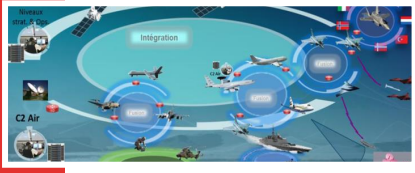
DEFENSE
& industries

Fondation pour la recherche stratégique
n°13 - Juin 2019

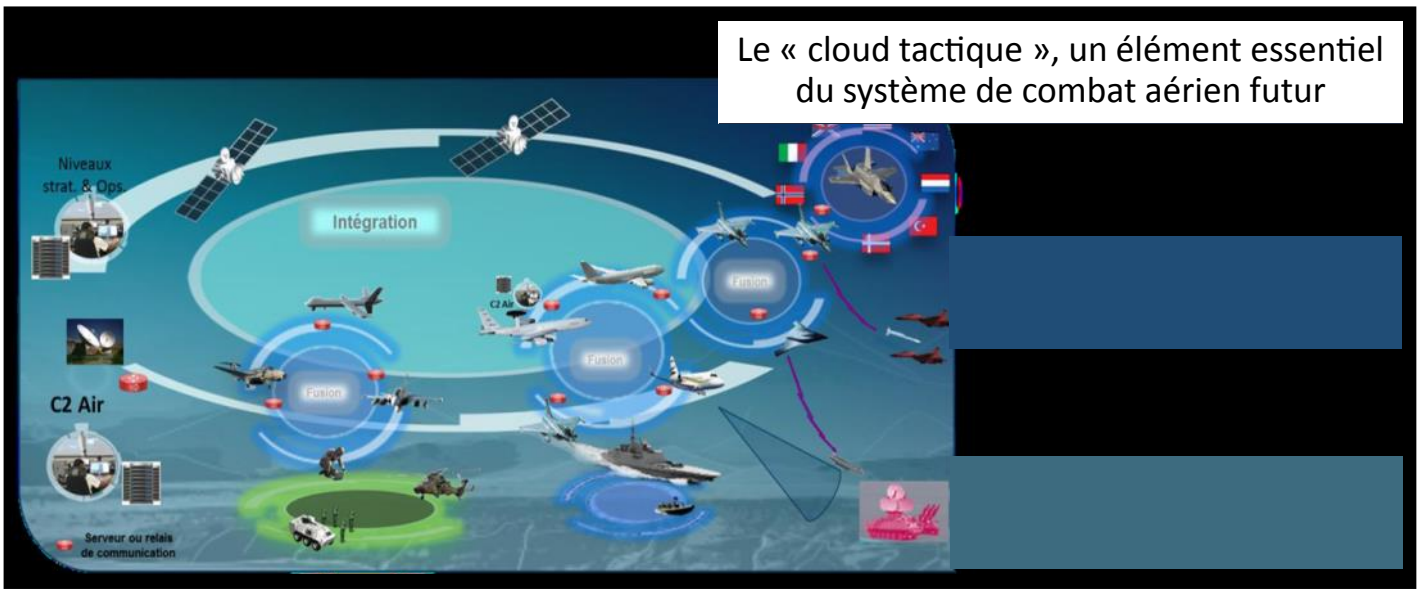


Rédacteur en chef de la revue *Défense & Industries*
Hélène Masson, maître de recherche, en charge du pôle Défense & Industries
h.masson@frstrategie.org

Équipe de rédaction
Kévin Martin, chargé de recherche, pôle Défense & Industries
Marie-France Lathuile, ingénieure de recherche en information
Fabien Herbert, chargé de communication numérique

www.frstrategie.org

Le « cloud tactique », un élément essentiel du système de combat aérien futur



Le système global de combat aérien vue par l'armée de l'air – source : David Pappalardo, « Combat collaboratif aérien connecté, autonomie et hybridation Homme-Machine : vers un 'Guerrier Centaure' ailé ? », DSI, janvier-février 2019, p.71

Au croisement de l'exigence opérationnelle et de l'opportunité technologique, le « cloud » tactique ou « cloud de combat », est la dernière transcription de la *Network Centric Warfare* conceptualisant depuis 20 ans la supériorité informationnelle et décisionnelle découlant de la mise en réseau. Il consiste à pousser jusqu'au cockpit les capacités les plus avancées de nos réseaux numériques, selon les technologies des cloud commerciaux, afin de renforcer l'efficacité, l'efficience et la résilience de la puissance aérienne dont il transformera les fonctions opérationnelles. Le cloud tactique doit devenir une pièce essentielle de notre système de combat aérien futur et, au-delà, de l'ensemble de nos forces armées, tout particulièrement en raison de leur volume compté. Encore faut-il que ses architectes parviennent à surmonter les énormes défis liés à son développement : la cybersécurité, tant le cloud accroît l'exposition de la force aux menaces cyber-électroniques, connectivité, interopérabilité, normes, partage de l'information.

Le système de combat aérien futur (SCAF) est le grand projet devant structurer les puissances aériennes de combat française, allemande et espagnole à partir de la décennie 2040. Rappelons ici que son cœur sera constitué d'un *Next Generation Weapon System*, comprenant l'avion de combat de nouvelle génération *(Next Generation Fighter, NGF*) sous le leadership de Dassault Aviation, qui doit succéder au Rafale, et de nouveaux autres éléments (drones, munitions, etc.). Cependant, le SCAF va au-delà d'un renouvellement de plateformes et de munitions. Le général Mercier, alors Chef d'état -major de l'armée de l'Air (CEMAA), expliquait ainsi en 2015 que « […] *pour le système de combat aérien futur [SCAF] que l'armée de l'Air conceptualise, le mot-clef est bien "système". Car il ne s'agira ni d'un avion piloté, ni d'un drone, mais d'un système de systèmes intégrant, au sein d'un véritable cloud, des senseurs et des effecteurs de différentes natures et de différentes générations* »[1].

Cet article propose de décrire ce que recouvre cette notion de cloud au profit du SCAF, en quelle mesure elle diffère des techniques actuelles de mise en réseau, les démarches incrémentales vers sa réalisation et d'en présenter les plus-values potentielles mais aussi les défis auxquels se heurte sa réalisation.

La notion de cloud

La notion de « *cloud computing* » illustre à la base une forme plus ou moins prononcée d'externalisation ou de mutualisation des capacités informatiques employées par un utilisateur. Si la notion émerge avec la location par Amazon de ses capacités de calcul à l'orée du millénaire, elle renvoie à des concepts et des technologies développées en réalité depuis le début de l'informatique. Il existe de multiples définitions du « cloud » mais la plus couramment rencontrée est celle donnée en 2011 par la *National Institute of Standards and Technology* américaine : « *Le cloud computing est un modèle permettant un accès réseau omniprésent, pratique et à la demande à un pool partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement fournies et mises à disposition avec un minimum d'effort de gestion ou d'interaction avec le fournisseur de services. Ce modèle de cloud computing est composé de cinq caractéristiques essentielles, de trois modèles de services et de quatre modèles de déploiement* »[2]. Les cinq caractéristiques sont le service à la demande, l'accès de l'utilisateur aux ressources par le réseau, la mise en commun de ces ressources avec d'autres utilisateurs, la flexibilité de ces ressources et un service mesuré. Les modèles de service renvoient à ce qui est effectivement partagé. Les trois principaux sont :

- IaaS (*infrastructure as a service*) : le partage concerne le réseau et les infrastructures (serveurs notamment). C'est le plus courant actuellement ;
- PaaS (*Platform as a service*) : le partage s'étend également aux plateformes informatiques, à leurs systèmes d'exploitation et logiciels de base ;
- SaaS (*Software as a service*) : enfin, le partage peut porter sur les données elles-mêmes et les applications utilisées par l'opérateur. C'est même techniquement le modèle le plus simple (cf. l'utilisation d'une messagerie Gmail ou Yahoo).

Dans le domaine commercial, le *cloud computing* répond surtout aux mêmes finalités économiques et managériales

que les autres externalisations : l'entreprise n'a plus à gérer l'évolution et la sécurité de ses capacités informatiques, leur « plasticité » en fonction de la variabilité de ses besoins, une main d'œuvre de techniciens dédiés, etc.

Le recours au cloud par les armées

Le recours au cloud pour les systèmes d'information et de communication (SIC) militaires est entamé depuis une dizaine d'années. Les Américains sont les premiers à franchir le pas. La migration vers le cloud est ainsi un des piliers de la refonte complète de l'architecture des systèmes d'information et de communication américains, le *Joint Information Environment* (JIE), menée depuis 2010 par le biais d'une vaste fédération d'initiatives coordonnée par le *Chief Information Officer* (CIO) du Pentagone et la *Defense Information Systems Agency*. Selon Teri Takai, le CIO qui a lancé le projet, l'objectif du JIE est triple : rendre la défense plus efficace, plus sécurisée contre les menaces cyber et réduire les coûts[3]. Concrètement, les efforts ont porté sur la « consolidation », donc la réduction massive du nombre de centres de données, le développement d'une architecture de sécurité unique et d'un socle de services communs et la mise sur pied d'une structure unique de gestion opérationnelle des réseaux. La dernière stratégie du DoD pour le développement du cloud montre cependant, sans réelle surprise pour l'observateur de la défense américaine, que les efforts entrepris ces dernières années sont loin d'être satisfaisants : manque de plasticité donc d'efficience, extrême disparité voire inadaptation des solutions qui ont proliféré. L'approche du Pentagone est maintenant de développer un cloud généraliste de type IassS/PaaS, le *Joint Enterprise Defense Infrastructure* (JEDI), et des cloud spécifiques (*Fit-for-Purpose*) en cas de besoin[4], une démarche remise cependant en cause par le Congrès. Notre ministère des Armées a lui aussi élaboré son propre cloud privé, principalement pour les tâches de son administration centrale[5].

La notion de « cloud tactique »

Ces premières migrations vers le cloud ont concerné l'infrastructure informatique fixe, celles des grands états-majors, des agences, éventuellement des PC déployables dans le cas américain. Le développement de cloud s'étendant aux ramifications tactiques, celles des unités et plateformes, commence également à émerger. Ces derniers sont expérimentés depuis plusieurs années par les forces américaines et en cours de conceptualisation dans nos armées. Dans son *Ambition numérique*, le MINARM explique que « [garantir la supériorité opérationnelle et la maîtrise de l'information sur les théâtres d'opérations] *nécessite une transformation importante de nos architectures opérationnelles pour mettre la donnée au cœur du futur combat en cloud. La maîtrise des architectures des chaînes fonctionnelles de bout en bout devra garantir l'interopérabilité, la résilience et la sécurité numérique (cybersécurité) de l'ensemble des systèmes et le partage de l'information entre tous les opérationnels* »[6]. Là encore, il n'existe pas une unique définition d'un « cloud de combat » ou « cloud tactique » (facilité de langage dans la mesure où de multiples nœuds se situent loin de la frange tactique). En réalité, à l'instar des réseaux actuels, tout dépend des organisations et des spécificités opérationnelles des différents milieux même si nombre de conceptions et de solutions techniques sont transposables d'une composante de force à l'autre.

Dans le domaine des opérations aériennes, vocation du SCAF, le promoteur le plus vibrant du cloud aura été le général à la retraite David Deptula, ancien planificateur de *Desert Storm*, inventeur du concept des *Effects-Based Operations* et infatigable avocat de l'*airpower* à la tête du Mitchell Institute. Dès 2013, il expose la notion de « *combat cloud* », un « *complexe ISR/frappe/manœuvre/soutien qui pourrait ouvrir la voie à une architecture entièrement différente pour la conduite de la guerre* ». Deptula considère ce cloud comme devant être le moteur non pas uniquement de la puissance aérienne mais de la synergie des 5 domaines de lutte (*cross-domain synergy*) qui est le mantra des conceptions opérationnelles américaines depuis 10 ans[7].

L'*Air Combat Command* de l'US Air Force élabore en 2016 un premier concept opérationnel de *combat cloud* de la puissance aérienne. Il le définit comme « *un réseau maillé global pour la distribution des données et le partage de l'information dans un espace de combat, où chaque utilisateur, plateforme 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* »[8]. Comme l'explique l'US Navy, elle-même très avancée – voire la plus avancée – sur le sujet, le cloud tactique ne réside pas en soi dans l'externalisation du stockage de données et de l'accueil des applications, ou dans la virtualisation des serveurs, qui caractérisent un cloud commercial, même si ces éléments peuvent être mis en œuvre. Il s'agit surtout de stocker et d'accéder à un volume massif de données, de les héberger sur des sources multiples et disparates dans un environnement commun et de fournir les outils permettant d'en extraire une signification, de corréler les données émanant de multiples domaines, en utilisant notamment les techniques de *big data* et de l'intelligence artificielle.

Le cloud tactique doit ainsi permettre aux plateformes et unités d'accéder à un outil autrefois uniquement disponible aux opérateurs de niveau stratégique[9].

Le cloud tactique, nouvelle traduction de la vision exprimée par le concept de *Network Centric Warfare*

A la lecture de ces définitions, le cloud tactique n'apparaît être ni plus ni moins que la poursuite de la mise en œuvre du concept de *Network Centric Warfare* (NCW) élaboré en 1998 par l'amiral Cebrowski et John Gartska, devenu le concept central de la « *Transformation* » des forces américaines pendant plusieurs années. Rappelons que la NCW postule que la mise en réseau des capteurs, des éléments de commandement et contrôle (C2) et des effecteurs offre un avantage décisif dans le combat.

En 2004, le Pentagone redéfinissait un nouvel ensemble de règles caractérisant le combat interarmées réseau-centré :

- La recherche primordiale de la **supériorité informationnelle sur l'adversaire** ;
- Le développement d'une **conscience et d'une compréhension partagée de la situation** entre l'ensemble des acteurs ;

- **L'auto-synchronisation** des plus bas échelons tactiques grâce à cette conscience situationnelle partagée ;
- La réalisation plus rapide **d'opérations non-linéaires**, l'obtention des effets recherchés par une force « démassifiée » ;
- **La compression des niveaux de la guerre** résultant de **l'intégration des opérations, du renseignement** (plus précisément de l'*Intelligence, Surveillance and Reconnaissance*, ISR) **et du soutien** et de la **fusion des capacités interarmées au plus bas échelon tactique** (ce que l'on rebaptise dernièrement les opérations « multidomaines ») ;
- **la vitesse du commandement** par la compression de la boucle « *sensor-to-decision-maker-to-shooter* » qui traduit la supériorité informationnelle en **supériorité décisionnelle** sur l'adversaire[10].

Certes, les implications par trop emphatiques de cette mise en réseau envisagées par les tenants de la « Révolution dans les affaires militaires », ont sombré dans les sables de l'Irak et de l'Afghanistan. Il n'en reste pas moins qu'au niveau tactique, une grande partie de ces postulats est amplement confirmée par les faits. Dès cette époque, les thuriféraires de la NCW conçoivent un autre cycle de gestion de l'information : le *Task, Post, Process, Use* (TPPU), dans lequel les capteurs orientés pour une mission, postent leurs données sur le réseau, les utilisateurs les retirent, les traitent et les utilisent en fonction de leurs besoins propres. C'est peu ou prou ce qui est envisagé dans les cloud tactiques.

Les LDT actuelles permettent une première réalisation de la NCW mais constituent un carcan limitant les informations partagées

L'actuelle mise en réseau des moyens aériens repose sur des systèmes de liaison de données tactiques (LDT), principalement la fameuse liaison 16 (L16) qui permet l'interopérabilité multinationale, même si les Américains disposent de plusieurs autres LDT. Cette L16 a déjà réellement transformé les opérations aériennes. Elle a ainsi permis l'identification de tous les aéronefs amis en étant dotés et l'élaboration d'une image unique de la situation air sur un théâtre. Elle rend la conduite de ces opérations beaucoup plus flexible. Depuis maintenant plus de 10 ans, les pilotes occidentaux reçoivent couramment durant le vol des informations critiques sur leur mission, voire des changements d'assignation d'objectifs.

