'y emploie d'ores et déjà ? L'exploitation d'un tel cadre de confiance peut-elle être légitimement confiée, dans le cadre d'une approche centralisée à l'échelle mondiale, à une entité privée, selon un modèle envisagé aux États-Unis ? Les Etats peuvent-ils raisonnablement l'envisager, alors qu'il en va de leur sécurité, que le cadre de confiance est susceptible de faire partie à terme des infrastructures critiques et qu'une des fonctions à assurer consistera à évaluer la fiabilité des acteurs participant à ce cadre de confiance y compris, le cas échéant, des entités publiques ? Beaucoup de travail est encore nécessaire pour aboutir à ce que l'IATF, dont la pertinence n'est pas en cause, voie le jour.

Comme dans chaque pays, l'OACI a aussi pris conscience que la cybersécurité appelle une approche transversale et une coordination étroite entre toutes les instances qui en traitent certains pans. C'est le cas de plus d'une dizaine de groupes d'experts au sein de l'organisation, les fameux panels, qui à titre ou à un autre sont amenés à intégrer la problématique cyber dans leurs travaux. Cet éparpillement existe aussi au sein du secrétariat de l'OACI, dont la direction du transport aérien a piloté l'élaboration de la stratégie et du plan d'action au titre de ses responsabilités en matière de sûreté, alors que la réflexion sur le cadre de confiance est portée par la direction de la navigation aérienne. Il en va de même pour les organes de gouvernance et leurs instances préparatoires.

C'est la raison pour laquelle l'assemblée a jugé nécessaire, en 2019, de lancer un travail sur la gouvernance des questions cyber à l'OACI, en vue de renforcer la coordination et d'assurer une meilleure transparence et leur indispensable supervision par le conseil. Il aura fallu près de deux ans et la mobilisation des Etats pour que cette étude de faisabilité aboutisse à une proposition qui a été approuvée, début 2021, et dont la mise en œuvre est bien engagée. Alors que les travaux sur la cybersécurité étaient jusqu'alors l'apanage de groupes d'étude du secrétariat, il a été décidé de transformer ces instances en panels en bonne et due forme, de manière à mieux identifier la chaîne de commandement et le suivi des travaux par

les organes de gouvernance. De même, un comité ad hoc de coordination relevant du conseil réunira un représentant de chacune des instances et des panels traitant de cybersécurité afin de veiller à la cohérence d'ensemble et à l'absence d'angle mort dans les travaux de l'organisation. Ce comité complétera la stratégie et le plan d'action de l'OACI d'un programme de travail unique. Cette nouvelle gouvernance, dont le caractère sui generis correspond à la spécificité et à la nature transversale de la cybersécurité, fait écho au choix que la France a fait pour elle-même, en instituant un conseil cyber pour le transport aérien qui réunit tous les acteurs concernés, publics ou privés.

A l'OACI comme partout ailleurs, la clé est en effet dans une association étroite des entreprises. Leurs experts participent déjà activement aux travaux de l'organisation. Ils continueront à le faire dans le cadre de cette nouvelle gouvernance. La France, qui a joué un rôle actif pour la porter sur les fonts baptismaux, y veillera.

Table des matières

Sécurité numérique & Aéronautique

CyberCercle - 92 Cours Lafayette, 69003 Lyon
contact@cybercercle.com - cybercercle.com

« Sécurité numérique & Aéronautique » est le troisième ouvrage de notre Collection CyberCercle - Regards croisés lancée fin 2020.

Des livres collectifs, dont chaque édition associe des auteurs représentant différentes organisations, publiques et privées, autour d'une thématique déterminée dans le champ de la confiance et de la sécurité numériques.

Des livres collectifs qui peuvent se lire de la première à la dernière page, ou de façon séquencée, par des entrées « auteur » ou « thématique ».

Ces ouvrages n'ont pas l'ambition d'être exhaustifs. Ils ont pour vocation, grâce à des contributions de personnalités expertes complémentaires, d'apporter aux lecteurs des éléments d'analyse de confiance propres à enrichir leur appréhension du sujet et leur réflexion.

La Collection CyberCercle - Regards croisés s'inscrit ainsi, à travers ses publications, comme une référence dans le panorama français de réflexion sur les sujets de confiance et de sécurité numériques, un outil de travail au service de la décision.

Ce troisième ouvrage est consacré au secteur aéronautique, secteur qui s'est engagé dans une démarche collective pour faire face au risque numérique, démarche collective d'autant plus nécessaire au vu des enjeux et de la diversité des acteurs, tant dans leurs champs d'action que dans leurs caractéristiques.

Cet ouvrage a été réalisé avec le soutien de

CERTitude NUMERIQUE

AvantdeCliquer.com
L'humain au cœur de la cybersécurité

PRIX : 21€
9 782494 223066