# Les enjeux de cybersécurité pour le secteur aérospatial

Aspirant (R) Nathan Juglard,
Analyste stratégie et business development chez Thales

Un responsable du département de la Sécurité intérieure a admis en novembre 2017 que l'agence américaine avait été capable de pirater à distance un *Boeing 757* lors d'un test effectué en 2016[1]. Si l'avionneur insiste sur le fait que le piratage s'est limité au système de communication de l'avion et qu'il n'a atteint aucun des contrôles ou des logiciels qui pourraient modifier sa trajectoire de vol[2], c'est toutefois une nouvelle alarmante pour l'industrie aéronautique. Jusqu'à présent, les cyberattaques pernicieuses n'ont réussi qu'à infecter les réseaux au sol mais là où les experts gouvernementaux réussissent à exploiter des failles, des acteurs malveillants le peuvent aussi. En juin 2015, une cyberattaque sur la compagnie aérienne polonaise LOT a ainsi empêché 1 400 passagers d'embarquer à l'aéroport Chopin de Varsovie[3]. Le système de plan de vol de dix avions était alors tombé en panne.

Plusieurs cyberattaques ont révélé les vulnérabilités du secteur aéronautique. Il s'agit pour l'essentiel d'intrusions dans le système de gestion des comptes grands voyageurs[4] ou du piratage de systèmes de ré-

1 Mark Matousek, « A *Boeing 757* was hacked and now DHS is worried more planes could be at risk » in *Business Insider*, 17 novembre 2017, http://nordic.businessinsider.com/planes-might-be-vulnerable-to-being-hacked-by-terrorists-2017-11, consulté le 20/09/2017.

2 Clive Irving et Joseph Cox « Could Terrorists Hack an Airplane? The Governement Just Did », in *The Daily Beast*, 17 novembre 2017. Https://www.thedailybeast.com/could-terrorists-hack-an-airplane-the-government-just-did, consulté le 19/11/2017.

3 Dominique Filippone « Une cyberattaque cloue au sol 1 400 passagers en Pologne », in *le monde informatique*, 22 juin 2015, http://www.lemondeinformatique.fr/actualites/lire-une-cyberattaque-cloue-au-sol-1-400-passagers-en-pologne-61549.html, consulté le 21/10/2017.

4 Il s'agit de British Airways en mars 2015 et de Air India en juin 2016 d'après un rapport de l'IATA.

servations ou de comptes clients[5] des compagnies aériennes. L'impact a été principalement financier et médiatique. Bien qu'elle ne soit pas imminente, la menace est bien réelle du fait de l'interconnexion croissante des systèmes dans le cyberespace définit dans la doctrine française comme un « *espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques* »[6].

Si les États restent les principaux instigateurs des avancées techniques dans le domaine du cyberespace, il en va de la responsabilité de toutes les parties prenantes du secteur aéronautique, y compris les organisations internationales et régionales, les compagnies aériennes, les aéroports et les industriels. Dans le domaine militaire, les opérations aériennes restent étroitement dépendantes des systèmes embarqués dans les aéronefs et des communications par satellites opérés depuis le cyberespace. Ces systèmes ont été conçus dans les années 1980 pour opérer dans un environnement cyber permissif. Cette époque est révolue. Des changements techniques profonds ont contribué à accroître et à accélérer l'interopérabilité ainsi que le partage d'informations en temps réel dans un environnement réseau-centré. Si ces systèmes ne peuvent être reconditionnés intégralement, des mises à jour logiciels peuvent permettre d'accroître leur résilience, c'est-à-dire leur capacité à s'adapter à des conditions contingentes, à se préparer à une perturbation, à y résister, et à s'en remettre rapidement. Cette cyber-résilience repose sur deux piliers : un premier volet technique (protection, capacité de traitement des attaques et de reprise des activités) et un second humain et organisationnel[7].

Des efforts ont ainsi été menés pour identifier et pour réduire les risques qui leur sont liés. Questionner les enjeux de la cybersécurité dans le domaine aérospatial suggère d'interroger l'existence d'une architecture de sécurité commune dans ce domaine, c'est-à-dire de mettre en lumière les progrès qui ont pu être effectués grâce à la collaboration entre les différentes parties

---

5 Les coptes clients de United Airlines (juin 2016), de American Airlines et de Sabre (août 2015) ainsi que de Vietnam Airlines (juillet 2016) ont été piratés d'après un rapport de l'IATA.

6 Agence nationale de la sécurité des systèmes d'informations (ANSSI), https://www.ssi.gouv.fr/entreprise/glossaire/c/, consulté le 30/11/2017 et *Doctrine interarmées DIA-3.40_CYBER (2014)*, CICDE, 2014, http://www.cicde.defense.gouv.fr/IMG/pdf/20160116_np_dia-6_sic-ops_2014__amendee_janvier_2016.pdf, consulté le 30/11/2017.

7 Gérard de Boisboissel, « La cyber-résilience des systèmes d'armes », DSI HS, n° 52, p. 70-74.

prenantes dans un effort de définition et de standardisation des capacités cyber. En réponse aux défis auxquels l'aviation civile est confrontée, plusieurs mesures ont tout d'abord été prises pour faire face aux cybermenaces (I). Assurer la continuité des opérations aériennes dans un cyberespace contesté et constamment menacé est aussi un grand défi pour l'aviation militaire dont les acteurs – industriels comme institutionnels – peinent à se coordonner efficacement sous une bannière unique (II). Le développement du concept de cyber résilience dans les secteurs civil et militaire a entraîné la création de multiples partenariats pour répondre à cette problématique et ce, dès la phase de conception des futurs systèmes aéronautiques (III).