Ces échanges n'en restent pas moins limités à bien des égards. La liaison 16 recouvre en fait deux choses différentes : d'une part, un réseau de transmission (liant les terminaux embarqués sur les différentes plateformes) mais aussi un catalogue d'environ 50 messages opérationnels formattés (la messagerie J, laquelle couvre le positionnement des plateformes, l'alerte, la surveillance de pistes, le contrôle et assignation des missions, etc.)[11] et une capacité « free text » selon les plateformes[12].

Or, cette liaison 16 a été conçue durant les années 1970. Elle connait certes de multiples améliorations : extension de sa portée par les communications par satellite, passerelles multi-réseaux avec d'autres LDT, *Network Enabled Weapons* (NEW, l'inclusion des munitions sur la L16 pour le guidage sur objectifs mobiles), etc. Cependant, un réseau L16 reste très complexe à planifier dans le cadre de chaque engagement et nécessite en conduite une méticuleuse gestion par la *Joint Data Link Management Cell*[13]. Ce n'est donc pas un *Mobile Ad Hoc Network* comme par exemple nos réseaux de téléphonie. Sa bande passante est en outre très limitée et sa latence élevée. Les capacités d'échange permises par ces messageries de LDT sont, elles aussi, limitées. Le général Breton, qui dirige le programme SCAF, explique qu'« *un aspect important de l'innovation sur le SCAF sera la mise en réseau : actuellement sur Rafale* [dans sa configuration actuelle] *le pilote se sert principalement de ses propres capteurs et d'un peu d'informations apportées par le réseau* »[14]. Ainsi, de multiples données glanées par l'avion ne sont pas partagées, comme les données de son détecteur Spectra ou de son capteur optronique[15].

Le cloud tactique, une architecture centrée sur les données opérationnelles

Le cloud renouvelle cette problématique de la NCW à l'ère des fameuses « *big data* », caractérisées par les 5V : leur volume, leur « vélocité » (leur écoulement en flux continu), leur variété (dans leur formatage), leur véracité et leur valeur. Les utilisateurs tactiques devraient ainsi être submergés à leur tour par le « tsunami de données », évoqué par le général Ferlet, directeur du renseignement militaire. Cette progression des *big data* au niveau tactique s'explique par la diffusion de plusieurs technologies jusqu'au niveau des plateformes et unités déployées :

- Les capacités des capteurs ;
- L'accroissement du volume de données transférables à émission identique ;
- La flexibilisation dans l'utilisation du spectre électromagnétique par les techniques « *software defined* » ;
- La capacité croissante de stockage informatique sur un volume donné ;
- Les logiciels d'extraction et de traitement automatisé de données qui reposeront sur une part croissante d'intelligence artificielle fondée sur le *machine learning*. Ils permettront (en théorie du moins…) des analyses « prédictives » de la situation opérationnelle ;
- Les outils et architectures de « fusion » de données hétérogènes, reposant non plus sur la simple corrélation ou sur le mélange d'informations mais sur l'intégration de données brutes émanant de capteurs embarqués ou déportés. C'est la « *fusion warfare* » que pratiquent déjà les patrouilles d'appareils de cinquième génération (F-22 et F-35) …de façon isolée[16] ;
- La diversité et la rapidité de développement des applications.

Ces technologies mènent à un changement de paradigme : passer d'une logique où le réseau dicte le volume mais aussi le format des données échangées à une logique où ce sont les données, dans leur extrême variété, qui deviennent le paramètre principal. En 2010, le président du comité des Chefs d'état-major *(Chairman du Joint Chiefs of Staff)* américain, alors le général Dempsey, mettait ainsi en exergue la

transition vers un environnement *Data-Centric*[17]. L'Air Force préfère désormais parler de cycle « *data-to-decision* » plus que de « *sensor-to-shooter* »[18].

Si l'on extrapole les conceptions de l'expérimentation de l'US Navy, *Data Focused Naval Tactical Cloud*[19], les données qui seraient échangées au sein d'un cloud de combat aérien seraient les suivantes :

- Les données des capteurs (non seulement des radars, mais aussi des systèmes d'alerte, ESM, des détecteurs optroniques) des différentes plateformes ;
- Les productions de renseignement préalablement élaborées ;
- D'autres données critiques sur l'environnement opérationnel (météo, topographie, etc.) ;
- Les données sur la disponibilité et les performances instanciées des systèmes des acteurs du cloud (statut des unités et des plateformes, capteurs, armes, etc.) ;
- Les données « historiques » de renseignement, d'environnement ou relatives à de précédentes opérations. On peut, par exemple, mentionner les bases thématiques permettant de produire du GEOINT temporel (géospatialisation d'une activité, etc.) ;
- Des données de sources ouvertes en lien avec l'opération émises notamment sur les réseaux sociaux.

Comme l'indique le 3ème V des *big data*, les données ne sont plus nécessairement extraites des sources puis formattées spécifiquement pour être transférées sur un système LDT. Pour exploiter les informations pertinentes dans une grande diversité de formats, les Américains travaillent ainsi depuis des années sur des stratégies relatives à ces données. L'Air Force, par exemple, articule la sienne sur l'enregistrement des sources de données de référence, le catalogage de l'information et la gestion des accès, le développement de bases de données relationnelles entre les informations fondées sur les métadonnées caractérisant ces sources disponibles, enfin évidemment le développement de l'interopérabilité et des mesures de protection des données[20]. L'expérimentation de la Navy repose sur le *Unified Cloud Model* utilisé dans le secteur commercial qui combine cette identification des sources par métadonnées avec le décorticage de leur contenu selon des modèles de données et des ontologies génériques, permettant de répondre plus précisément ensuite aux requêtes de l'utilisateur[21].

Le NGF, futur appareil de combat du SCAF, nœud de ce cloud à l'extrême frange tactique, comprendrait ainsi :

- Des applications diverses conçues pour ses différentes fonctions opérationnelles ;
- Des outils d'analyses automatisés, éventuellement partagés avec les autres systèmes, mis en œuvre via ses applications ;
- Des services communs partagés eux aussi avec les autres systèmes, fonctionnant de façon transparente pour le pilote ;
- Le stockage de quantités importantes de données ;
- La connexion au réseau de communication avec les autres plateformes et unités, un réseau MANET « autoformé et auto-régénérateur » (*self forming & self-healing*).

Ce système d'information opèrerait avec un large degré d'automatisation voire d'autonomisation car sa complexité croissante ne sera plus gérable par un équipage, qui plus est dans une situation de combat. Le général Breton explique ainsi que « *sur le SCAF […] La gestion du transfert des données par le réseau se fera indépendamment du pilote, qui verra les données fusionnées. Il supervisera ainsi la globalité du processus* »[22].

Pour décrire empiriquement ce que permet ce cloud et sa facilité de mise en œuvre pour l'opérateur, **la comparaison avec l'usage du smartphone, complété d'une automatisation accentuée des tâches, est d'ailleurs assez omniprésente** dans les explications de ses concepteurs et architectes, des généraux américains au général Breton.

Une progression incrémentale vers ce cloud tactique

La réalisation de ce cloud ne va pas advenir d'un coup car des briques technologiques de cette construction sont en cours de développement voire déjà mises en œuvre. C'est évidemment le cas aux Etats-Unis. On pense notamment aux capacités de fusion de données dont disposent les appareils de 5ème génération (la *fusion warfare* étant la marque de fabrique du F-35 au demeurant) ou encore les architectures mises en œuvre « en tâches d'huile », dès aujourd'hui par l'US Navy (*Cooperative Engagement Capability*, puis *Naval Fire Control – Counter Air*, puis son extension aux autres missions).

L'armée de l'Air a elle aussi entrepris une démarche incrémentale de développement de ce cloud avec des jalons en 2025 et 2030, destinée à préparer l'arrivée du SCAF. C'est le programme Connect@aero qui va de pair avec le déploiement du standard F4 sur le Rafale. Il vise notamment l'introduction d'un système de communication à plus haut débit et une ramification plus développée de cette connectivité, incluant les munitions sur le modèle des NEW. L'objectif de ce programme est ainsi de « *détecter plus précisément les systèmes de défense sol-air adverses* » et « *d'adapter de manière collaborative les trajectoires et les manœuvres* » des effecteurs et de leurs munitions, en environnement de positionnement, navigation, timing (PNT) dégradé. Il s'agit donc dès la prochaine décennie de mettre en place un « système global de combat aérien » (SGCA)[23]. En outre, les conceptions n'envisagent pas l'avènement d'un cloud tactique englobant d'emblée toutes les tâches de la puissance aérienne. Le cloud prendra en compte, là encore incrémentalement, les différentes fonctions opérationnelles, en partant probablement de la tenue de situation partagée (ce que permettent les LDT actuelles) pour progresser vers les fonctions type analyse prédictive, exploitant massivement le renseignement, mettant ainsi en œuvre les objets les plus complexes et les plus grosses quantités de données, nécessitant les outils les plus sophistiqués[24].

L'apport du cloud : exemple d'une mission d'appui aérien rapproché

Prenons l'exemple d'une mission d'appui aérien rapproché. Ses acteurs incluent l'avion « effecteur » ; le *Joint Terminal Attack Controller* (JTAC), intégré au sein de l'unité terrestre pour demander un appui et ensuite coordonner ou guider la frappe ou l'action d'appui et éventuellement l'observateur avancé si le JTAC n'est pas présent sur zone ; le chef interarmes, le colonel, dans son PC ; le réseau de « contrôle air » qui va du JTAC au centre des opérations aériennes ou au centre opérationnel d'appui aérien et inclut des officiers positionnés en interface des échelons de commandement terrestres pour recueillir les besoins de CAS en planification et répartir les appareils en conduite.

Le processus est le suivant : sur demande de son chef d'unité, ses observations ou celles de l'observateur, le JTAC fait une demande d'appui où il recommande une frappe aérienne que le chef interarmes valide. Le JTAC émet une demande au centre opérationnel lequel assigne l'appareil si ce n'est déjà fait en planification. Une fois arrivé sur zone, l'appareil prend contact avec le JTAC ; ce dernier communique au pilote un brief formaté (le « *9 Line brief* » précisant le cap à prendre par l'appareil, sa distance à l'objectif, l'élévation, la description et les coordonnées de la cible, les forces amies dans la zone, le type de marquage qu'effectuera le JTAC) ainsi que des remarques complémentaires : menaces sol-air, mesures de coordination (par exemple si un tir d'artillerie est exécuté concomitamment), munitions souhaitées, l'approche à exécuter pour la frappe. Le pilote collationne le brief. Puis le JTAC et lui corrèlent leur perception de la situation et vérifient l'acquisition de l'objectif par l'effecteur. Le pilote effectue son approche et le JTAC lui donne alors sa « clearance » pour le tir.

Dans la pratique, **à l'ère du « tout radio » que nous quittons progressivement**, ce dialogue entre le JTAC et le pilote peut parfois durer des dizaines de minutes pour être certain que le pilote frappe la bonne cible sans dommages collatéraux. Encore peut-il être source d'erreurs voire impossible en cas d'incompréhension linguistique.

La période actuelle est au CAS aidé par la numérisation (DACAS), autrement dit au recours aux LDT afin de réduire ces risques d'incompréhension et d'erreurs et accélérer la boucle de décision, même si la radio reste nécessaire pour la clearance ou l'abandon de mission. Le JTAC communique sa demande par le *Variable Message Format*, une LDT choisie par les forces terrestres car diffusable sur les appareils de réseau radio classique. Le centre opérationnel d'appui valide et assigne l'appareil sur la L16. Les éléments du *9 Line brief* sont dispatchés soit par message VMF si les appareils sont dotés de cette LDT (ce qui n'est pas le cas du gros des appareils de l'USAF) soit sur plusieurs messages L16. Afin de préparer son action, l'aéronef va extraire la position des forces amies en interrogeant, via la L16, le serveur de *Blue Force tracking* (la position précise des forces terrestres dans la zone) collationnée par le PC des forces terrestres, généralement au niveau brigade. La numérisation lui permet également de recevoir éventuellement le fameux brief et autres informations du JTAC même avant la prise de contact. Lorsque la prise de contact est effectuée, la numérisation permet en complément au JTAC d'annoter une image transmise par la nacelle de ciblage de l'appareil pour bien marquer la cible et permet à l'aéronef de communiquer son point de visée au JTAC pour confirmation avant l'attaque. Le DACAS se heurte cependant encore à de multiples obstacles : domaines de sécurité différents entre le JTAC et l'aéronef (opérant sur une L16 niveau Secret) ne permettant pas au pilote d'intégrer automatiquement les données dans son SNA, l'obligeant à avoir recours à un outil séparé, corrélation des données extraites des serveurs et émanant du JTAC en phase terminale, etc[25].

Avec un cloud tactique arrivé à maturité, la rapidité de partage de l'information, la richesse de ce partage et l'exploitation de chaque intervenant seraient potentiellement démultipliées. On peut imaginer que le JTAC partage très tôt non seulement les éléments de la demande et du *9 Line Brief* mais aussi la figuration des volumes 3D (la répartition des volumes d'espace aérien), les éléments d'environnement (topographie, environnement civil, etc.) et une simulation informatique de l'approche tactique proposée. Le JTAC posterait l'ensemble de ces informations sur le cloud puis les mettrait à jour. Dès connaissance de l'appareil assigné, il pourrait automatiquement disposer du statut et des capacités des capteurs et des armements de ce dernier au regard de la situation présente, permettant de préparer la frappe. Sur l'appareil assigné, le pilote déclencherait une application qui retirerait puis mettrait à jour automatiquement ces éléments à partir des serveurs, lesquels éléments s'intègreraient dans son système de navigation et d'attaque qui lui proposerait des options de mode d'action tactique en fonction de son cap d'approche. Une fois sur zone, les données de son SNA seraient corrélées avec celles du JTAC, lui fournissant par exemple des perceptions complémentaires émanant de ses capteurs, voire du drone qu'il mettrait en œuvre, en *manned-unmanned teaming*, permettant au pilote et au JTAC de partager une meilleure vue de la situation.

On imagine aussi la plus-value potentielle de cet apport de données pour des missions d'interdiction dynamiques, comme par exemple les missions SCAR (*Strike Coordination and Reconnaissance*). La meilleure exploitation des analyses existantes, voire la capacité à mener ses propres corrélations à partir des données historiques et de situation, peut puissamment contribuer à l'évaluation des modes d'action adverses en cours d'exécution à l'orientation de la conduite de missions. Ce type d'analyse n'est actuellement réalisé, au mieux, qu'en appui renseignement à la planification de la mission.

Le cloud : un facteur majeur d'efficacité, de résilience et d'efficience du SCAF

Le cloud est théoriquement un facteur d'accroissement notable de l'efficacité du SCAF. Le général Verney (2S), conseiller opérationnel SCAF pour Airbus**,** estime ainsi que « *pour la première fois, le besoin d'information à bord d'une plateforme aérienne va supplanter celui de vitesse dans le mantra du pilote de chasse* »[26].

La conscience situationnelle partagée permise par le cloud sera un facteur d'accroissement ou de renforcement de la supériorité informationnelle sur l'adversaire, et de la supériorité décisionnelle qui en découle, comme postulé par la NCW. En outre, ses interconnexions, de même que la conscience situationnelle partagée qu'elles génèrent, permettent, potentiellement, **la pleine transition d'un combat connecté à un combat collaboratif** comme l'appelle de ses vœux Caroline Laurent, directrice de la stratégie de la Direction générale de l'armement (DGA)[27] et comme l'armée de l'Air entend l'entreprendre incrémentalement au travers du programme Connect@aero. Le combat collaboratif signifie que les capacités des différentes plateformes sont mises en œuvre comme un unique système pour améliorer la détection de systèmes adverses et générer plus rapidement et efficacement, en action comme en réaction, l'effet recherché. Il peut s'agir par exemple d'armements délivrés par une plateforme sur la base des données intégrées provenant de capteurs d'autres plateformes (que le NEW préfigure). Le gain d'efficacité ne se traduit pas uniquement en termes de rapidité d'exécution de la boucle OODA. Comme l'exemple sur le CAS le laisse envisager, une meilleure exploitation du renseignement, une connaissance partagée plus fine, en temps réel, des capacités opérationnelles des unités engagées dans une situation donnée et la capacité de combat collaborative seront de nature à accroître **la précision des effets recherchés**.

La mise en œuvre d'un tel cloud de combat devrait également aboutir à transformer la fonction C2 des opérations, un sujet qui génère beaucoup de débats depuis plusieurs années. Les opérations aériennes obéissent traditionnellement à un double principe doctrinal :

- leur contrôle (la planification, l'élaboration de l'*Air Tasking Order* réglant le « ballet » des opérations sur 24h, la conduite dynamique de ces 24h d'opérations, puis leur évaluation) est centralisé au niveau du centre des opérations aériennes (le CAOC) pour gérer au mieux une ressource comptée ;
- leur exécution est décentralisée, c'est-à-dire pour partie réalisée au CAOC et pour partie déléguée au niveau des plateformes de « *battle management* » comme les AWACS, les effecteurs (etc.), afin de garantir la liberté d'action nécessaire pour faire face aux contingences tactiques.

Avec leurs capteurs modernes, les appareils de combat récents sont déjà devenus autant des effecteurs que des moyens ISR. Avec la conscience situationnelle et les moyens de traitement apportés par le cloud, ces appareils et leurs successeurs disposeront d'une capacité d'initiative leur permettant, selon beaucoup d'acteurs, d'assumer une charge accrue de contrôle local des opérations allant bien au-delà de l'exécution décentralisée actuelle, c'est-à-dire de se voir déléguer certaines autorités actuellement conservées au niveau du CAOC. C'est le concept de « contrôle distribué »[28]. L'emploi des F-35 et F-22 américains, comme « quarterback » des appareils de 4ème génération, préfigurerait cette évolution en dépit des limitations de connexion avec les autres aéronefs. Cela étant, son impact sur la doctrine et l'organisation de la fonction C2 reste encore limité. Des visions extrêmes, outre-Atlantique, envisageraient même un « *Disaggregated C2* », une beaucoup plus grande distribution du contrôle impliquant des cycles décisionnels entièrement revus et éventuellement la disparition du CAOC tel qu'il existe, ou encore de l'AWACS[29]. Inversement, dans la mesure où des délégations de contrôle existent déjà dans la pratique, d'autres minimisent la portée de ce concept de « contrôle distribué ».

Le combat collaboratif et ces éventuelles réorganisations du contrôle des opérations confèreraient **un degré accru de résilience et de flexibilité à la puissance aérienne** face à des systèmes intégrés de défense antiaérienne aux capacités de détection et d'interception redondantes, en garantissant la polyvalence et la dispersion des acteurs de la « *kill chain* ». C'est l'adage selon lequel il faut un réseau pour combattre un autre réseau. Ils permettent en outre **d'optimiser le rendement, l'efficience de la puissance aérienne utilisée**. C'est là un point particulièrement important. Notre puissance aérienne est certes la plus importante d'Europe avec celle des Britanniques, elle n'en est pas moins anémiée. C'est le cas des capacités ISR aéroportées. C'est aussi vrai pour les capacités d'engagement/combat. Avec le parc de 225 appareils de combat (Air et Marine) prévu par la Loi de programmation militaire, nos forces doivent pouvoir, dans le contrat opérationnel d'engagement majeur, déployer 45 avions (en comptant le groupe aéronaval). Dans la pratique, l'armée de l'Air aura peiné ces dernières années pour déployer en permanence une quinzaine d'appareils. Encore a-t-elle dû y concentrer l'essentiel de ses moyens de soutien, obérant ses facultés à la régénération de ses capacités. En d'autres termes, l'armée de l'Air peut réaliser des prouesses en raid à longue distance, assurer des appuis limités, mais n'est plus en mesure, seule, de réaliser une campagne. Or, il apparaît depuis plusieurs années, que la participation américaine à nos engagements est passée d'une confortable présupposition à une inquiétante variable. Une intervention en coalition limitée sans les énormes moyens de l'US Air Force devient parfaitement plausible. Si la transition du système actuel au SCAF s'inscrit dans la droite ligne de la totalité des sauts de génération vécus par nos forces aériennes et celles de nos partenaires, il est alors à craindre que l'inventaire se réduise à nouveau même si l'incorporation de drones pourra peut-être compenser cette tendance continue à l'étiolement. Dans ce contexte, les apports du cloud n'en seront que plus critiques.

Enfin, actuellement, **seules les forces aériennes occidentales et israéliennes ont démontré leur maîtrise des opérations aériennes en réseau. Cette avance n'est cependant pas gravée dans le marbre** à l'horizon du SCAF. Ainsi, la L16 a été distribuée à l'ensemble des partenaires américains (incluant aussi l'Arabie Saoudite, les EAU, le Japon, la Corée du sud, le Pakistan et Taiwan). L'armée de l'Air chinoise aurait naturellement développé ses propres LDT[30], celle du Pakistan également[31]. On assiste donc à un nivellement progressif dans le « combat connecté ».

Or, le développement des *big data* et des capacités de traitement associées, incluant l'intelligence artificielle, est un phénomène assez universel. Il est donc mécaniquement à la portée de multiples pays, pas uniquement des Occidentaux et de leurs partenaires les mieux dotés. Ne pas développer cette capacité, c'est donc prendre le risque de faire face à terme à une situation d'infériorité informationnelle contre un adversaire. Certes, nos forces ont déjà rencontré de telles situations, surtout dans les environnements de guerre irrégulière, mais rarement dans la confrontation tactique elle-même et jamais dans le domaine aérien. **Le cloud apparaît donc comme une étape obligée dans la compétition militaire**.

Le risque principal : une exposition accrue à la menace cyber-électronique

Le passage au cloud n'est pas sans risque. Le principal réside évidemment dans la menace des attaques cyber-électroniques (c'est-à-dire, la convergence de la guerre électronique et de la lutte informatique, déjà largement actée sur le plan doctrinal et qui se développe technologiquement)[32]. Il faut ici distinguer les menaces de brouillage portant sur le réseau de transmissions et les capteurs et celles relevant de la LIO portant potentiellement sur l'ensemble du cloud.

Jusque dernièrement, la L16 était considérée comme assez sécurisée contre le brouillage. Cependant, là encore, l'évolution rapide des technologies de l'information peut rebattre les cartes. Certes, la distribution fonctionnelle dans les domaines C2 et ISR contribue précisément à contourner les actions de brouillage portant sur tel ou tel système et à réduire l'impact de ces actions sur un nœud donné. Le recours à des LDT à basse probabilité de détection et d'interception (LPD/LPI) continuera voire renforcera la difficulté du brouillage de ces communications. Encore faut-il que ces nouvelles LDT n'utilisent pas l'heure des GNSS (comme le GPS), vulnérables au brouillage, comme outil de synchronisation. Il n'en reste pas moins que l'emploi du cloud deviendra une gageure dans un environnement électromagnétique fortement contesté par un adversaire étant lui-même passé à des procédés de « guerre électronique adaptative » distribuant de façon flexible ses efforts.

La menace de LIO, qu'elle passe ou non par cette exploitation du spectre électromagnétique, apparaît à terme plus problématique encore. Les rapports du *Director Operational Test & Evaluation* du Pentagone se font régulièrement l'écho de « vulnérabilités cyber » de bon nombre de systèmes américains, y compris des systèmes récents ayant en théorie pris en compte cette menace, dont le F-35[33]. Or, la multiplication des interconnexions accroît les potentialités d'intrusions électroniques dans le cloud et augmente les risques d'effets systémiques de ces dernières. De plus, en asservissant une large part de l'avantage compétitif de la puissance aérienne à cette mise en réseau approfondie et étendue, le cloud démultiplie également la criticité de cette vulnérabilité. En d'autres termes, avec un cloud tactique insuffisamment insécurisé face à un adversaire efficace, apparaît potentiellement **le risque d'une paralysie systémique** de la puissance aérienne.

Les défis majeurs de la connexion, de l'interopérabilité et du partage de l'information

Le premier défi majeur à surmonter par le cloud sera donc probablement **son aptitude à opérer dans cet environnement électromagnétique extrêmement contraint, à l'exploitation souvent dégradée voire interdite**, qui n'a rien à voir avec le solide maillage de fibres et de tours relais qui sous-tend nos réseaux de téléphonie. Elle impose des procédés de fonctionnement adaptés à cette connexion intermittente, comme par exemple, la compensation par la recherche du débit des LDT, le renforcement des transmissions asynchrones, le stockage massif de données en planification de mission, les modèles de combat collaboratif exécutables sans connexion.

Vient ensuite la question de l'interdépendance entre les acteurs de ce cloud. **Réussir cette interdépendance suppose en premier lieu un niveau inédit d'interopérabilité.** Or, pour l'observateur de longue date, la plupart des discours actuels prônant l'avènement futur de ce système de systèmes, d'échanges d'informations parfaitement fluides entre les acteurs (etc.) font furieusement écho aux emphases sur la numérisation et la NCW qui parcourent la littérature et les briefing depuis 25 ans : à la sombre évaluation des performances du moment succède toujours les mêmes objectifs. Leur répétition, année après année, ou à chaque nouveau projet visant à avancer l'intégration, montre en réalité le caractère très élusif de ces objectifs. L'expérience outre-Atlantique démontre en effet que la fixation de standards n'est pas suffisante pour garantir l'interopérabilité entre systèmes acquis dans un paysage institutionnel à décideurs multiples, lesquels adaptent ces standards et/ou développent leur feuille de route en fonction de leurs propres calendriers d'architectures.

Cette interopérabilité a certes progressé, en témoignent les LDT évoquées ci-dessus. Simplement, elle a jusqu'à maintenant été acquise lorsqu'une autorité organique ou opérationnelle a suffisamment de poids pour imposer ses normes aux acteurs sous son contrôle (voir par exemple l'histoire du *Blue Force Tracking*, de la L16 ou de l'architecture de défense antimissile), lorsque des partenaires de cette autorité consentent pleinement à adopter ces normes dans leur moindre détail, voire l'équipement qui va avec (alliés avec la L16 par exemple), enfin, et dans une moindre mesure, lorsqu'un travail de convergence s'opère sur certaines missions dont la criticité est reconnue (exemple du DACAS donné ci-dessus). En d'autres termes, l'interopérabilité est obtenue vers le haut, au sein des éléments d'une armée donnée et éventuellement de ses partenaires directes, ou d'une agence. La période actuelle connaît cependant des inflexions avec la généralisation de systèmes d'information à architectures ouvertes modulaires, aux évolutions en théorie beaucoup plus flexibles, de préférence à la juxtaposition de systèmes « clients ». Il reste encore à mesurer si ces nouveaux systèmes constitueront un progrès réel en la matière.

Ceci pose donc la question de l'autorité normative présidant à la conception du cloud du SCAF. A première vue, deux options apparaissent envisageables. La première option

serait celle de l'intégration au « cumulonimbus » de la puissance aérienne américaine (fondé sur le F-35, le *Joint Aerial Layer Network* – le réseau de communication air – et ses passerelles multi-réseaux, sa conception de la fonction C2, etc.) que les Américains chercheront mécaniquement à imposer au sein de l'OTAN. Cette option pose à nouveau la question de notre principe d'autonomie stratégique. Elle pose aussi la question de la survie d'une part importante de notre BITD. La seconde, dans laquelle le MINARM se lance comme évoqué ci-dessus, est donc de développer notre propre « cumulus ». Dans ce cas, se posera la question de l'interopérabilité avec l'architecture américaine et probablement otanienne. A moins que les technologies qui se développent permettent des liens flexibles, à la demande, entre les deux ensembles. Quoi qu'il en soit, elle plaide pour un développement incrémental de notre cloud, concomitamment à celui développé actuellement par les Américains, sans quoi cette question des normes risque d'être définitivement réglée au moment où le SCAF arrivera à maturité.

En second lieu, en présupposant que les technologies et les normes soient au rendez-vous, l'interdépendance passe par **une politique symétrique et ouverte de partage de l'information, tout particulièrement dans le cas du SCAF bâti sur un partenariat international**. Or, la facilitation de l'accès aux productions de renseignement sera un défi permanent de même que la « *fusion warfare* » entre capteurs d'aéronefs de pays différents. C'est tout particulièrement le cas des capteurs de soutien électronique, dont les données alimentant le ROEM, sont parmi les plus sensibles de la fonction renseignement. Dans la pratique, ce type de politique de partage (ou plus précisément d'échange dans le domaine renseignement) ne va pas de soi et n'est mis en œuvre que si les hautes autorités le précisent. Elle pose donc le défi de l'entraînement en accès informationnel appauvri et le risque, en opération, d'avoir un cloud asymétrique.

Se pose enfin la question du périmètre du cloud. **Une des principales craintes que l'on peut nourrir concernant le cloud tactique du SCAF a trait à la réelle prise en compte des autres domaines**, actuellement présentés comme relevant du second cercle « extérieur ». Il est à noter que la vision promue par le général Deptula est celle d'un cloud multidomaine, non uniquement dédié aux forces aériennes, éventuellement spatiales et cyber (approche multidomaine de beaucoup d'autres acteurs de la puissance aérienne) mais aussi aux forces terrestres et navales. Cette vision n'en est que plus pertinente concernant notre appareil de forces, précisément en raison des limites de volume de chacun de ces milieux. Ainsi, le cloud devrait être bâti non pas uniquement en fonction des missions type de la puissance aérienne, mais des missions interarmées. Dans notre exemple du CAS, le cloud devrait typiquement englober l'appui-feu dans sa globalité, dont le CAS n'est qu'un procédé et qui inclurait aussi les feux d'artillerie terrestre et naval. En d'autres termes, le cloud destiné au SCAF devrait viser l'intégration avec celui du combat Scorpion. Bien entendu, cette ambition nous plongerait plus encore dans les affres de l'interopérabilité décrites plus haut. Cela étant, **le maintien de notre puissance militaire sur l'avant-scène de l'Europe, dans un environnement stratégique lourd de risques, et de notre ambition à rester une nation cadre de coalition limitée, impose cette aptitude aux opérations interarmées intégrées, dont le cloud doit être une pièce essentielle**.

Philippe GROS
Maître de recherche, FRS
p.gros@frstrategie.org

Notes

1. Général Denis Mercier, « Les opérations aériennes et le cyber: de l'analogie à la synergie », *Res Militaris*, hors-série "Cybersécurité", juillet 2015.

2. Peter Mell (NIST), Tim Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology , September 2011 (traduction de l'auteur avec l'aide du traducteur Deepl)

3. Defense Information Systems Agency, *Enabling the Joint Information Environment, Shaping the Enterprise for the Future Conflicts of Tomorrow*, 5 May 2014, p.2

4. *DoD Cloud Strategy*, December 2018.

5. Axel Dyèvre, Pierre Goetz et Martin de Maupeou, *Emploi du Cloud dans les Armées, Première approche des concepts et contraintes*, Les notes stratégiques, CEIS, août 2016, p.14.

6. MINARM, *Ambition numérique du ministère des Armées,* DICoD - Bureau des éditions - décembre 2017, p.9.

7. « Deptula: 'Combat cloud' is 'new face of long-range strike' », *Armed Forces Journal*, September 18, 2013.

8. Air Combat Command, *Combat Cloud Operating Concept*, cité dans : Major Jacob Hess *et alii*, *The Combat Cloud Enabling Multidomain Command and Control across the Range of Military Operations*, Wright Flyer Paper No. 65, Air University, March 2017, p.1.

9. Office of Naval Research, *Data Focused Naval Tactical Cloud (DF-NTC)*, ONR Information Package, June 24, 2014.

10. Director, Force Transformation, Office of the Secretary of Defense, *Military Transformation : A Strategic Approach*, Fall 2003, pp. 31-32.

11. Sans compter ceux destinés à la gestion du réseau.

12. Voir sur ce plan la fiche wikipédia française, élaborée par un spécialiste de la LDT https://fr.wikipedia.org/wiki/Liaison_16

13. Voir de façon générale, CICDE, *Les liaisons de données tactiques* (LDT), Publication interarmées PIA-3.50_LDT(2017), N° 109/DEF/CICDE/NP du 13 juin 2017.