## I - Des vulnérabilités inhérentes au domaine de l'aviation civile

### L'aviation civile en proie à de nombreuses cyberattaques

Les avions de dernière génération sont de plus en plus dépendants des systèmes connectés. Par conséquent, ils sont aussi plus vulnérables aux cyberattaques[8]. La principale menace pour le secteur aérien réside dans les réseaux au sol connectés aux avions, qui contiennent toutes les informations liées au vol. Ces systèmes seraient moins sécurisés que l'avionique embarquée dans les aéronefs selon l'Agence européenne de la sécurité aérienne (EASA)[9]. Bien que l'avionique présente certaines vulnérabilités, pour le moment, le transport aérien n'a été victime que d'attaques perpétrées au sol. Cependant, « *les technologies modernes de communication sont de plus en plus utilisées par les systèmes des avions, ce qui permet à des individus non autorisés d'avoir accès et de compromettre les systèmes avioniques de l'appareil* »[10] note la Cour des comptes américaine, le *Government Accountability Office* (GAO), dans un rapport de 2015. Toutefois, les avions de ligne disposent de liaisons informatiques permanentes avec les compagnies aériennes qui les opèrent, afin de détecter, en amont, des potentielles compromissions des données. La navigation aérienne et les autres systèmes de contrôle sont sé-

8 « Les avions plus vulnérables aux cyberattaques », in *Le Figaro*, 16 avril 2015, http://www.lefigaro.fr/actualite-france/2015/04/16/01016-20150416ARTFIG00424-les-avions-plus-vulnerables-aux-cyberattaques.php, consulté le 30/11/2017.

9 Jorge Valero, « L'UE peine à combattre les cyberattaques dans l'aéronautique », in *EURACTIV.com*, 30 mars 2017, https://www.euractiv.fr/section/politique/news/europe-struggles-to-tackle-cyber-attacks-in-aviation/, consulté le 20/10/2017.

10 *Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen, GAO-15-370*, GAO, 2015, http://www.gao.gov/assets/670/669627.pdf, consulté le 13/09/2017.

parés des systèmes non critiques tels que le divertissement à bord ; le risque de piratage des systèmes critiques reste par conséquent relativement faible.

Un potentiel détournement d'avion par un pirate informatique soulève de nombreux défis. En 2015, le chercheur Chris Roberts a fait l'objet d'un mandat d'arrêt du FBI après avoir prouvé la possibilité de pirater une dizaine d'avions entre 2011 et 2014 grâce à un virus informatique implanté *via* l'*In-Flight Entertainment System* (IFE) – les écrans placés derrière chaque siège qui diffusent le divertissement en vol[11]. Il est important de noter que les industriels ne restent pas pour autant démunis et que parer ces cybermenaces est une préoccupation permanente. Marc Darmon, directeur général adjoint de Thales en charge des activités « *systèmes d'information et de communication sécurisés* » insiste notamment sur la mise en place de « *systèmes de cybersécurité intégrés dès la conception, puis la supervision des systèmes et enfin le chiffrement des données* »[12].

Les systèmes embarqués ne sont pas les seuls vulnérables : leur connectivité croissante avec les satellites de communication renforce la nécessité d'une liaison sécurisée avec l'espace. Ainsi, la nouvelle génération des systèmes de gestion du trafic aérien nord-américains (*NextGen*[13]) et européens (*SESAR*[14]) entérine le passage du radar aux systèmes satellitaires. L'intégration du concept SWIM (*System Wide Information Management*) marque aussi un changement de paradigme dans la gestion de l'information tout au long de son cycle de vie et dans l'ensemble du système de gestion du trafic aérien européen. Il s'agit d'une plate-forme unique qui regroupe les informations critiques comme les changements météorologiques, la position ainsi que les plans de vol de l'avion[15]. Ce système permet d'échanger des données en temps réel entre les pilotes, les opérateurs au sol et les capteurs embarqués. Cette transformation se traduit par des réseaux informatiques et numériques hautement intégrés et interdépen-

11 Martin Untersinger, Damien Leloup et Morgane Tual, « Le FBI s'inquiète du possible piratage d'un avion », in *Le Monde*, 18 mai 2015, http://www.lemonde.fr/pixels/article/2015/05/18/le-fbi-s-inquiete-du-possible-piratage-d-un-avion_4635603_4408996.html, consulté le 09/10/2017.

12 « La résistance contre une cyber-attaque dans l'ADN des avions », in *Bilan*, 21 juin 2017, http://www.bilan.ch/economie/resistance-contre-une-cyber-attaque-ladn-avions, consulté le 23/02/2018.

13 Système de transport aérien de nouvelle génération.

14 *Single European Sky* – Ciel Unique Européen.

15 http://www.eurocontrol.int/swim

dants, tant à bord des avions que dans les installations de contrôle du trafic aérien, ce qui crée des vulnérabilités inhérentes[16].

**L'évolution et enjeux de la coopération internationale dans le secteur de l'aviation commerciale**

« *Les politiques actuelles sont mieux adaptées à des environnements simples, stables et prévisibles qu'à la réalité complexe, changeante et imprévisible de l'environnement cybersécurité actuel* »[17] souligne un rapport de la RAND Corporation sur la cybersécurité dans l'aviation. Selon ce *think-tank* américain, il n'existerait, pour le moment, pas de vision commune, de stratégie, d'objectif, de norme, de modèle de mise en œuvre ou de politique internationale définissant la cyberdéfense pour l'aviation[18]. Le contrôle et la responsabilité de l'évaluation des systèmes militaires en matière de cybersécurité seraient répartis entre de trop nombreuses organisations. Il s'agit pourtant d'une responsabilité partagée par toutes les parties prenantes du secteur aéronautique.