14. Général Breton cité dans Yves Pagot « Le SCAF raconté par ses concepteurs », *Portail Aviation*, 31 janvier, 2019.

15. Entretien avec un industriel.

16. Thomas L. Frey et alii, Lockheed Martin Corporation, « F-35 Information Fusion » in Jeffrey W. Hamstra, *The F-35 Lightning II : From Concept to Cockpit*, Progress in Astronautics and Aeronautics, volume 257, American Insitute of Aeronautics and Astronautics, 2019, pp 421-440.

17. Martin E. Dempsey, Chairman of the Joint Chiefs of Staff, *Joint Information Environment*, 22 January 2013.

18. *Air Superiority 2030 Flight Plan*, May 2016, p.5.

19. Office of Naval Research, *Data Focused Naval Tactical Cloud (DF-NTC)*, ONR Information Package, June 24, 2014.

20. Maj Gen Kim Crider, Air Force Chief Data Officer, *Air Force Data Strategy*, non daté.

21. Office of Naval Research, *Data Focused Naval Tactical Cloud (DF-NTC)*, *op. cit.*

22. Général Breton cité dans Yves Pagot, *op. cit*.

23. David Pappalardo, « Combat collaboratif aérien connecté, autonomie et hybridation Homme-Machine: vers un 'Guerrier Centaure' ailé ? », *DSI*, janvier-février 2019, p 70-75.

24. Démarche de l'expérimentation de la Navy, *Data Focused Naval Tactical Cloud* et entretien avec un industriel.

25. Considérations tirées de *l'étude technico-opérationnelle pour la mise en œuvre d'échanges numérisés lors des missions d'appuis aériens*, élaborée en 2014-2015, à laquelle a contribué l'auteur.

26. Jean-Michel Verney, « Le Combat Cloud : une feuille de route pour le projet Scaf », *Revue de défense nationale*, 28 juin 2018, p.1.

27. Natasa Laporte, « A quoi ressemblera le combat aérien collaboratif du futur ? », *La tribune*, 28/06/2018.

28. Lire par exemple, Gilmary Michael Hostage III and Larry R. Broadwell, Jr. « Resilient Command and Control. The Need for Distributed Control », *Joint Force Quarterly*, JFQ 74, 3rd Quarter 2014.

29. George I. Seffers, « Air Force Seeks Disaggregated Command and Control », *Signal*, February 1, 2019.

30. Defense Intelligence Agency, *China Military Power*, January 2019, p.86.

31. Bilal Khan, « "LINK-17" – PAKISTAN'S HOMEGROWN DATA-LINK SYSTEM », *Quwa,* 5 April 2016.

32. Voir Philippe Gros, *Les opérations en environnement électromagnétique dégradé*, note n°1 de l'Observatoire des conflits futurs, FRS, avril 2018.

33. Les rapports du DOT&E sont disponibles à l'adresse internet suivante https://www.dote.osd.mil/

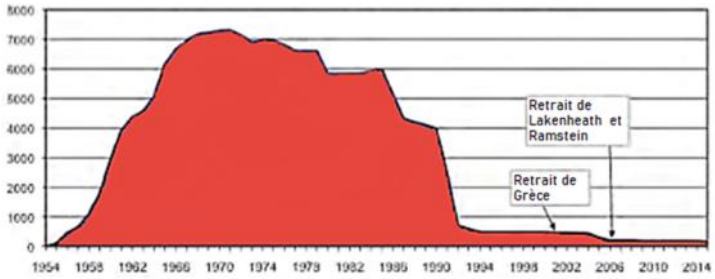
Forces aériennes européennes et mission nucléaire de l'OTAN

Le renouvellement des forces aériennes en Europe est régulièrement abordé sous des angles techniques ou industriels. En effet, le choix des pays de se tourner vers le F-35 de Lockheed Martin ou des porteurs européens renvoie des signes sur l'intégration des armées de l'air européennes avec leurs alliés américains, ou au contraire des volontés de privilégier les coopérations à l'échelle du continent. Par ailleurs, les capacités militaires des avions retenus et les volumes commandés sont également scrutés pour mieux comprendre les ambitions militaires des Etats dans le domaine aéronautique. Leur participation à la mission nucléaire de l'OTAN est rarement évoquée comme un élément central dans cette prise de décision. Pourtant, quatre Etats européens ont la capacité d'emporter des armes nucléaires avec leurs chasseurs nationaux. Ils semblent aujourd'hui attachés à poursuivre cette mission, ce qui conditionne en réalité fortement les capacités aériennes qu'ils cherchent à acquérir.

Le partage du nucléaire au sein de l'OTAN

Depuis les années 1950, plusieurs Etats européens sont directement impliqués dans la politique de dissuasion de l'Alliance atlantique. En effet, les Etats-Unis ont déployé pendant la guerre froide des armes nucléaires sur plusieurs bases aériennes pour crédibiliser leur posture vis-à-vis de l'Union soviétique mais également pour rassurer des Alliés contre un éventuel « découplage » de leurs intérêts et de ceux de Washington. A l'heure actuelle, on estime à environ 140 armes entreposées en Allemagne (BA Büchel), aux Pays-Bas (BA Volkel), en Belgique (BA Kleine Brogel), en Italie (BA Aviano et Ghedi Torre) et en Turquie (BA Incirlik)[1].

Evolution du nombre d'armes américaines déployées en Europe (FAS) – 1954-2014

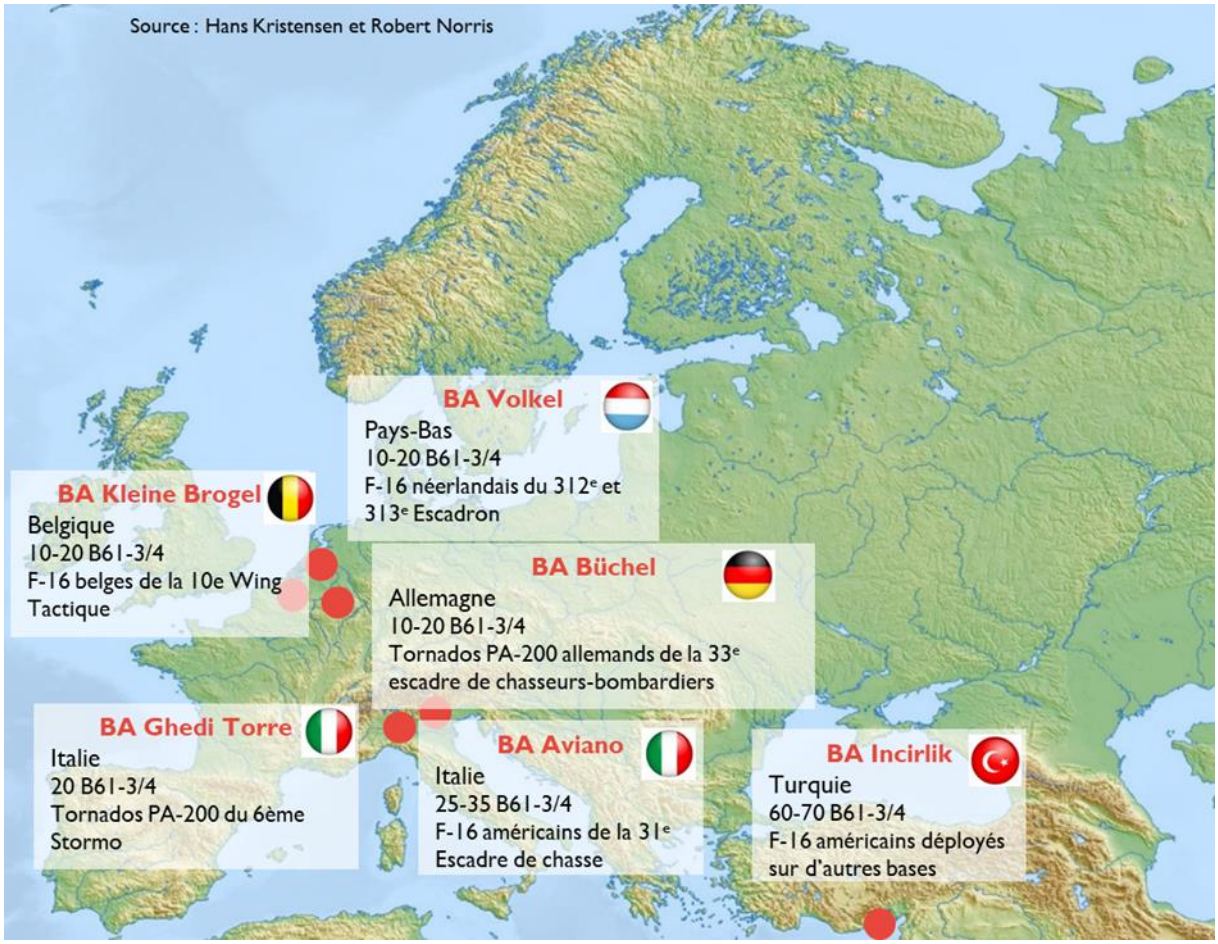


Cela représente un fragment au regard du pic de la guerre froide où le Royaume-Uni ou la Grèce étaient également pays hôtes et où le nombre d'armes estimé sur le continent dépassait 7 000[2]. Les armes stationnées à ce jour sont des bombes à gravité B61.

Le dispositif actuel est relativement connu bien qu'il ne fasse l'objet d'aucune confirmation officielle de la part de l'OTAN ou des Etats hôtes. Sur la plupart des bases, les armes sont entreposées sous la responsabilité d'unités de soutien américaines. Des chasseurs bombardiers du pays hôte sont affectés et des pilotes formés pour pouvoir emporter ces armes à gravité en cas de décision d'y avoir recours. Ainsi, l'Allemagne entretient pour cette mission la 33ème escadre de chasseurs bombardiers équipée de Tornado PA-200. Les Pays-Bas et la Belgique y dédient des équipages de F-16 (10e Wing Tactique pour la Belgique ; 312ème et 313ème Escadron de la RNAF). En Italie, les Tornado PA-200 du 6ème Stormo ont également la capacité de transporter les B61. Pour ce qui est d'Aviano et d'Incirlik, ce sont *a priori* des avions américains qui se chargeraient de transporter les armes.

Une mission réaffirmée

La composante B61 n'est qu'un aspect de la dissuasion nucléaire de l'Alliance, qui est également assurée par les arsenaux stratégiques des Etats-Unis, et auxquels concourent les forces nucléaires autonomes du Royaume-Uni et de la France. Elle a été fortement remise en cause dans les années récentes. En effet, beaucoup ont jugé que l'utilité militaire de ces arsenaux était négligeable. Il serait en effet difficile d'imaginer un scénario où l'Alliance ferait le choix unanime de mener une mission de riposte nucléaire avec des bombes à gravité, armes qui restent aujourd'hui vulnérables au regard des défenses les plus modernes et dont la portée est limitée. Par ailleurs, au niveau politique, les armes restent impopulaires dans la plupart des pays hôtes. En 2010, le parti libéral allemand, représenté au gouvernement par Guido Westerwelle, a tenté de faire pression pour obtenir le retrait des B61 du territoire allemand. D'autres pays, comme les Pays-Bas et la Belgique, semblaient à l'époque intéressés par le retrait[3].



Pour autant, il y a désormais un relatif consensus sur l'intérêt de préserver le dispositif actuel. Au niveau militaire, le remplacement des armes actuelles par les B61-12 modernisées devrait améliorer les performances du dispositif et pallier à certaines vulnérabilités des bombes à gravité, en offrant en particulier une capacité modeste de tir à distance. Couplées à de nouveaux bombardiers, ces nouvelles armes seront plus crédibles dans une mission de dissuasion. Il n'est pas certain cependant qu'elles soient considérées comme parfaitement performantes, puisque Washington a appelé à l'acquisition de nouveaux missiles de faible portée dans la *Nuclear Posture Review* de 2018.

C'est en réalité pour leur rôle politique et symbolique que les B61 font désormais de nouveau consensus. Dans le contexte de durcissement des relations russo-européennes, et suite, à l'invasion de la Crimée, de nombreux alliés européens ont souhaité préserver les signes de solidarité transatlantique et rester impliqués dans la mission de dissuasion nucléaire de l'OTAN, à nouveau perçue comme pertinente.

A ce titre, des documents récents comme le Communiqué du Sommet de l'OTAN de Varsovie, datant de 2016, évoquent formellement ce rôle en rappelant que « *la posture de dissuasion nucléaire de l'OTAN repose également, en partie, sur les armes nucléaires des États-Unis déployées à l'avant en Europe, ainsi que sur les capacités et l'infrastructure mise à disposition par les Alliés concernés…L'Alliance assurera une participation aussi large que possible des Alliés concernés aux arrangements agréés pour le partage du fardeau dans le domaine nucléaire* »[4].

Depuis cette date, les gouvernements concernés n'ont plus contesté ouvertement le stationnement avancé et plusieurs ont même indiqué de manière discrète ou en réponse à des interrogations directes de leurs parlementaires qu'ils comptaient poursuivre leur participation dans cette mission.

La question des capacités aériennes

Ce choix politique et stratégique n'est pas sans conséquence pour le dimensionnement et l'acquisition des forces aériennes des pays hôtes, et en particulier pour ceux qui participent directement au transport des armes. En effet, cette mission nécessite des appareils certifiés et adaptés par l'armée américaine et des pilotes formés. Seuls les Tornado PA-200 et les F-16 Fighting Falcon sont actuellement certifiés dans ce cadre. Or, ces deux appareils arrivent en fin de vie dans les différents pays hôtes, avec des retraits anticipés pour 2025 environ. Les cinq pays ont donc entamé des procédures de renouvellement qui sont à des stades d'avancement divers. Dans la plupart de ces pays, la question de la mission nucléaire semble jouer un rôle important dans le choix de l'appareil, même si la question n'est que rarement évoquée publiquement.

Le choix du F-35, un appareil conçu clairement pour être certifié pour une mission nucléaire, est souvent perçu comme offrant la possibilité de mener cette mission. En effet, l'US Air Force a très tôt consacré une ligne budgétaire à l'adaptation du chasseur à l'emport des B61, un surcoût qui a d'ailleurs été contesté au Congrès[5]. Compte-tenu des difficultés rencontrées par le programme F-35, le calendrier initial a

été retardé et l'adaptation à la mission nucléaire, *via* l'installation de composants dénommés "bloc 4", a été retardée. Le premier vol du bloc 4, prévu à l'origine pour 2018, est maintenant prévu pour l'année suivante[6].

Les Pays-Bas font partie des partenaires historiques du programme F-35. La position officielle néerlandaise est régulièrement rappelée par les ministres des Affaires étrangères et de la Défense au Parlement. Elle indique qu'il est trop tôt pour savoir si les F-35, qui viendront succéder au F-16 d'ici à 2024, auront une mission nucléaire. En effet, lorsque les commandes ont été passées, la politique officielle des Pays-Bas visait à faire en sorte que d'ici là, les circonstances internationales et les accords de l'OTAN permettent de rendre cette dernière caduque[7]. Cette posture est rappelée régulièrement par le gouvernement, mais on peut cependant lire en creux que le F-35 devra reprendre l'ensemble des missions du F-16, ce qui dans le contexte stratégique prévisible inclut de prendre en charge la mission nucléaire[8].

Pour rappel, les Pays-Bas ont pour l'instant commandé 37 F-35A, dont deux ont été livrés en 2013. Le premier avion opérationnel a été présenté le 30 janvier 2019[9]. Dans le cadre du plan d'investissement de l'OTAN, les Pays-Bas pourraient envisager d'accroître leur commande initiale, une information qui n'est pas encore officielle mais semble avoir le soutien du gouvernement[10].