Pourtant, en septembre 2014, les États-Unis ont créé un Centre d'analyse et de partage des informations en matière d'aviation (A-ISAC) qui a pour objectif d'échanger dans le cadre « *d'un réseau de confiance sécurisé* »[19] des informations sensibles à propos d'incidents et des failles potentielles dans le domaine cybernétique. Le groupe comprend les principales compagnies aériennes américaines ainsi que l'avionneur *Boeing* qui interagissent en étroite collaboration avec les agences de renseignement et de sécurité des États-Unis. D'après Elizabeth A. Pasztor, vice-présidente en charge de la sûreté, de la sécurité et de la conformité chez *Boeing* : « *l'élaboration de normes de cybersécurité pour les compagnies aériennes et le partage d'informations entre l'industrie et les gouvernements figurent parmi les mesures de coopération les plus importantes* »[20].

16 Alexander Defazio et Michal Kalivoda, « Defending NATO's Aviation Capabilities from Cyber Attack », JAPCC Journal, n°23, Autome/Hiver 2016, p. 104.

17 Don Snyder, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, Michael Powell « Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles », Rand Corporation, 27 octobre 2015.

18 Alexander DeFazio et Michal Kalivoda, « Defending NATO's Aviation Capabilities from Cyber Attack », JAPCC Journal, n°23, Autome/Hiver 2016, p. 104.

19 Jorge Valero, « L'UE peine à combattre les cyberattaques dans l'aéronautique », in *EURACTIV.com*, 30 mars 2017, https://www.euractiv.fr/section/politique/news/europe-struggles-to-tackle-cyber-attacks-in-aviation/, consulté le 20/10/2017.

20 Jorge Valero, « L'UE peine à combattre les cyberattaques dans l'aéronautique », in *EURACTIV.com*, 30 mars 2017, https://www.euractiv.fr/section/politique/news/europe-struggles-to-tackle-cyber-attacks-in-aviation/, consulté le 20/10/2017.

Si les efforts menés aux États-Unis semblent attester d'une prise de conscience généralisée face aux cybermenaces, en Europe au contraire, les agences gouvernementales et l'industrie peinent à collaborer et à élaborer une approche aussi globale. Le suivi des menaces et la rétro-information sur la cybersécurité restent incomplets, peu coordonnés et insuffisants pour une prise de décision et pour une responsabilisation efficaces. Sous l'impulsion de Patrick Ky, l'AESA s'est emparée du sujet à partir de 2015 : « *croire que le transport aérien est à l'abri de ce genre de menace revient à se voiler la face. C'est un sujet sérieux auquel nous devons nous attaquer* » affirme le directeur exécutif de l'agence européenne[21]. À l'occasion d'une réunion de haut niveau sur la cybersécurité dans l'aviation civile à Bucarest les 8 et 9 novembre 2016, l'AESA a été chargée de mettre en place une plate-forme européenne pour coordonner la définition et la mise en œuvre d'une stratégie européenne dans le domaine de l'aviation. À cette fin, l'AESA, en collaboration avec la *Computer Emergency Response Team* (CERT-EU) de l'Union européenne, ont mis en œuvre, en février 2017, le Centre européen pour la cybersécurité dans l'aviation (ECCSA)[22]. Chargée d'identifier les menaces et les risques cybernétiques, l'AESA a invité toutes les parties prenantes et notamment les constructeurs aéronautiques et les compagnies aériennes à devenir membres de l'ECCSA afin de bénéficier d'une plate-forme de partage de renseignements concernant les cyberattaques. Plus d'un an après sa mise en œuvre, l'ECCSA peine à dégager une feuille de route précise. Sa page Internet se limite à un fil d'actualité avec 11 filtres dédiés à la sécurité dans le domaine de l'aéronautique auxquels n'importe quel utilisateur peut s'abonner. Principale avancée au niveau européen, l'Agence de l'Union européenne pour la sécurité des réseaux et de l'information (ENISA) prévoit de concentrer son cyber exercice annuel, prévu pour 2018, sur la cybersécurité dans le domaine de l'aviation.

### Une interdépendance des systèmes civil et militaire

Le contrôle et la responsabilité de la cybersécurité des systèmes civil et militaire s'étendent à de nombreuses organisations, souvent mal intégrées. Man-

21 Interview avec Guillaume Poupard, directeur général de l'ANSSI – Agence Nationale de la Sécurité des Systèmes d'information, Gerome Billois, Spécialiste en cybersécurité à Solucom, Jean Carlioz, Responsable de la sécurité des systèmes d'information à la DGAC (direction générale de l'aviation civile), « Aviation : les menaces de cyberattaques prises très au sérieux », in France Inter, 16 octobre 2015, https://www.franceinter.fr/emissions/a-code-ouvert/a-code-ouvert-16-octobre-2015, consulté le 29/10/2017.

22 Jorge Valero, « L'UE peine à combattre les cyberattaques dans l'aéronautique », in *EURACTIV.com*, 30 mars 2017, https://www.euractiv.fr/section/politique/news/europe-struggles-to-tackle-cyber-attacks-in-aviation/, consulté le 20/10/2017.

daté par les deux organisations, le groupe *NATO/EUROCONTROL ATM Security Coordinating Group* (NEASCOG)[23] assure la coordination des travaux dans le domaine de la sécurité de la gestion du trafic aérien en Europe pour des intérêts civil et militaire. Ce forum réunit les principaux acteurs de la gestion du trafic aérien tels que les autorités civiles et militaires nationales, les organisations régionales ou internationales comme l'Organisation de l'aviation civile internationale (OACI), l'Association du transport aérien international (IATA), la Conférence européenne de l'aviation civile (ECAC), les associations de pilotes et de contrôleurs professionnels. Cette coopération a pour but de faciliter une approche commune civilo-militaire et une meilleure coordination internationale afin de partager les meilleures pratiques pour protéger efficacement les systèmes de gestion du trafic aérien en cas de cyberattaques. Une montée en puissance de l'OACI est en cours sur le sujet de la cybersécurité au cours du triennat 2017- 2019, à la suite de la résolution A39-19 adoptée par la 39e Assemblée en octobre 2016[24].

En raison des interdépendances entre les systèmes de l'aviation civile et de l'aviation militaire, une cyberattaque ne peut être contenue de manière isolée. Une attaque contre le secteur de l'aviation civile affectera également les capacités militaires car les aéronefs civils comme militaires sont reliés au même écosystème. La gestion du trafic aérien (*ATM – Air Traffic Management* en anglais) comprend, par exemple, des données de plus en plus numérisées et distribuées à travers un réseau d'infrastructures qui connecte des systèmes à la fois civil et militaire. De plus, les infrastructures aéroportuaires et l'aviation commerciale sont des éléments critiques pour les opérations militaires en temps de paix ou dans les zones hors théâtre d'opérations. Une approche globale s'avère donc nécessaire.

## II - Une dépendance accrue des opérations aériennes envers le cyberespace nécessite une meilleure coordination des stratégies nationales

### Des opérations aériennes de plus en plus dépendantes du cyberespace

De plus en plus connectés, les aéronefs militaires compilent et distribuent vers d'autres plate-formes des données sensibles en temps réel. Les appareils de 5e génération sont qualifiés de « *système de systèmes* » dans la mesure où

**23** Site Internet Eurocontrol, https://www.eurocontrol.int/articles/atm-security, consulté le 28/11/2017.

**24** https://oaci.delegfrance.org/Dossier-Cybersecurite-et-transport-aerien consulté le 04/01/2018.

ils combinent « *furtivité, radars à balayage électronique et à antennes actives, manœuvrabilité extrême et d'excellentes capacités de fusion des données ISR* [Intelligence, Surveillance, Reconnaissance][25] ». Cette connectivité les rend, par nature, particulièrement vulnérables aux cyberattaques. Dès 2009, un groupe d'insurgés en Irak a ainsi intercepté en direct des flux vidéos en provenance d'un drone *Predator* américain au moyen d'un logiciel *Skygrabber* acheté sur Internet pour seulement 26 dollars[26]. Un adversaire sophistiqué peut ainsi chercher à exploiter des vulnérabilités dans les logiciels, les systèmes de soutien ou la chaîne d'approvisionnement d'un avion afin d'obtenir des renseignements ou de saboter des opérations.

Les systèmes de maintenance et de planification des missions constituent des nœuds critiques par lesquels un ennemi potentiel peut manipuler des données. Afin de maximiser l'autonomie de sa nouvelle flotte de chasseurs de combat, Israël a par exemple annoncé vouloir équiper ses *F-35I* « Adir »[27] avec son propre système de *Command, Control, Communications and Computing* (C4). Le logiciel israélien, produit par *Israel Aerospace Industries* (IAI), serait une mise à niveau d'un système C4 que l'armée de l'air israélienne exploite déjà sur ses *F-15* et sur ses *F-16*. Israël a affirmé vouloir développer son propre système de cybersécurité et vouloir disposer d'un centre de maintenance implanté nationalement et déconnecté de la plate-forme de maintenance prédictive ALIS (*Autonomic Logistics Information System*) conçue par *Lockheed Martin*. Ce système critique est capable de déterminer en temps réel l'état de l'appareil, de surveiller ses plans de vol et de revoir l'historique complet de chaque avion depuis sa sortie de la chaîne d'assemblage. Israël met aussi l'accent sur la cyber-résilience des systèmes d'armes dès leur conception. Plusieurs responsables israéliens affirment que cette volonté d'autonomie industrielle est dictée par la situation géopolitique du pays[28], qui exige l'indépendance dans l'exploitation et la maintenance de ses avions de chasse. La cybersécurité devient dès lors un enjeu de souveraineté.

**25** Corentin Brustlein, Etienne de Durand, Elie Tenenbaum, *La suprématie aérienne en péril, menace et contre-stratégies à l'horizon 2030,* La Documentation Française, Paris, 2014, p.144.

**26** Ewen MacAskill, « US drones hacked by Iraqi insurgents », in *The Guardian*, 17 décembre 2009, https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked, consulté le 19/11/2017.

**27** « Adir Who? Israel's *F-35i* Stealth Fighters. Defense », in *Industry Daily*, 8 novembre 2017, https://www.defenseindustrydaily.com/israel-plans-to-buy-over-100-f35s-02381/, consulté le 04/10/2017.

**28** Lara Seligman, « Israel Seeks Changes To Its *F-35* Version », in *MRO-Network.com*, 30 juin 2016, http://www.mro-network.com/maintenance-repair-overhaul/israel-seeks-changes-its-f-35-version, consulté le 16/09/2017.