La contribution italienne au programme JSF/F-35 a débuté en 1998 avec le projet de retombées importantes pour l'industrie aéronautique italienne. Au lancement du programme, l'Italie avait évoqué l'achat de 131 appareils. Ce volume a été réduit à 90 par le gouvernement Monti à la suite de la crise financière. Le changement politique avec l'arrivée au gouvernement en 2018 du parti M5S, très hostile au programme pour des raisons budgétaires, mais également connu pour ses positions antinucléaires, a posé de nombreuses questions sur son évolution. Initialement chahutée par ses sympathisants sur l'avenir du programme, la ministre de la Défense Elisabetta Trenta a laissé entendre que le volume des 90 avions n'était pour l'instant pas remis en cause mais que le rythme d'acquisition allait ralentir[11]. Concernant l'adaptation à la mission nucléaire, on ne dispose pas d'informations officielles sur ce point à l'heure actuelle. Interrogé par les députés sur cette question, l'ancien secrétaire adjoint à la Défense avait répondu de manière vague[12]. Le nouveau gouvernement ne s'est pas exprimé à ce sujet.

En Belgique, le renouvellement des F-16 a connu certains rebondissements depuis le lancement de la procédure en 2014. Plusieurs modèles ont initialement été présentés comme de possibles candidats : le F-35A de Lockheed Martin mais aussi le F/A-18E/F Super Hornet de Boeing, le Gripen de SAAB, le Rafale de Dassault et l'Eurofighter. En février 2018, deux constructeurs ont finalement remis leurs offres à Bruxelles, Lockheed Martin et le consortium Eurofighter. La France a proposé le Rafale dans une procédure parallèle d'accord de coopération gouvernementale[13]. À noter que lors de la publication de l'appel d'offres, le critère « adaptable à la mission nucléaire » était apparu comme anecdotique dans le processus d'attribution, comptant selon la presse pour moins d'1% dans l'évaluation des offres[14]. Néanmoins, un document ultérieur émanant du ministre de la Défense a semblé indiquer qu'il s'agissait d'un critère de choix fondamental. Le flou entourant cette question a notamment suscité des contestations au Parlement où l'honnêteté de la procédure d'appel d'offres a été mise en cause[15]. La décision, plusieurs fois repoussée, a été rendue le 25 octobre 2018 avec l'annonce du gouvernement de l'acquisition de 34 F-35A pour un montant de 4 milliards d'euros[16]. Les premières livraisons devraient intervenir à compter de 2023[17].

Le cas turc est particulier puisque la livraison des avions F-35A commandés par Ankara devrait être provisoirement suspendue par Washington. En effet, le Sénat a ajouté un amendement à la *National Defense Authorization Act* de 2018 pour bloquer les transferts à destination de la Turquie en opposition à l'emprisonnement du pasteur américain Andrew Brunson, accusé d'espionnage, par le gouvernement d'Erdoğan. Il a également estimé plus substantiellement que les systèmes F-35 seraient mis en danger en cas de transferts vers la Turquie du fait de l'acquisition par l'armée turque du système antimissile russe S-400[18]. Si l'exclusion de la Turquie du programme F-35 devait intervenir, on pourrait penser qu'Ankara abandonnerait définitivement la capacité d'emporter les B61 stationnées sur son territoire.

L'Allemagne est un autre pays pour lequel subsistent des interrogations sur ce sujet. Le gouvernement n'a pas encore pris de décision officielle sur le remplacement des Tornado actuellement consacrés à la mission nucléaire. En janvier 2019, le ministère de la Défense a présélectionné l'Eurofighter et le F/A-18 Hornet, alors que le F-35 a été éliminé de l'appel d'offre. Priorisant la montée en puissance d'un avion de 5ème génération franco-allemand, Berlin envisagerait d'acquérir un nombre limité d'appareils comme une solution « transitoire ». La capacité à prendre en charge toutes les missions du Tornado, y compris celles liées à l'OTAN a été affirmée à plusieurs reprises. La capacité de l'un ou l'autre de ces appareils à être adaptée à la mission nucléaire serait actuellement à l'étude[19]. Le gouvernement a indiqué que les critères de sélection de ces deux appareils avaient été la possible harmonisation avec le NWGS/FCAS franco-allemand, le calendrier d'acquisition d'un avion successeur et la capacité à maintenir sans interruption un rôle dans la mission de partage du nucléaire[20]. Ainsi, les autorités nationales ont précisé que seuls des modèles américains et allemands avaient été examinés justement pour éviter des problèmes complexes[21] de certification. Pour rappel, le F/A-18 Hornet a été certifié pour l'emport d'armes nucléaires jusqu'en 1994, mais devrait être reconfiguré pour pouvoir porter les B61-12. Concernant l'Eurofighter, la certification semble *a priori* possible, mais des interrogations persistent sur le coût d'une telle opération, ses conséquences en termes de protection des secrets industriels et le temps que l'opération pourrait prendre[22]. Le gouvernement a été interrogé par les députés allemands en avril et a évoqué la certification comme « possible » sans donner de précisions sur les éventuelles complications[23].

Pour autant, la poursuite de la mission nucléaire demeure sources de controverses. Ainsi, le parti SPD a initié une commission d'examen de ses positions en matière de relations internationales, de Défense et de stratégie visant spécifiquement à réétudier la participation allemande à la mission nucléaire de l'OTAN. Ralf Stegner, vice-président du SPD, a d'ores et déjà annoncé que la mission de partage nucléaire ne lui semblait plus adaptée aux défis actuels et qu'il était peu probable que le groupe soutienne la commande du F/A-18[24].

Dans le contexte actuel, le facteur nucléaire reste donc essentiel pour au moins quatre pays de l'OTAN, et leur volonté de conserver la capacité d'emporter les armes nucléaires stationnées sur leur territoire joue un rôle important dans les choix retenus pour leurs forces aériennes. La participation à cette mission particulière et confidentielle n'oblige pas un Etat à sélectionner un seul type d'appareil, comme le F-35, mais restreint ses options. Ainsi, certains constructeurs, comme SAAB, ont indiqué par le passé ne pas vouloir développer d'appareils pouvant emporter des armes nucléaires[25]. Il est donc important de prendre en compte ce facteur dans les réflexions qui entourent le renouvellement des capacités aériennes des différents alliés de l'OTAN, d'autant plus qu'il peut être sujet à des débats politiques internes. Cela s'applique également pour les programmes coopératifs futurs. Dès lors, le projet franco-allemand FCAS ne devrait pas faire l'économie d'une réflexion sur sa capacité à emporter des armes nucléaires, qu'elles soient d'origine françaises ou américaines. Le gouvernement allemand a déjà été interrogé sur cette question, qui reste particulièrement ouverte.

EMMANUELLE MAITRE
Chargée de recherche, FRS
e.maitre@frstrategie.org

Notes

1.K/N.
2.Hans Kristensen, « d », Strategic Security, FAS, 26 juin 2008.
3.Paolo Foradori (éd.), *Tactical Nuclear Weapons and Euro-Atlantic Security: The Future of NATO*, Routledge, Londres, 2013.
4.Communiqué du Sommet de l'OTAN de Varsovie, juillet 2016.
5.John A. Tirpak, « Nuclear Lightning », *Air Force Magazine*, 17 mars 2014.
6.« PE 0207142F / F-35 Squadrons », Department of Defense Fiscal Year (FY) 2019 Budget Estimates, Air Force Justification Book Volume 3a of 3 Research, Development, Test & Evaluation, Air Force Vol–III Part 1, février 2018.
7.Tweede Kamer der Staten-Generaal, Vergaderjaar 2013-2014, Brief van de Ministers van Defensie en van Buitenlandse Zaken, Nucleaire ontwapening en non-proliferatie, 33 783, n°5, 14 janvier 2016.
8.Antwoord op vragen van de leden Karabulut, Van Ojik en Ploumen over kernwapenbeleid, Antwoord schriftelijke vragen, n° 2018D22439, 1er mai 2018. « *The government states that the F-35 is intended to take over this task from the F-16* ».
9.« The Royal Netherlands Air Force First Operational F-35 Rolls Out », *F-35.com*, 30 janvier 2019.
10.Visie op de toekomst van Defensie, Stenogram, n°2019D04684, 22 janvier 2019.
11.Franco Lacch, « F-35, l'Italia rallenterà le acquisizioni », *Il Giornale*, 12 novembre 2018.
12.Gioacchino Alfano, Resoconto stenografico dell'Assemblea Seduta n. 205 di venerdì 4 aprile 2014, 4 avril 2014.
13.Laurent Lagneau, « Rafale : Dassault Aviation abat ses cartes en Belgique », *Zone Militaire*, 14 février 2018.
14.Antoine Clevers et Dominique Simonet, « Le choix du remplaçant du F-16 sera tout aussi économique », *La Libre Belgique*, 16 mars 2017.
15.Chambre des Représentants de Belgique, Compte-rendu intégral avec compte rendu analytique traduit des interventions, Commissions réunies de l'économie, de la politique scientifique, de l'éducation, des institutions scientifiques et culturelles nationales, des classes moyennes et de l'agriculture et de la Défense Nationale, CRIV 54 COM 990, 24 octobre 2018.
16.Anne Bauer et Derek Perrotte, « La Belgique préfère le F-35 américain au Rafale et au Typhoon », *Les Echos*, 25 octobre 2018.
17.Joseph Trevithick, « Belgium Decides To Join The F-35 Club Over Competing Offers For European Fighter Jets », *The Drive*, 25 octobre 2018.
18.Roxana Tiron, « F-35 Jets for Turkey Held Back in Compromise Pentagon Bill », *Bloomberg Government*, 13 septembre 2018.
19.Andrea Shalal, « Germany drops F-35 from fighter tender; Boeing F/A-18 and Eurofighter to battle on », *Reuters*, 31 janvier 2019.
20.Antwort des Parl. Staatssekretärs Thomas Silberhorn auf die Frage des Abgeordneten Dr. Marcus Faber (FDP), Frage 49, Deutscher Bundestag Stenografischer Bericht 79. Sitzung Berlin, Plenarprotokoll 19/79, 13 février 2019.
21.Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Marcus Faber, Alexander Graf Lambsdorff, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/8311 – Tornado-Nachfolge und Zukunftsfähigkeit der Luftwaffe, Drucksache 19/9353, 9 avril 2019.
22.Joseph Trevithik, « The German Air Force Wants To Know If Its Eurofighters Can Carry U.S. Nuclear Bombs », *The War Zone*, The Drive, 21 juin 2018.
23.Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gerold Otten, Jens Kestner, Dietmar Friedhoff, weiterer Abgeordneter und der Fraktion der AfD – Drucksache 19/8744 – Tornado-Nachfolge und Konsequenzen, Drucksache 19/9402, 11 avril 2019.
24.Bojan Pancevski, In Germany, a Cold War Deal to Host U.S. Nuclear Weapons Is Now in Question », *The Wall Street Journal*, 12 février 2019.
25.« Saab haakt af als België kernwapens wil », *De Morgen*, 14 September 2015.

The Gripen Fighter: Present and Future Flight

Sweden started producing its own fighter aircraft after the Second World War. The succession of fighters counts to five jet fighter families, all developed and produced by Saab: Tunnan, Lansen, Draken, Viggen and Gripen.

The Viggen was produced in four versions: reconnaissance, sea surveillance, ground attack and air defence. Studies and research started in the 1970s for a replacement of the Viggen fighter. After assessing and abandoning other alternatives, the choice was made to go ahead with a Swedish solution. A decision was taken that what would become Gripen should be a multi-role fighter, optimizing the air defence capability. The Gripen development started with a concept study in 1979, and in 1982 with the first order to Saab, with the first flight in 1988. It was the first fighter to use a fly-by-wire flight control system. To solve this challenge became a serious problem in the early development. The first version, the A/B, became operational in 1996. The next version, the C/D, had its first flight in 1995, and became operational in 2004. By 2008, the last of the 204 ordered A/B and C/D Gripens was delivered to the Defence Material Administration (FMV), for further delivery to the Swedish Air Force. In 2013, FMV signed a contract with Saab for development of the E version. The E version is a one-seater, and the F a double seater. In 2019, the first E was delivered to FMV from Saab. On June 10, 2019, the first successful test flight was performed with the third[1] Gripen E test aircraft.

The plan is to deliver the first E/F:s to the Swedish and Brazilian Air Forces in 2021, and reach initial operational capability in Sweden by 2023, and full operational capability around 2025. 60 Gripen E have been ordered by the Swedish Air Force. Sweden has not so far ordered any units of the F version.

The Swedish government has declared three essential security interests: fighters (2014), underwater capability (2015) and "cyber and parts of C4I" (2017). The implication for Gripen is that Sweden will maintain a domestic capability for fighter development and capabilities, or as expressed in the official government policy: "to maintain national freedom of action regarding fighter aircraft ability and to be able to act without external constraint". As a consequence, this in practice cements Saab's presence in the fighter domain for decades to come.

Present status

♦ *C/D*

The now operative Gripen is the C/D version, with D being a double-seater. The latest modification package – MS20 – is the most comprehensive Gripen modification so far. The equipment and software is delivered and operational, and is under final implementation by Saab together with FMV. The primary capability upgrades with MS20 are the integration of the IFF Mod 5 version, integration of the Meteor missile software and an enhanced CBRN protection. Gripen C/D is planned to be operative until around 2027, in order to be replaced by the E version. There is however no formal decision to phase out the C/D at that time.

Compared to other nation's setup of upgrading fighters, Sweden has a different setup. Most nations upgrade their aircraft at long intervals, where the aircraft is practically being disassembled and most systems, components and features receive a profound upgrade or midlife upgrade up to a new version. The Swedish setup is to have less comprehensive but more frequent upgrades, compared to other nations' less frequent, more fundamental upgrades. An advantage of this is that the specialized engineers and developers engage in further technology and capability development at much shorter intervals – thereby maintaining competence and personnel at the cutting edge. Another advantage is that the production facilities will have a more even level of assignments. As expressed by FMV, more frequent modifications and upgrades also bring with it that sustained operational advantage is maintained over time. An estimate is that the Gripen update tempo is on average five times higher than for comparable fighters produced in other countries. This higher update tempo is also an adaptation to the fact that Gripen is produced in lower numbers than other fighters are. A disadvantage of the higher tempo is that it requires a continuously high level of administration together with more frequent processes and decisions in order to validate full operational capability.

♦ ***E/F***

The first Gripen E:s will be delivered to the Swedish Air Force in 2021, and are expected to be in initial operating capability operational use in 2023. It will be in operative use beyond 2040. What will happen after that is under discussion.

The step from A/B to C/D was not highly dramatic. The airframes were withheld to a high extent. The E/F should be seen as a new aircraft that builds upon the experience and knowledge from its predecessors and takes it to a new and higher level. The E/F will have a larger airframe that can carry a higher weapons payload. The E will also carry more fuel. It will have a new and stronger version of the General Electric F404 engine, which produces more thrust and paired with the increased fuel capacity highly increases the range of the aircraft. The E/F will not be a 'stealth' aircraft but is described as 'stealthy'.

The most dramatic capability boost – according to interviews - concerns its electronic warfare (EW) capability, which is intended to improve the operational advantage in combat air beyond visual range. The EW capability builds upon new Saab EW antennas, more advanced avionics integration and data fusion, a new Selex AESA radar, IR search and track sensors, and an increased capability for passive surveillance. Instead of having three displays in the cockpit, Sweden chose the integrated single display demanded by Brazil – co-developed by Saab and Brazil. The nozzles have in previous Gripen versions been hydraulically controlled with a separate oil system but will now use the jet fuel as hydraulic liquid.

The E will have two more pylons for carrying weapons, compared to C. The weapons suite will largely be the same as for the C/D, but with the strategically interesting addition of being able to carry a long-range precision weapon, likely the KEPD or the JASSM. This new proposed[2] capability enhancement of carrying a long-range precision weapon would make it possible to perform strike missions for strategic, fortified targets at long range. This can be understood as a proposed sharp doctrine enhancement, adding a higher threshold effect.