La survivabilité des aéronefs doit être pensée dans le cadre d'une approche globale. « *Chacun des systèmes critiques par lesquels nous accomplissons nos missions essentielles est construit sur les capacités du cyberespace. Les aéronefs, les satellites, les camions et les missiles balistiques intercontinentaux dépendent tous de notre capacité à manœuvrer et à fonctionner dans le cyberespace* »[29] d'après le général de l'*United States Air Force* (USAF), William J. Bender. Un chercheur britannique en cybersécurité, Adam Laurie, a ainsi démontré en 2009 qu'il était possible de pirater un satellite à l'aide d'un simple ordinateur assorti d'un décodeur de satellite de type *Dreambox* et accompagné de quelques logiciels spécialisés[30]. Malgré ces alertes, il faudra attendre 2014 pour qu'une enquête américaine démontre que les flux de communications par satellites peuvent être piratés du fait d'une liaison descendante qui ne serait pas suffisamment sécurisée. « *Une série de systèmes satellitaires cruciaux fabriqués par certains des plus grands sous-traitants gouvernementaux du monde contiennent de graves vulnérabilités qui pourraient être exploitées pour perturber les opérations militaires et les communications de la sécurité aérienne* »[31] d'après la société américaine de sécurité informatique *IOActive* dans un rapport dont les conclusions furent confirmées par la suite par le *Computer Emergency Response Team* (CERT) du département américain de la Sécurité intérieure[32].

Les opérations aériennes deviennent indissociables du cyberespace. La manœuvre militaire interarmées intègre de manière croissante des capacités cyber. « *Les meilleurs garants de la survivabilité restent la résilience, l'intégration interarmes et interarmées ainsi que la manœuvre, le vrai défi étant peut-être surtout d'intégrer à cette dernière les dimensions cyber et spatiales*[33] » affirme Rémy Hémez. Cette intégration s'opère rapidement, d'autant plus que la maitrise de capacités défensives offrent un avantage crucial dans le domaine offensif. L'opération *Orchard*, menée par les forces aériennes israé-

29 Lieutenant Général William J. Bender et Colonel William D. Bryant, *Assuring the USAF Core Missions in the Information Age*, Air & Space Power Journal, Automne 2016.

30 Laurent Lagneau, « Les armes anti-satellites ont changé de nature », in *Opex360*, 18 novembre 2017, http://www.opex360.com/2017/11/18/les-armes-anti-satellites-ont-change-de-nature/, consulté le 18/11/2017.

31 Tom Brewster, « Crucial military satellite systems are vulnerable to hacking, experts says », in *The Guardian*, 17 avril 2014, https://www.theguardian.com/technology/2014/apr/17/military-satellite-system-vulnerable-hacking, consulté le 11/11/2017.

32 *Vulnerability Note VU#250358, Hughes Network Systems Broadband Global Area Network (BGAN) satellite terminal firmware contains multiple vulnerabilities*, 31 janvier 2014, CERT, Software Engineering Institute, Carnegie Mellon University, sponsorisé par le département américain de la Sécurité intérieure.

33 Rémy Hémez, *La survivabilité sur le champ de bataille, entre technologie et manœuvre*, IFRI, Paris, mars 2017, p.11.

liennes en 2007 en Syrie, constitue l'exemple type d'une attaque combinée mêlant attaque aérienne en profondeur, guerre électronique et cyberattaque[34]. L'aviation de chasse, alors constituée d'appareils *F-15C* et *F-16I* non furtifs, a réussi à passer outre des défense antiaériennes avancées afin de bombarder une installation suspectée d'abriter un réacteur nucléaire plutonigène. Une cyberattaque, opérée grâce au ver informatique *Suter*[35] à l'encontre des systèmes de défense syriens, a rendu inopérante la liaison de données entre le radar et son moniteur. Cette attaque combinée souligne la nécessité de considérer la « *manœuvre électronique intégrée* » comme facteur de survivabilité future[36]. Les capacités cyberoffensives vont être intégrées dans la reconstitution, nécessaire mais longtemps retardée[37], des capacités de neutralisation des défenses aériennes ennemies (SEAD)[38], une mission critique pour les forces aériennes occidentales que l'OTAN cherche notamment à mettre en avant dans ses travaux actuels. À moyen terme, les cyber-armes pourraient en effet être considérées comme des capacités clefs des missions SEAD et un vecteur indéniable de supériorité aérienne.

**Un effort d'interopérabilité dans le cadre de l'OTAN**

D'abord à l'initiative des États, cet effort d'intégration des capacités cybernétiques au sein des opérations a été rapidement réapproprié par l'OTAN qui cherche avant tout à renforcer l'interopérabilité dans un soucis d'opérations combinées en coalition. La crise ukrainienne a montré que la cyberdéfense doit être intégrée à un concept opérationnel plus large. En 2014, la déclaration du sommet du Pays de Galles a affirmé que la cyberdéfense faisait partie de la mission fondamentale de l'OTAN qu'est la défense collective et que le droit international s'applique dans le cyberespace. Depuis le sommet de Varsovie en 2016, l'Alliance atlantique a réaffirmé le mandat défensif de l'OTAN et reconnaît que le cyberespace est un domaine d'opérations dans lequel l'OTAN doit se défendre efficacement comme elle le fait dans l'air, sur terre et en mer[39].

---

**34** David Betz, *Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power,* Oxford, Oxford University Press, 2015, p. 148-149.

**35** Thomas Withington, « Code of Mass Disruption », in *Armada International*, octobre 2012.

**36** Christian Malis, *Guerre et stratégie au XXIe siècle*, Fayard, 2014, p. 166.

**37** Olivier Zajec, « Le trou capacitaire et opérationnel de la SEAD/DEAD. Bientôt dans les standards européens ? », DSI, n°64, novembre 2010, p. 79-83.

**38** Élie Tenenbaum, « Le rôle stratégique des forces terrestres », *Focus stratégique*, n° 78, Ifri, février 2018, p.63.

**39** *Paragraphe 70 du Communiqué du Sommet de Varsovie* publié par les Chefs et les États participant à la réunion du Conseil de l'Atlantique Nord à Varsovie les 8-9 Juillet 2016.

Les implications de la reconnaissance du cyberespace comme son propre domaine a déplacé l'orientation de l'Alliance d'une « *assurance de l'information* »à une « *assurance de la mission* »[40]. Soulignant l'importance de leur coopération, l'OTAN et l'Union européenne (UE) ont signé, en février 2016, un arrangement technique sur la coopération en matière de cyberdéfense. Dernière avancée en la matière : à l'occasion d'une réunion des ministres de la défense de l'Alliance atlantique les 8 et 9 novembre 2017, le secrétaire général de l'OTAN, Jens Stoltenberg, a affirmé vouloir « *intégrer les capacités nationales des alliés en matière de cyber dans les missions et les opérations de l'OTAN* ». Par ailleurs, il a fait part de la volonté de l'OTAN de créer un « *nouveau centre d'opérations cyber* » dans le cadre de la refonte de la structure de commandement.

Depuis mai 2016, le comité Aviation de l'OTAN contribue à la résilience du système global de l'aviation en entamant un effort de définition et de standardisation. L'OTAN a défini trois domaines dans lesquels des vulnérabilités pourraient se produire : l'informatique traditionnelle, la technologie opérationnelle et les plates-formes et senseurs[41]. La cybersécurité est alors considérée comme une combinaison de mesures de défense en profondeur, de résilience et de défense avancée au cœur même de l'architecture-système[42]. « *Chaque approche est nécessaire et aucune n'est suffisante en soi* » selon Alexander Defazio, ancien colonel de l'USAF[43]. L'OTAN s'inspire des avancées de l'*Air Force* en matière de cyberdéfense et notamment des rapports de la générale Ellen Pawlikowski, commandant de l'*Air Force Material Command*[44], des écrits du général William J. Bender et du Colonel William Bryant, directeur-adjoint

**40** De même que pour le terme « *cyberspace* », l'OTAN n'est pas encore convenue d'une définition officielle du terme « *assurance de mission* »(*mission assurance*). Dans sa stratégie relative à l'assurance de mission (*Mission Assurance Strategy*), le Département de la Défense des États-Unis définit le terme comme suit : « *[a] protéger ou garantir le fonctionnement permanent et la résilience des capacités et des ressources (y compris le personnel, les équipements, les installations, les réseaux, l'information et les systèmes d'information, les infrastructures et les chaînes d'approvisionnement) qui constituent des éléments cruciaux des fonctions essentielles aux missions (Mission-Essential Functions) du Département de la Défense* », *Mission Assurance Strategy*, Département de la Défense des États-Unis, 2012 p.1, in Brad Bigelow, *Mission Assurance: Shifting the Focus of Cyber Defence*, NATO CCD COE Publications, Tallinn, 2017.

**41** En anglais : « Traditional IT, Operational Technology and Platforms & Weapons ».

**42** Colonel William Bryant, directeur adjoint de la Task Force Cyber USAF « Mission Assurance through Integrated Cyber Defense », *Air and Space Power Journal*, hiver 2016.

**43** Alexander Defazio et Michal Kalivoda, « Defending NATO's Aviation Capabilities from Cyber Attack », JAPCC Journal, n°23, Autome/Hiver 2016, p. 104.

**44** Sergent Christopher Gross, « AFMC commander says cyber threats are real, need to get ahead of them , in *Air Force News Service*, 21 septembre 2016, http://www.af.mil/News/Article-Display/Article/951715/afmc-commander-says-cyber-threats-are-real-need-to-get-ahead-of-them/, consulté le 23/11/2017.

du groupe de travail Cyber de l'*US Air Force*[45]. Face à cette réalité complexe, l'USAF préconise un processus en trois phases : analyser l'écosystème de l'aviation militaire pour identifier les potentielles vulnérabilités, développer des standards militaires pour la cybersécurité dans le domaine de l'aviation et mettre en œuvre une méthodologie pour une évaluation à long terme et une amélioration continue de ces processus[46].

L'Alliance atlantique contribue ainsi à assurer la continuité des opérations aériennes dans le domaine du cyberespace, un environnement contesté et constamment menacé. L'OTAN doit prendre en considération la sécurité des aéronefs et ainsi mieux répondre aux défis de la cybersécurité lors de la mise en œuvre d'exercices qui impliqueraient une cyberattaque pouvant compromettre les réseaux au sol intégrés aux aéronefs. Cette situation est considérée comme préoccupante du fait de « *la dépendance accrue des forces de l'OTAN aux systèmes de communication et de localisation par satellite, et ce parallèlement à l'investissement de la Russie et de la Chine dans ce domaine* »[47]. Plusieurs *scénarii* sont envisageables comme la perte de GPS et son impact sur la navigation mais aussi sur l'utilisation de munitions dites « *intelligentes* ». Le 26 janvier 2018, l'USAF a donné le coup d'envoi de l'exercice annuel *Red Flag* sur la base aérienne de Nellis au Nevada. Cet entrainement d'une ampleur jusque-là inégalée aura aussi la particularité de mettre l'accent sur le brouillage des signaux GPS[48].

## III - Le concept de cyber résilience à travers des partenariats innovants avec les industries

### Une coopération renforcée entre les secteurs public et le privé

Le développement du concept de cyber-résilience des infrastructures à l'échelle nationale a suscité de multiples initiatives qui permettent de repenser

45 Lieutenant Général William J. Bender et Colonel William D. Bryant « Assuring the USAF Core Missions in the Information Age », *Air & Space Power Journal*, Automne 2016.