Gripen E will also have a new cockpit design. Overall, the avionics development in the cockpit and its data presentation strives to reduce the pilot's intellectual commitment to continuously engage in performing flying manoeuvres, and thereby enhancing the pilot's capability and capacity to continuously optimize tactical decisions and situational awareness. Naturally, this without compromising the aircraft's flight performance abilities. Furthermore, an overarching incentive is to facilitate shorter decision loops. The underlying avionics technology has been designed to separate the operational systems from the flight and safety critical systems. This gives, according to interviews, the advantage of fast upgrades and integration of new technologies through-life without disturbing the flight and safety-critical systems.

An interesting aspect is that the type certificate for the fighter engine was commissioned to GKN (previously Volvo flygmotor) for previous Gripen versions with the GE F404 version – named RM12. The E/F engine responsibility – GE F414[3] – is will be commissioned to GKN, Saab or General Electric.

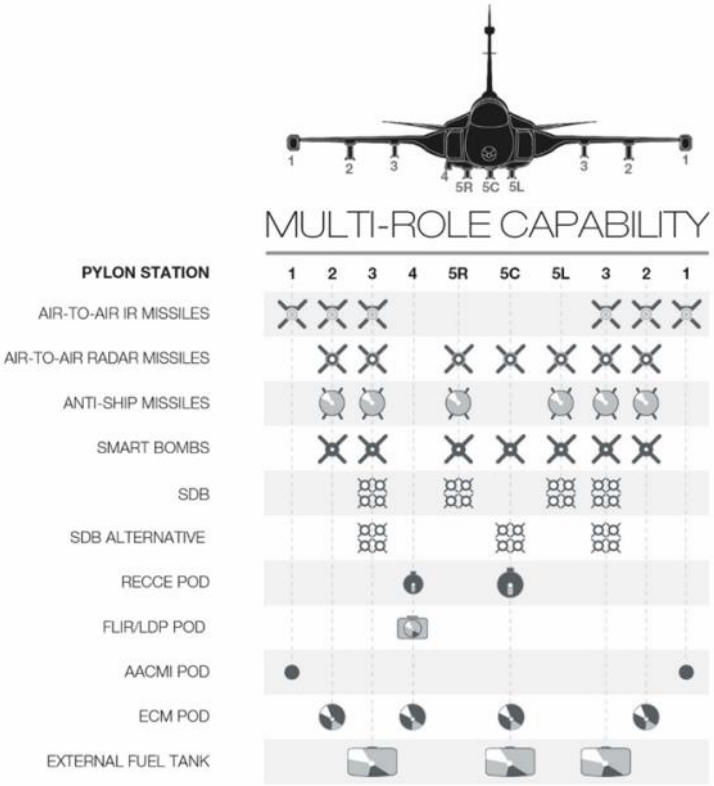


Figure: Gripen E weapons suite (Source: www.saabgroup.com)

No final decision is however taken at present. GKN is eager to receive this certificate in order to ensure a long-term presence (beyond 2040). GKN will in any case have the RM 12 certificate until at least at least the late 2030s and can thereby also sustain operational competence and full provide support to foreign users. If Saab is awarded this responsibility, they will have to build up a sufficient competence and infrastructure – likely building upon GKN's present capability. If General Electric is chosen, this has its advantage of not having to sustain a Swedish competence and infrastructure. Disadvantages with a GE solution are primarily two. Firstly, more profound design measures will have to be performed abroad by other European users, or in the US. Clearly, this will add uncertainties and time to the logistics functions. Secondly, Sweden will decrease its strategic autonomy and level of security-of-supply. This dilemma is a pending political question.

Export

The Swedish Air Force is presently flying the second version, the C/D. This version has also been exported to South Africa and Thailand[4] and is being leased to Hungary and the Czech Republic[5]. The UK has signed an availability contract to have access to one Gripen C/D for use in training. The C/D's for South Africa were co-produced with South Africa[6], the other nations have received surplus C/D's from the Swedish Air Force inventory[7]. The Swedish Air Force ordered a total of 204 C/D, and 40 of these are presently in service in other nations. The Swedish Parliament had decided in March 2000 to reduce the number of Gripen divisions from twelve to eight. Thereby more aircraft were delivered or under production than what the Air Force needed, and therefore a part of the inventory could be offered to other nations.

Saab have responded to procurement interests and is presently (June 2019) offering Gripen at various levels of capability to (at least) the following nations: the C/D version to Austria, Botswana, Bulgaria, Colombia, Malaysia, Philippines and Slovakia; and the E/F version to Canada, Finland, India and Switzerland[8]. Out of these prospective buyers, some are unlikely buyers, and others more promising from a Saab perspective. Paired to this, the Gripen users in the Czech Republic, Hungary and Thailand appear to be long-term Gripen users, and might acquire more aircraft. In South Africa, the Air Force performs limited operative use of its Gripen, apparently due to financing difficulties of operating its fleet.

Regarding its capabilities as a military platform, Saab and the Swedish Air Force stress that the Gripen enables more flexibility and a more decentralized decision making – pilots in other fighters have a narrower protocol for their tactical options and decisions. The Gripen E development has enhanced its Beyond Visual Range (BVR) capability. An extended situational awareness enables detection of threats earlier and at a longer range. The Meteor missile's BVR capability complements this capability.

The efficiency advantages related to cost and maintenance of Gripen – as being put forward by Saab and supporting Swedish government agencies and ministries – are its lower price, lower cost for maintenance and per flight hour, that it demands a smaller personnel turnaround structure and that the turnaround time (10 minutes) is much faster compared to its competitors.

Its competitors tend to stress that Gripen has one single engine (whereas most competitors have two), thereby adding risks if the single engine would fail. However, no engine failures have so far occurred under the Gripen lifetime. Another argument is that it has a limited range. Regarding range, the E/F version has profoundly extended its range with its increased fuel capacity, and it can also be air-fuelled.

The cost of a Gripen is clearly lower than its competing alternatives, on average 30-50 % lower. The competing alternatives for fighters are however difficult to compare. For one thing, different aircraft have their optimized performance, capabilities, range etc. – they can perform different things. Furthermore, nations' choice of fighters is not solely dependent on price and performance. A number of aspects become a part of the deal: e.g. technology transfer; offset of different kinds; support and commitment of the selling nation's Air Force, ministries and government authorities; maintenance and logistics issues; education and training; local investments; local production. How the selling company and its supporting government resources has performed in relation to previous exports will also strongly affect the product's attractiveness. The security policy element also becomes important, for example if a nation wants to have strong bonds with the US – or reversely to *not* become dependent upon the US. A fighter deal constitutes a security policy handshake between the selling nation and the buyer.

In October 2018, Boeing and Saab won the US Air Force order for the next US trainer aircraft, the T-X. In its first phase until 2023, the project will produce five T-X, and the program plans to produce 351 T-X aircraft. The system is planned to be fully operational by 2031 with all aircraft delivered. The aircraft is also likely to have very strong export potential, especially for the international F-35 users. Saab's share of the program is around 10 %, and its production will be undertaken in the US. Swedish procurement plans do not point to that the Air Force will acquire the T-X. Saab's engagement in T-X does bring with it a competition for advanced competence within Saab in relation to the same competence being directed to Gripen development. FMV and the Ministry of Defence keep a close watch on Saab not decreasing its priorities and resources needed for Gripen. According to interviews, Saab manages to balance these two large responsibilities.

Customer collaboration and development

♦ *C/D*

The present foreign users of the C/D version – the Czech Republic, Hungary, South Africa and Thailand – serve as an extended network for the continuous development of the C/D. According to interviews, the existing customers are the most important counterparts. They meet in different forms together with Sweden within the Gripen User group, where they exchange experiences and plan the implementation of upcoming upgrades. These users commit to selected parts of Swedish Gripen upgrades. It is in the interest of Saab and the Swedish Air Force to reach as much shared functionality as possible with foreign users – thereby creating cost-efficient synergies. They also submit important information about experiences from their use of Gripen. According to interviews, the Czech and Hungarian buyers have in a short time period transformed its Air Force from the Soviet legacy systems and are highly committed and motivated in reaching their new air power capabilities in a new security environment.

As stated above, Sweden has sold or leased out some of the acquired C/Ds. Presently, the Air Force inventory does not offer any more produced Gripen units to foreign customers. But if the Defence White book's outline is fully implemented, some 10-20 Gripens could become on offer, based on the outlined division structure. Saab could in theory produce more C/Ds, but the development and infrastructure is now geared for E/F, and a reactivation of C/D production is not plausible. If a very large export order for C/D would arise, I assume that a restart could be arranged.

♦ *E/F*

So far, Brazil is the only foreign buyer of the E/F. It ordered 36 aircraft (28 E and 8 F) in 2014 at a cost of SEK 38 billion. In this export setup, the E/F is co-developed and co-produced between Saab and Brazil, with Embraer as the main Brazilian counterpart. An underlying incentive for Brazil is to (in a longer time perspective) be able to have a national capability to develop and produce its own fighter aircraft. Therefore,

Saab performs (under its offset commitment) an extensive knowledge transfer and education program in order to raise the development competence in Brazil. Saab performs educational programs in Brazil for military personnel and engineers regarding e.g. innovation and product development organization; Brazilian engineers and pilots are trained in Sweden; Saab performs together with the Swedish Air Force training and education. Paired to Saab's extensive interaction with Embraer and other Brazilian companies, the Swedish Air Force also has intense interaction with the Brazilian Air Force. The shared Gripen development enables cost sharing, and synergies between national capabilities. Admittedly, the aggregate Swedish competence for building fighters and operating them is at a much higher level than Brazil's. It also appears likely that Brazil will order more Gripen E. One could argue, however, that the E/F "marriage" between Sweden and Brazil and the industrial and production integration to some extent reduces the afore-mentioned freedom of action for Sweden.

Operational collaboration and integration

In recent years, the Swedish Air Force has intensified its operative integration with other nations' air forces. Large, mutual, border-crossing exercises are performed regularly with neighbouring nations and with NATO constellations. The most intense interaction is with Finland, Norway and Denmark – in that order. Sweden is also a partner in the Baltic Air Policing Mission together with NATO countries. The Czech Republic and Hungary also contribute to this mission, and operative and logistics synergies between these three Gripen users are exploited.

Future Swedish capabilities

The Swedish parliamentary Defence Commission issued the Defence White book on May 14, 2019. The White book is issued every five years and structures the military priorities for the next defence planning period – in this case for the years 2021-2025. The Defence Commission's White Book by tradition becomes the outline for the next defence planning period; the defence ministry will largely implement it. Overall, the 2019 White Book is highly ambitious and changes the conditions and future of the Gripen fighter. The 2019 Defence White Book describes a deteriorated security situation since the previous 2014 White book that requires fundamental reinforcements of capabilities, personnel and equipment. The Armed Forces will according to the White Book's outline increase from 60,000 to 90,000 personnel until 2025.

One important suggestion in the White book is that the operative use of the C/D version should be extended from the planned year 2027 until around 2038. Thereby Saab will have around ten more years of maintaining the C/D capabilities. This extension of the C/D life is in order to strengthen the long-term air power capability and also to serve as a capability bridge across the first decade of the operative use of E/F. The C/D capability will be organized in C/D air force divisions, and the E in its separate divisions. Two more Air Force divisions will be added, increasing the number to eight. Furthermore, the double-seated D version will serve as the primary advanced trainer until at least 2038.

The parallel use of C/D and E presents opportunities as well as challenges. An opportunity is that it enables an extended capability spectrum with two aircraft versions that can perform different roles in the air defence. The C/D will not be a second-rate alternative to the E – the respective roles will be optimized for the best capability combination based on their respective performance and capabilities. A challenge is that having two different versions will lead to a larger logistics and maintenance footprint, with the two versions requiring partly differentiated resources, facilities and personnel. How these aspects can be implemented is presently not decided.
Another significant suggestion in the White book is to partly rebuild the dispersed base system. The Swedish Air Force had until the late 1990s an extensive infrastructure of dispersed, smaller bases where fighters could be refuelled and rearmed. These bases were placed all over Sweden and served as alternatives to the principal Air Force bases, where the divisions are stationed in peace time. Through this extensive base system, the fighter units could be served by mobile turnaround units - thereby creating dispersed turnaround capabilities and protection. This system was gradually reduced during a decade from around 2000 onwards. The bases can however to a certain extent be reactivated. In sum, this reactivation will improve the Swedish air power capability, but will also require considerable resources and bring with it logistical challenges.

European industrial restructuring

Presently in Europe, only Sweden and France have the domestic capability to be the full system integrator of a cutting-edge fighter. Globally we can add USA, Russia and China[9]. Sweden sources around half of its systems from foreign companies, primarily from the US, UK and Italy, in that order. France meets its sourcing needs almost entirely from national sources. The United Kingdom, Germany and Italy have abandoned their domestic capability as full system integrators. There are presently three European fighters for sale: Gripen, Rafale and Eurofighter. But what happens after the end of these fighters' lifetimes? Will all nations acquire American aircraft? Not likely.

Extensive and complicated discussions are presently undergoing concerning the future European fighter development capabilities. European combat aircraft manufacturers have laid out a vison for a European Future Combat Air System (FCAS, SCAF in French: Système de combat aérien du futur). The FCAS outcome is intended to take over after the end of the lifetimes of Eurofighter, Gripen and Rafale. The demands, specifications and timelines of the primarily concerned nations (France, Germany, Italy, Spain, Sweden and UK) are not synchronized. Firstly, the nations have different timelines for when to replace their fighters, when to order and when have new fighters in operational use. Secondly, the UK will operate the F-35 for many years to come and strives to develop an aircraft (i.e. their aspired FCAS solution) that complements the F-35 with different performance and capabilities. France and Germany strive to develop an aircraft with similar performance and capabilities as the F-35. The Gripen E's lifetime extends a bit longer than the replacement needs of the other nations. Thus, a tricky and complex negotiation is ongoing.

France and Germany in 2017 initiated a mutual demonstrator program in order to develop a future fighter together, under the umbrella name SCAF. Spain joined the project in February 2019. According to the present tentative outline, France and Dassault will be the primary integrator of this concept.

The United Kingdom have through its strong integration into the Joint Strike Fighter/F-35 program largely bound its fighter development resources for many years to come. Lockheed Martin and the US have also through its F-35 sales in Europe (and elsewhere) bound buyer nation's fighter procurement finances to a large extent. However, the UK presented its FCAS vision – the Tempest sixth generation fighter demonstrator – at the Farnborough Air Show in June 2018. The UK at the same time expressed that Sweden and Saab would be an attractive partner. Italy's Leonardo expressed in March 2019 its interest to be a partner in the program. Saab has expressed an interest and is also courted by the SCAF constellation.

The Franco-German-Spanish SCAF project has compared to Tempest a firmer and more developed structure at present. The latter does not have as firm government declarations and commitments.

This entire complexity regarding an expected restructuring and fusion of national industrial and development capabilities regarding fighters has many possible outcomes. There is immense political prestige and interest in the outcome of the expected restructuring process. Each nation wants to maintain as much strategic autonomy as possible. Each nation wants to sustain domestic, advanced development of such a highly strategic military platform. Each nation aims for a position on as high a tier as possible in the tiered integration hierarchy for fighter aircraft. To maintain the national industry and all the high-tech employment it brings is also a strong political incentive. Added to these national incentives, there is a shared European incentive to maintain Europe's strategic autonomy and to minimize dependency on the US.

So where does Saab and Sweden fit into the equation? High-level discussions and negotiations concerning SCAF as well as Tempest are performed at present with all concerned parties in industry, Air Forces and government. If partnering with the UK Tempest program, Saab has a strong negotiation position in having the capability as full system integrator. The UK and BAE Systems has a strong position with its home government likely ordering a much higher number of aircraft. Saab and Sweden have not committed (to my knowledge) to any alternative or constellation. We should not foresee that two final programs – SCAF and Tempest – already have been formed and serve as the only two alternatives. It is also plausible that France and Germany will not go through with their shared initiative. And of course, the US also has an interest to help to orchestrate an outcome that will be favourable to them – perhaps they will divide and conquer.

Dr Martin LUNDMARK
Swedish Defence University

The analysis in this text is based on an assessment by the author as an academic researcher at the Swedish Defence University. It does not represent an official statement of a Swedish government authority.

Notes

1.Three test versions of Gripen have been produced. These three have been gradually modified over the versions, based on the experiences from testing with the preceding version. So this the first flight with the most developed and advanced Gripen E Test aircraft.
2.Proposed in the 2019 Defence White Book, described at the end of this article.
3.The same engine as in the latest F/A Super Hornet version.
4.South Africa signed a contract in 1999 to acquire 28 Gripen C/D, later reducing the number to 26. Thailand signed a contract in 2008 to acquire six Gripen C/D, and extended the order in 2009 to six more.
5.Hungary signed a contract in 2003 to lease 14 Gripen C/D for ten years. In 2012, Hungary signed a contract for ten more years. The Czech Republic signed a contract in 2004 to lease 14 Gripen C/D for ten years. In 2013 it was announced that the leasing was prolonged until 2029.
6.The South African company Denel produced parts of the rear fuselage.
7.The Swedish Air Force ordered a total of 204 Gripen C/Ds, but later declared that it needed 100. Thereby a pool of surplus C/Ds became available for export.
8.This list of nations is likely not entirely true. Some nations can be omitted, and some can be added. Some nations have previously declared their choice of an aircraft other than Gripen, and thereafter rumors start to circulate in defense press, claiming that they are revising their previous declarations. Furthermore, some nations previously declaring intent may be showing diminishing commitment to acquire new aircraft at all. Thus, this list is tentative and is based on my assessment, based on interviews and articles in defence press.
9.China's ability to bring a cutting-edge fighter to full operational capability still needs to be proven.

Export russe des systèmes anti-aériens S-400 : intentions stratégiques, atouts industriels et politiques, limites

Sergei Karpukhin/REUTERS

L'industrie de défense russe bénéficie de longue date de positions fortes sur le marché d'exportation de systèmes anti-aériens. Cette problématique s'est dernièrement réaffirmée sur le devant de la scène internationale du fait de la signature de différents contrats d'exportation du S-400 politiquement notables (Chine, Turquie, Inde) et de l'intérêt pour ce système qu'auraient exprimé plusieurs pays, dont certains ne sont pas des clients traditionnels de l'industrie russe (pays du Golfe notamment). A l'heure où, d'après les Russes, la Turquie commencera à recevoir, comme prévu, ses S-400 en juillet prochain, il convient de faire un point aussi précis que possible sur un sujet qui, comme beaucoup d'autres concernant la défense et l'industrie d'armement russes, fait l'objet de nombreuses conjectures, de jeux de communication voire de désinformation de diverses origines, et, en définitive, d'un « brouillard » sans doute en partie organisé.

Des contrats politiquement marquants

Ces dernières années ont en effet vu la signature de contrats particulièrement marquants d'un point de vue politique. La Chine est devenue le premier acquéreur étranger du S-400 avec la signature du contrat pertinent en 2015 ; il est actuellement en cours d'exécution. Le contrat avec l'Inde a, quant à lui, été signé en octobre 2018. Ces deux transactions soulignent l'importance du « vecteur asiatique » dans l'actuelle politique étrangère de la Russie – et de la nécessité, dans l'esprit du Kremlin, de poursuivre cet axe de manière équilibrée. Entre ces deux contrats, la Turquie a elle aussi opté pour l'achat du S-400, en 2017. Malgré la polémique et les tensions avec ses alliés de l'OTAN que cette décision suscite, Ankara semble déterminée à aller au bout de son projet, et des personnels militaires turcs seraient déjà en formation en Russie. L'on notera également qu'une bonne dizaine de pays ont exprimé leur intérêt pour le S-400, pays dont certains ne sont traditionnellement pas des clients de l'industrie d'armement russe (monarchies du Golfe). La liste des clients potentiels fait d'ailleurs la part belle au Moyen-Orient, ce qui permet au moins à Moscou d'étayer l'idée de son retour dans la région comme acteur central (ce même si les perspectives semblent assez hypothétiques pour beaucoup d'entre eux – Arabie saoudite, Qatar[1], Bahreïn, Emirats arabes unis, mais aussi Irak, Syrie, Egypte, Algérie, Maroc, Iran…)[2].

Vases communicants : succès à l'export et visibilité des systèmes anti-aériens au cœur de la Défense russe

L'attention de la communauté internationale sur ces transactions a évidemment été attisée par le fait que la Russie, ces dernières années, a installé des S-300 et des S-400 en plusieurs zones stratégiques pour l'institution militaire russe (Kaliningrad, Crimée, Grand Nord, Extrême-Orient…). Les S-400 ont également été déployés en Syrie, même s'ils n'ont pas été activés. Ces systèmes sont des composantes essentielles des bulles A2/AD qui préoccupent vivement les stratèges occidentaux, inquiets du durcissement opératif des environnements dans lesquels les forces occidentales sont amenées à travailler.

L'énergie déployée ces dernières années pour assurer la dotation des forces armées russes en systèmes S-400 est logique compte tenu des orientations prioritaires de la politique de défense russe. Celle-ci, depuis de longues années, est marquée par la prise en compte d'une vulnérabilité clef pour le pays, selon ses responsables militaires, à savoir le risque de frappes aériennes et de missiles de croisière contre des infrastructures vitales – installations militaires, centres administratifs, sites économiques stratégiques ou nœuds de communication. Le fait que les objectifs de dotation des forces en S-400 tels qu'ils avaient été fixés pour 2020 soient en passe d'être atteints[3] renforce au passage l'image de fiabilité des industriels qui servent la commande – même si cela ne préjuge pas de l'efficacité opérationnelle réelle du S-400.

La « diplomatie du S-400 »[4] : une politique export conforme à la politique extérieure de la Russie

La propension de la Russie à diffuser ses technologies anti-aériennes sophistiquées marque une évolution importante puisqu'il y a encore quelques années, le gouvernement russe

affichait une approche prudente concernant l'export de systèmes anti-aériens de la gamme S-300 et disait ne pas vouloir exporter les S-400. Il prenait davantage en compte qu'aujourd'hui le coût politique possible de la cession de ces systèmes à certains acteurs. Les questions de respect de la propriété intellectuelle étaient également prises en considération (les autorités russes ayant observé que le HQ-9 chinois était quelque peu « inspiré » du S-300)[5]. En outre, des contraintes liées à l'état de l'outil industriel et à la priorisation de la commande nationale contribuaient évidemment à cet état de fait.

Aujourd'hui, la position de la Russie sur le sujet a évolué, pour plusieurs raisons qui sont pour le Kremlin des motivations de premier ordre, au-delà des seuls enjeux de nature commerciale. D'une part, elle intègre clairement la problématique du bras de fer stratégique qui l'oppose aux Etats-Unis et à l'OTAN. La diffusion de la technologie anti-aérienne russe la plus sophistiquée doit donner corps à l'idée de la fin du *leadership* international de ces derniers dans le domaine militaire en laissant entrevoir un durcissement, dans plusieurs directions stratégiques, des environnements opératifs dans lesquels leurs aéronefs et missiles de croisière pourraient être amenés à opérer. D'autre part, elle s'inscrit dans l'effort de Moscou visant à diluer la solidarité de ce qu'elle voit comme le « bloc occidental » en cherchant à le diviser. On voit bien les problèmes que pose à l'OTAN la question de l'acquisition par la Turquie du S-400... Enfin, elle compte parmi les arguments mobilisés par le Kremlin pour étayer ce qu'il présente comme le déclin de l'autorité internationale des pays occidentaux. On peut ainsi lire dans la presse russe que si les pays du Golfe envisagent d'acquérir des systèmes aussi stratégiques auprès de la Russie, c'est probablement qu'ils ne sont pas très confiants dans leurs relations avec les Etats-Unis ou dans la technologie militaire occidentale, ou encore que leurs partenaires occidentaux ne leur proposent pas des conditions de coopération industrielles suffisamment attrayantes…

Par ailleurs, la longue liste de clients potentiels pour le S-400, de même que l'inquiétude des Occidentaux sur les dispositifs anti-accès dans lesquels s'inscrivent les S-300 ou les S-400, permettent, du moins c'est ainsi que le conçoivent les Russes, de donner de la Russie l'image d'une puissance technologique et industrielle de premier ordre. Et de faire mentir les propos de Barack Obama, qui disait en 2014 que « *Russia makes nothing* », ce qui se voulait une référence au poids des ressources du sous-sol dans l'économie et dans les exportations de la Russie, ainsi qu'à sa faible présence sur les marchés internationaux de haute technologie. Cet aspect concerne peut-être, aussi, la Chine, même si Moscou s'applique à ne rien dire de négatif sur son partenaire stratégique chinois. Certaines sources russes pointent en tout cas le souci de répondre à la concurrence chinoise sur le segment anti-aérien pour expliquer le choix russe de diffuser la technologie S-400[6].

In fine, la valorisation par les autorités russes d'un succès commercial international (même si rien n'indique que les trois contrats précédemment signés seront suivis de nombreux autres) sur le S-400 crédibilise en creux la posture de défense russe face à l'OTAN et aux Etats-Unis. Elle permet aussi aux autorités russes de faire un pied de nez aux Occidentaux, qui ont infligé des sanctions à Almaz-Anteï, sanctions qui sont souvent présentées dans la presse russe comme un moyen pour les Occidentaux d'étouffer un concurrent[7].

Un effort à la hauteur des enjeux

L'importance de ces multiples enjeux, auxquels s'ajoute celui du marché de la modernisation des S-300, a amené l'Etat russe, en partenariat avec Almaz-Anteï, à se donner les moyens de les satisfaire. Suite à une décision de 2011, les capacités d'Almaz-Anteï ont été considérablement renforcées[8]. Deux nouvelles usines ont ainsi été établies à Kirov et à Nijniï-Novgorod (« Usine de Nijniï-Novgorod des 70 ans de la Victoire », qui devrait recruter au total 3 000 personnes[9]) en vue de disposer de capacités de production suffisantes pour à la fois assurer la commande de défense (*gosoboronzakaz*), priorisée, et consolider les positions d'Almaz-Anteï sur les marchés export. Selon une source, les deux nouvelles installations seraient beaucoup plus automatisées que les capacités existantes. Cet effort a été en avant par des experts russes quand il s'est agi de convaincre que la réduction des délais pour la réalisation du contrat turc ne poserait pas de problème (la Russie a accepté de proposer un calendrier resserré de livraisons, livraisons qui devraient ainsi commencer en juillet 2019 au lieu du premier trimestre 2020). L'investissement cumulé dans ces nouvelles capacités, aux-quelles il faut ajouter le Centre nord-ouest (parc technologique situé à Saint-Pétersbourg), représenterait environ 120 milliards de roubles, dont 104 (approximativement 1,5 milliard USD) sur financement propre d'Almaz-Anteï[10], qui a aussi investi plus de 30 milliards de roubles dans la modernisation de l'usine Oboukhov, le fabriquant du S?350 (sur ce produit, voir *infra*)[11]. Selon le constructeur général d'Almaz-Anteï, le groupe a procédé à la modernisation de pratiquement toutes les principales usines engagées dans la production en série des missiles de systèmes anti-aériens[12]. Le même évoque enfin l'établissement en cours d'une ligne de production nouvelle à Oulianovsk (notamment microélectronique)[13]. Le tout doit être accompagné d'un plan de rationalisation des dépenses, qui devrait passer par la vente de certaines usines et des licenciements. Ces efforts offrent certainement à Almaz-Anteï une plus grande réactivité pour les clients étrangers. Le groupe a également travaillé à aplanir les difficultés, assez traditionnelles dans l'industrie russe, dans les coopérations entre les acteurs de l'industrie – bureaux d'étude, usines…

Au niveau politique, l'Etat russe accompagne le mouvement en insistant sur l'absence de conditionnalité politique dans le cadre des contrats d'armement – qu'elle porte sur la nature des régimes dans les Etats clients ou sur leurs inimitiés/affinités géopolitiques. Il montre aussi, sur ce segment comme sur d'autres, une propension à donner des coups de pouce financiers. Par exemple, l'achat des S-400 par la Turquie est financé à un peu plus de 50 % par un prêt russe.

L'Etat russe et Almaz-Anteï : échange de bons procédés

Le rôle de l'Etat dans la promotion des S-400 est donc visible et actif. Almaz-Anteï relève d'ailleurs de Rostec, groupe public tentaculaire concentrant près des 2/3 de la production militaire en Russie et dont le PDG, Sergeï Tchemezov, est un proche de Vladimir Poutine depuis l'époque où les deux hommes officiaient en RDA comme membres du KGB. Pour Almaz-Anteï, la forte visibilité médiatique des contrats à l'exportation du S-400, effectifs ou potentiels, est tout bénéfice. Souvent appuyée par les articles dithyrambiques sur le système russe dans la presse spécialisée occidentale, cette visibilité permet de nourrir une image d'excellence et de créer la confiance sur l'ensemble de sa gamme de produits. Le calcul du groupe semble être que la disponibilité sur les marchés à l'export et le succès du S-400 au travers de quelques contrats marquants sont de nature à servir la réputation de ses autres produits et nourrir ainsi la demande export, ce dans un contexte où se profile à l'horizon le marché de la modernisation des S-300. Il s'agit notamment de mettre en valeur le nouveau système S-350 Vityaz[14]. En développement depuis 2009, il a été conçu sur la base des coopérations intervenues dans les années 2000 entre Almaz-Anteï et la Corée du Sud sur le KM-SAM. Le début de sa production en série a été annoncé en avril 2019. Dans les forces russes, il doit remplacer les S-300PS, produits dans les années 1980 ; moins coûteux que le S-400 et le S-500, il est supposé apporter un complément utile aux forces nationales. Il est également espéré qu'il intéressera les armées étrangères opérant déjà des S-300 ou des S-400 et constituera une option pour les pays aux budgets de défense relativement modestes[15].

La mise à disposition sur le marché mondial du S-400 suggère aussi que les autorités russes sont confiantes que le programme de montée en gamme, le S-500, pourrait bientôt arriver à maturité[16]… ou elle aide à convaincre que c'est le cas même si cela ne l'est pas –, ce dans le souci d'impressionner les adversaires militaires et commerciaux de la Russie. En tout état de cause, la publicité indirecte qu'offrent les tensions internationales liées à l'export de S-400 permet à Almaz-Anteï de faire oublier ou de gommer certaines difficultés, comme les retards dans la mise en service de certains produits phare (dont le S-350 et le missile intercepteur longue portée du S-400, le 40N6, censé être enfin opérationnel depuis 2018), ou les problèmes apparemment rencontrés au niveau du MCO d'Almaz-Anteï ainsi que certaines limites technologiques (circuitique). On notera aussi ici que des spécialistes occidentaux émettent des doutes quant à certaines fonctionnalités du système et pointent des vulnérabilités de divers ordres[17].

Contrats ou pas, la Russie gagnante ?

Si les contrats avec la Chine, l'Inde et la Turquie revêtent une forte portée politique et symbolique, des questions se posent sur la possibilité pour Almaz-Anteï de réaliser d'autres ventes pour le S-400. On peut notamment s'interroger sur les déclarations d'intérêt en provenance du Golfe. Par exemple, l'Arabie saoudite a plus d'une fois fait miroiter de grands contrats d'armement avec la Russie sans que ces projets se soient matérialisés. Ryad tend en effet à utiliser ces possibles transactions comme un levier dans des négociations plus larges – avec la Russie, avec les Etats-Unis… – ou dans son rapport de forces avec ses rivaux régionaux. Beaucoup des autres possibles clients sont peu ou pas solvables, ou ont un dispositif de défense dominé par les équipements occidentaux.