46 *Urgent Need for DoD and FAA to Address Risks and Improve Planning for Technology that Tracks Military Aircraft*, Rapport GAO-17-509C, États-Unis, Government Accountability Office, Juillet 2017.

47 « Le bel avenir de la guerre électronique », in *TTU*, 20 avril 2016, https://www.ttu.fr/bel-avenir-de-guerre-electronique/, consulté le 14/03/2018.

48 Laurent Lagneau, « Les participants à l'exercice aérien Red Flag 2018-1 devront se passer du système GPS », in *Opex360*, 28 janvier 2018, http://www.opex360.com/2018/01/28/participants-a-lexercice-aerien-red-flag-2018-1-devront-se-passer-systeme-gps/, consulté le 28/02/2018.

la manière dont les secteurs public et privé peuvent travailler en partenariat. En 2007, à la suite des cyberattaques en Estonie, l'OTAN a décidé de créer un centre spécialisé dans le domaine de la cyberdéfense. Le Centre d'excellence pour la cyberdéfense en coopération de l'OTAN[49] basé à Tallinn est ainsi un « *centre de recherche et d'entraînement accrédité par l'OTAN s'occupant de formation, de consultation, de retour d'expérience, de recherche et de développement en matière de cyberdéfense* »[50]. C'est dans le cadre du Centre d'excellence que dix-neuf experts ont rédigé le Manuel 2.0 de Tallinn sur le droit international applicable aux opérations cybernétiques. Il s'agit d'une ressource influente pour les conseillers juridiques qui traitent des problèmes cybernétiques.

Le renforcement des partenariats public-privé à travers des pactes de coopération cybernétiques est l'une des priorités des gouvernements qui profitent de l'expertise des entreprises les plus avancées en la matière. D'après Erki Kodar, sous-secrétaire d'État Estonien à la Défense : « *la plupart des innovations se produisent dans le secteur privé ou dans le milieu universitaire* »[51] d'où l'importance d'une coopération renforcée entre les secteurs public et privé. Cette forme de coopération, entamée d'abord à l'échelle des nations, a été ensuite imitée par l'OTAN et l'UE dans un cadre multilatéral. Les pays membres de l'OTAN ont par exemple intensifié leur coopération avec l'industrie et le monde universitaire dans le cadre du cyber partenariat « *OTANindustrie* » (NCIP), conçu pour aider les nations à suivre le rythme rapide des changements technologiques et pour favoriser l'innovation. « *Ce partenariat, qui s'appuie sur les structures existantes, réunit des entités OTAN, des centres nationaux d'alerte et de réaction aux attaques informatiques* (CERT) *ainsi que des représentants d'industries des pays membres de l'OTAN* »[52].

Conscients que des partenariats stratégiques jouent un rôle clé dans la résolution des défis cybernétiques, les Alliés continuent de collaborer avec

**49** *La cyberdéfense à l'OTAN Juillet 2016*, OTAN Division Diplomatie Publique, juillet 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160705_1607-factsheet-cyber-defence-fre.pdf, consulté le 14/09/2017.

**50** *La cyberdéfense à l'OTAN Juillet 2016*, OTAN Division Diplomatie Publique, juillet 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160705_1607-factsheet-cyber-defence-fre.pdf, consulté le 14/09/2017.

**51** Interview avec Erki Kodar, effectuée le 19 octobre 2017 par Nathan Juglard pendant NIAS17 à Mons.

**52** *La cyberdéfense à l'OTAN Juillet 2016*, OTAN Division Diplomatie Publique, juillet 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160705_1607-factsheet-cyber-defence-fre.pdf, consulté le 14/09/2017.

l'industrie et avec les universités. Ces partenariats sont déterminants pour assurer un contrôle effectif tout au long du cycle de vie des composants de l'aéronef et des systèmes qui l'entourent. Il faut cependant garder à l'esprit que même un aéronef de dernière génération ne peut être invulnérable à une cyberattaque pas plus qu'il ne le serait lors d'un combat aérien contre un autre aéronef. Par conséquent : les opérateurs du cyberespace doivent aller au-delà de la question de « *comment sécuriser au mieux ce système contre les attaques ?* » et réfléchir à « *comment opérer dans un environnement cyber-contesté où l'ennemi va passer au travers d'au moins une partie des défenses* » souligne le général William J. Bender de l'USAF[53].

**La nécessité de repenser la chaîne logistique d'amont en aval**

La générale Ellen Pawlikowski a souligné sept domaines essentiels pour mieux sécuriser les structures de commandement et de contrôle (C2) dont dépendent les aéronefs. Une initiative clef de l'USAF est d'intégrer des dispositifs de cybersécurité dès les premières phases de développement : « *nous examinons beaucoup plus tôt dans le cycle de vie de ces systèmes, non seulement leur sécurité, mais aussi leur interface avec d'autres éléments du réseau. Nous voulons intégrer la cybersécurité plus tôt dans le processus* »[54] a-t-elle affirmé. L'ensemble des sous-traitants doit être inclus dans ce processus, les grands groupes comme les PME : « *l'enjeu est pour les plus petits d'avoir les moyens de se protéger* »[55] souligne Pascal Pincemin, associé chez Deloitte France, responsable du secteur Aéronautique et Défense.

Dans un rapport de 2015 intitulé « *Améliorer la cybersécurité des systèmes militaires des forces aériennes des États-Unis tout au long de leur cycle de vie* », la RAND Corporation[56] établit une liste de recommandations destinées à améliorer la résilience des systèmes aéronautiques. Les experts affirment que, de manière générale, les avionneurs devraient maximiser la flexibilité de leurs

53 Lieutenant Général William J. Bender et Colonel William D. Bryant « Assuring the USAF Core Missions in *the Information Age* », *Air & Space Power Journal*, Automne 2016.

54 Sergent Christopher Gross, « AFMC commander says cyber threats are real, need to get ahead of them , in *Air Force News Service*, 21 septembre 2016, http://www.af.mil/News/Article-Display/Article/951715/afmc-commander-says-cyber-threats-are-real-need-to-get-ahead-of-them/, consulté le 23/11/2017.

55 Gil Roy, « Cyber attaque : y-a-t-il un administrateur sûreté à bord ? » in *Aerobuzz*, 28 juin 2017, https://www.aerobuzz.fr/industrie/cyber-attaque-y-a-t-il-un-administrateur-surete-a-bord/, consulté le 11/11/2017.

56 Don Snyder, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, Michael Powell « Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles », Rand Corporation, 27 octobre 2015.

systèmes en construisant délibérément une capacité excédentaire redondante et inefficace. Paradoxalement, la surface d'attaque des systèmes doit être réduite : il s'agit d'éliminer les capacités inutiles du matériel et des logiciels, de s'assurer que les tests de sécurité adéquats ont bien été effectués et de segmenter leurs réseaux et leurs systèmes en enclaves distinctes. L'organisation récurrente de formations et d'exercices permet de garantir la flexibilité du personnel ainsi que leur responsabilisation face aux cybermenaces. Enfin, les autorités militaires doivent répondre dynamiquement aux attaques grâce à une meilleure connaissance de la situation, à un commandement et à un contrôle (C2) efficace et à des moyens de défense actifs. Seule la combinaison de ces approches permettra aux systèmes de résister aux attaques dans le cyberespace.

La cybersécurité doit couvrir l'intégralité du cycle de vie d'un système. Une flotte entière peut être clouée au sol parce qu'un *bug* informatique aura été introduit dans un composant, des années plus tôt. Afin de garantir que les données d'un système opérationnel ne soient pas altérées, la mise en œuvre régulière de tests d'intrusions grâce à des *Red Team* (un groupe d'attaquants amicaux qui tentent de pénétrer les systèmes pour trouver leurs vulnérabilités et leurs faiblesses) pourrait progressivement devenir la norme au sein des forces aériennes. Airbus a ainsi travaillé en collaboration avec une équipe de *hackers* qui effectuent des « *tests de pénétration* »[57] sur les systèmes. Les failles découvertes lors de ces tests ont permis de construire l'architecture sécurisée de l'*A380*.

## Conclusion

L'industrie aéronautique est largement dépendante des systèmes informatiques, que ce soit les réseaux au sol, dans les airs ou dans l'espace. Des brèches de sécurité dans les systèmes de gestion des compagnies aériennes, des avions infectés à distance par des virus, des drones détournés de leurs objectifs suite à un piratage malveillant… les cybermenaces se sont récemment multipliées. Retards des vols, impact médiatique négatif pour les compagnies aériennes mais surtout une prise de conscience des autorités publiques, des régulateurs et de l'industrie face à une réalité alarmante.

Aujourd'hui encore, l'axiome du général Giulio Douhet, théoricien de la guerre aérienne reste valide : « *la victoire appartient à ceux qui anticipent les*

**57** « La résistance contre une cyber-attaque dans l'ADN des avions », in *Bilan*, 21 juin 2017, http://www.bilan.ch/economie/resistance-contre-une-cyber-attaque-ladn-avions, consulté le 23/02/2018.

*mutations des caractéristiques de la guerre, et non a ceux qui attentent de s'adapter une fois les mutations devenues réalités* ». Un manque de coordination des parties prenantes a rendu difficile la définition d'une approche holistique dans le secteur aéronautique et la mise en œuvre de normes ou de standards à l'échelle internationale. D'importants progrès ont néanmoins déjà été réalisés tant à l'échelle des nations qu'au niveau international. Toutefois, le contrôle et la responsabilité de la cybersécurité des systèmes militaires s'étendent à de nombreuses organisations souvent mal intégrées. Pour les industriels, le suivi et la rétro-information sur la cybersécurité sont performants mais demeurent incomplets, peu coordonnés et insuffisants pour une prise de décision et pour une responsabilisation efficaces.

Face à cette situation, les différentes parties prenantes, sous l'impulsion de l'ICAO et de l'IATA dans le secteur civil et de l'OTAN et de l'UE dans le domaine militaire, ont progressivement développé une stratégie reposant sur trois piliers. Il s'agit tout d'abord de comprendre, de définir et dévaluer les menaces et les risques des cyberattaques, pour ensuite mettre en place une réglementation adéquate et enfin d'instituer des mécanismes pour améliorer la coopération au sein de l'industrie, avec le soutien des gouvernements. Bien qu'encore au stade embryonnaire, cette coopération peut accoucher d'innovations surprenantes. Aux États-Unis par exemple, la DARPA travaille sur des applications *blockchain* en se concentrant sur son potentiel de plate-forme de transaction et de messagerie militaire non-piratable. La technologie *blockchain* est ainsi en cours d'évaluation pour des applications dans le domaine de la cybersécurité spatiale : elle permettrait de garantir l'authenticité des informations et des données spatiales, et de certifier leur intégrité à chaque étape du traitement des données[58].

**58** Luca Del Monte et Géraldine Naja, *Hack-My-Sat : Cyber-Threats and the Digital Revolution in Space,* in Laurence Nardon, *European Space programs and the digital challenge, IFRI, Paris, novembre 2017.*