La pression extérieure sera une variable importante. Elle est particulièrement pressante du côté des Etats-Unis, qui évoquent des problèmes de compromission de certaines données pour le moins sensibles dans le cas de pays – Inde, Turquie – disposant de matériels aéronautiques d'origine américaine (via le dispositif *Identification Friend or Foe*)[18]. Le *Countering America's Adversaries Through Sanctions Act* (CAATSA) est évidemment invoqué. Washington a mis en question les coopérations avec la Turquie sur le F-35. L'Inde est menacée de conséquences négatives pour l'avenir des liens de défense avec les Etats-Unis, qui lui proposent des alternatives[19]. La Chine, quant à elle, a déjà essuyé des sanctions pour avoir acquis le S-400 (et le Su-35)[20]. Ces trois pays, soucieux d'affirmer leur souveraineté, pourraient ne pas céder. La pression américaine pourrait, en revanche, dissuader plusieurs autres clients potentiels. La Russie ne se privera pas de dénoncer les sanctions extra-territoriales américaines et, le cas échéant, de mettre en exergue les éventuelles différences de traitement, toujours dans le souci de rogner la réputation des Etats-Unis (Washington est en effet susceptible de, pour des raisons géopolitiques, ne pas soumettre au même type de sanctions les différents acquéreurs du S-400).

Mais, en définitive, pour le gouvernement russe comme pour Almaz-Anteï, l'effet d'image produit par les nombreuses déclarations d'intérêt et les tensions internationales autour du S-400 est en soi gratifiant, voire bénéfique dans une certaine mesure : tout en véhiculant l'image d'une Russie influente tous azimuts sur la scène internationale, il porte la réputation des produits de l'industrie d'armement de la Russie et projette l'idée, déjà bien ancrée, de la solidité de ses capacités de défense…

Isabelle FACON
Directrice adjointe, Maître de recherche, FRS
i.facon@frstrategie.org

Notes

1.On notera que l'Arabie saoudite a menacé le Qatar de représailles militaires s'il faisait l'acquisition du S-400, adressant même une lettre en ce sens au président français apparemment doublée d'appels similaires aux autorités américaines et britanniques… (Vladimir Karnozov, « Russian S-400 SAM System Causes Middle East Upsets », www.ainonline.com, 6 juin 2018 ; Benjamin Barthe, « L'Arabie Saoudite menace le Qatar d'une 'action militaire' s'il se dote de missiles S-400 », L*e Monde*, 1er juin 2018).

2.Sont évoqués, parmi les autres acheteurs potentiels, et là aussi de manière plus ou moins crédible selon les cas, la Serbie, le Vietnam, le Pakistan, des pays de l'ex-URSS… Sur l'Iran, la position officielle de Moscou est qu'il n'y a pas eu de requête en ce sens de la part de Téhéran. Pour un panorama très complet et critique des transactions conclues ou à l'étude, voir « Le S-400 à l'export ? », Red Samovar, 17 juin 2018.

3.Fin 2018, les forces russes avaient reçu 54 des 56 divisions de S-400 prévues aux termes du Programme d'armement 2011-2020. Selon certains spécialistes russes, elles pourraient en recevoir encore une vingtaine de divisions, après quoi le producteur passera à la modernisation des premières séries livrées (Ilia Kramnik, « Vmesto S-400 : kakie sistemy PVO boudout zakoupat' rossiïskie voennye » [A la place des S-400 : quels systèmes anti-aériens achèteront les militaires russes], *Izvestiia*, 3 mai 2019).

4.Pour reprendre l'expression d'un spécialiste russe des questions militaires, Alexandre Golts, « La diplomatie du S-400 », *Le Courrier de Russie*, 26 juillet 2018.

5.La Russie semble cependant toujours soucieuse de protéger sa technologie. Apparemment, le client turc n'a pas obtenu satisfaction sur la perspective d'une production sous licence du S-400 en Turquie, et on se souvient qu'il y a eu des désaccords entre les deux pays sur la question des transferts de technologies. L'accès à l'électronique du système serait « *jalousement gardé par la Russie* » (A. Golts, op. cit.).

6.Mikhail Barabanov, « Russian Air Defense Systems on the Global Markets », *Moscow Defense Brief*, janvier 2014.

7.Voir par exemple « Oboronka RF pod oudarom » [L'industrie de défense sous les coups], Rambler, 26 janvier 2017.

8.Leonid Nersisian, « Potchemou vajen vvod v stroï dvoukh novykh zavodov kontserna VKO 'Almaz-Anteï' ? » [Pourquoi la mise en service des deux nouvelles usines d'Almaz-Anteï est-elle importante ?], regnum.ru, 3 mars 2017.

9.« Russian Company Almaz-Antey to Invest $1,7 billion to Build New Facilities », TASS, 30 mars 2016.

10.Ibid.

11.Le président Poutine s'était fait présenter le S-350 lors d'une visite à cette usine à l'été 2013 (« State Trials of Vityaz Missile System to End by 2015 – Almaz-Antey Exec », Interfax-AVN, 24 janvier 2014 ; « Over 30 bln Rubles Invested into Obukhov Enterprise Upgrade », ITAR-TASS, 16 mai 2018).

12.« Novymi sanktsiiami nas ne napougat' » [Personne ne peut nous impressionner avec de nouvelles sanctions], gazeta.ru, 29 novembre 2017.

13.Ibid.

14.Le nouveau programme d'armement 2018-2027 prévoit l'acquisition par les forces armées de systèmes S-350 et S-500.

15.Ilya Kramnik, op. cit.

16.La campagne d'essais a été déclarée achevée fin avril 2019. Dans le cadre du programme 2011-2020, l'armée russe devait recevoir dix divisions de S-500, à partir de 2017, un objectif qui n'a pas été tenu. Aujourd'hui, il est estimé que la première division pourrait être prête début 2020. L'armée russe pourrait acquérir 20-30 divisions de ce système pour assurer la protection de la capitale, d'autres grands centres industriels et de communication, ainsi que les forces nucléaires stratégiques (Ibid.). La Turquie aurait exprimé son intérêt pour ce système.

17.Voir par exemple Robert Dalsjö, Christofer Berglund, Michael Jonsson, *Bursting the Bubble? Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*, FOI (Stockholm), 2019.

18.« Russian S-400 System Requires Friendly Aircraft Data to Identify Friend or Foe », www.defenseworld.net, 16 mai 2019.

19.« India's Buying of S-400 from Russia will Have Serious Implications on Defence Ties: US », *The Economic Times*, 31 mai 2019 ; « After Turkey, India Offered US Missile Defense Systems as an Alternative to Russia's S-400 », www.defenseworld.net, 14 mai 2019.

20.Franz-Stefan Gady, « US Sanctions China over Purchase of S-400 Air Defense Systems, Su-35 Fighter Jets from Russia », *The Diplomat*, 21 septembre 2018.

L'évolution du contexte spatial américain*

Des investissements encore inégalés à ce jour continuent de faire des États-Unis la première puissance spatiale dans le monde. Cette première place repose sur les deux piliers que sont l'exploration spatiale habitée et le développement de l'espace militaire. L'époque récente s'est même caractérisée par une croissance des dépenses militaires liée à un sentiment croissant de vulnérabilité face à la montée en puissance de la Chine et le maintien par la Russie de capacités importantes. En parallèle, l'émergence d'une nouvelle industrie spatiale à vocation plus directement commerciale s'est exprimée à travers des entreprises emblématiques comme Space-X ou Blue Origin dans le domaine du lancement. Les applications spatiales connaissent aussi des évolutions avec l'espoir pour les investisseurs de nouveaux débouchés dans le secteur de l'information. Mais le soutien apporté par l'État apparaît indispensable pour garantir le succès de ce qui reste encore un pari industriel incertain.

Du point de vue gouvernemental, et en dépit d'effets d'annonce parfois déroutants, l'activité spatiale américaine reste marquée sous l'administration Trump par deux grandes tendances : la consolidation d'un programme d'exploration habité qui demeure structurant pour l'industrie et la poursuite d'un effort militaire inégalé, qui, à la fois, nourrit et tire parti des avancées d'une nouvelle économie spatiale.

Le secteur industriel spatial américain se trouve ainsi consolidé dans ses fondements mêmes en même temps qu'il étend ses relations avec le monde des technologies de l'information. Cette interaction de deux cultures différentes, voire de deux mondes étrangers, apparaît sans doute comme l'une des nouveautés formelles (à défaut de l'être au fond) les plus radicales de ces dernières années pour tout observateur assidu du secteur spatial américain.

Un resserrement de la stratégie spatiale américaine sur l'exploration habitée

Le programme spatial civil a toujours été sensible aux aléas politiques. Plus précisément, l'exploration humaine de l'espace n'a existé qu'en rapport avec des conjonctures extérieures qui lui donnaient ponctuellement une valeur particulière. Ce fut le cas pour la course à la Lune.

Cela a été également vrai avec la décision d'engager puis d'accélérer le programme de la station spatiale internationale, voire avec la décision de relancer l'exploration lunaire avec le programme Constellation annoncé en 2004 par George W. Bush. Mais, en dehors de ces périodes spécifiques, le thème de l'Homme dans l'espace n'a, en général, présenté que peu d'attrait politique aux États-Unis. Le programme de la navette spatiale n'a été décidé en 1972 par Richard Nixon que pour éviter de coûteuses fermetures d'usines dans un contexte électoral tendu, alors que l'engouement pour Apollo était retombé. La station spatiale, elle-même, a parfois connu des temps difficiles à la fin des années 1980 avec des risques d'annulation au Congrès. Et au cours des années récentes, les mêmes difficultés se sont manifestées avec l'arrivée au pouvoir de Barack Obama.

Les débuts de la présidence démocrate se sont traduits par l'abandon du programme du retour sur la Lune annoncé par son prédécesseur républicain. L'espace habité passait alors avec difficulté le test de l'alternance politique et se trouvait en butte aux critiques des défenseurs des programmes sociaux, le cœur même de l'électorat du nouveau président. Celui-ci prit la décision d'annuler le programme dès les premiers mois de son mandat. La nécessité d'augmenter le budget du programme lunaire de 3 milliards de dollars par an, selon l'étude d'un panel d'experts missionnés par le président, suffira à justifier cette mesure. La Lune ne présentait plus suffisamment d'intérêt (« *déjà fait* », dira Obama) pour pouvoir endosser la vision du président républicain.

Mais le choix fut aussi tactique, Barack Obama subissant les mêmes contraintes que ses prédécesseurs. Un des grands directeurs de l'administration spatiale américaine, doté lui-même d'une vision assez critique de l'Homme dans l'espace, estimait en effet, dans les années 1970, qu'« aucun président ne pourrait jamais sortir les États-Unis du vol habité ». La charge symbolique reste lourde et place chaque exécutif dans la situation de devoir « gérer au mieux » ce type d'engagement. Il n'en a pas été différemment pour l'administration Obama. Et c'est par choix tactique qu'en même temps que se confirmait l'annulation du programme du retour sur la Lune, la présidence démocrate prit soin, sous la pression

*Article publié dans *Réalités industrielles*, Mai 2019, Annales des Mines, pp.21-24

du Congrès, de confier à la NASA un effort d'investissement à long terme dans un lanceur lourd (le *Space Launch System*, ou SLS, dont on attend le premier vol pour 2020) et un véhicule « à tout faire » (*Multi-Purpose Crew Vehicle*, ou MPCV devenu depuis *Orion*) appelé à préparer les premières étapes d'un voyage martien à un horizon non spécifié. En parallèle, la NASA a été invitée à passer ses premiers contrats dits de « services commerciaux de transport en orbite » (COTS) dès 2006, permettant ainsi à de nouveaux acteurs tels que Space -X ou Orbital ATK (qui sera ensuite repris par Northrop Grumman) d'émerger comme de nouveaux entrants capables de devenir des partenaires de l'agence au-delà du rôle classique de sous-traitant. L'ambition pour l'administration était de réduire au silence les critiques républicains qui commençaient alors d'accuser la présidence démocrate de saper la base industrielle américaine. La décision prise montrait précisément l'inverse et allait même jusqu'à faire de la Maison Blanche le soutien de l'industrie la plus moderne et la plus compétitive. Ce mouvement tactique magistral eut l'effet politique escompté privant l'opposition de tout moyen de critiquer les orientations spatiales d'un président qui pouvait par ailleurs se prévaloir d'avoir mis fin à des dépenses lunaires jugées excessives par son électorat.

Cette position a eu des conséquences durables au plan industriel. Au programme COTS succédera un premier programme concernant le transport d'équipages vers la station spatiale. Ce programme CCDev (*Commercial Crew Development*) a été initié en 2009, puis renouvelé en 2012. Il apportera une première tranche de 440 millions de dollars à Space X, presqu'à égalité avec Boeing (460 millions). Puis une version renouvelée du contrat conduira, en 2014, à verser à Boeing 4,2 milliards de dollars contre 2,6 milliards à Space-X qui s'affichait ainsi comme le *leader* de la « nouvelle industrie » dans l'activité de lancement. Une troisième vague de contrats concernant cette fois le réapprovisionnement de la station spatiale à compter de 2019 jusqu'à sa fin de vie supposée intervenir en 2024 (*Commercial Resupply Service 1* et *2*) a confirmé en 2016 l'installation de Space-X et d'Orbital ATK comme principaux prestataires de transport par capsules (respectivement Dragon pour Space-X et Cygnus pour Orbital ATK) avec un montant global de 14 milliards de dollars au titre de la rémunération de leurs services[1].

Cette période Obama a placé la NASA dans une position délicate que créait pour elle la perte apparente d'objectifs à moyen terme. L'annulation du programme du retour sur la Lune, couplée à l'émergence de prestataires privés, a remis en question le rôle de l'agence. Les projets lointains de « redirection » d'astéroïdes pour évaluer l'intérêt d'une exploitation de ressources *in situ* ou les idées très hypothétiques de tests d'atterrissage sur Phobos, une des lunes de Mars, n'ont pas suffi à cette époque à structurer une véritable vision de long terme.

À l'issue du mandat de Barack Obama, l'agence devait retrouver en urgence un plan susceptible de convaincre l'exécutif et les parlementaires. Alors que le nouveau pouvoir encourageait l'idée d'un retour vers la Lune, prenant ainsi le contrepied de l'administration précédente, les responsables de la NASA ont pu imposer l'idée d'une nouvelle station circumlunaire destinée cette fois à permettre un retour durable sur la base d'une idée originale. Cette idée ira nourrir la première directive spatiale de l'administration Trump qui appelle « au retour d'humains sur la Lune pour une utilisation et une exploration sur le long terme, suivi de missions humaines vers Mars et d'autres destinations[2] ». Sans bien sûr que ce texte court aux contours vagues puisse faire office de plan spatial, il a redonné à la NASA un élan fédérateur et un rôle identifiable. De ce point de vue, et sans juger d'objectifs scientifiques qui peuvent être contestés, cette évolution traduit un succès de l'Agence qui réapparaît comme un acteur central doté d'un véritable poids politique dans ses relations avec les acteurs industriels émergents. Ceux-ci ne semblent d'ailleurs pas s'y tromper en réaxant certains de leurs discours sur l'objectif lunaire, qu'il s'agisse de la communication d'Elon Musk concernant les premiers voyages d'amateurs fortunés vers la Lune, ou, plus sérieusement, l'annonce par Jeff Bezos, au travers de sa société Blue Origin, de plans destinés à soutenir cet effort, notamment sur le plan logistique.

L'espace et le monde de l'information

Les transformations des rapports de force industriels aux États-Unis n'ont pas seulement affecté le secteur du lancement. Un trait frappant de ces dernières années a été l'efflorescence de nombreuses « jeunes pousses » dans le champ des applications spatiales. C'est d'abord dans le domaine de l'observation de la Terre que ces *start-ups* sont apparues à l'aube des années 2000, pour certaines d'entre elles. Le mouvement concentré en Californie est d'abord apparu comme une nouvelle étape d'un processus de commercialisation des services spatiaux mis en place dès les années 1990 par l'administration Clinton[3]. Suite à cette volonté d'installer l'industrie américaine dans le domaine jugé stratégique de la collecte et de la diffusion de données satellitaires, la société Digital Globe, par exemple, est devenue le premier acteur de vente d'images satellitaires dans le monde (devant Airbus, l'autre acteur majeur de ce domaine).

Et c'est dans la continuité de ces premiers efforts que le terrain a continué d'être préparé pour une extension du rôle des États-Unis dans la fourniture de données et dans la maîtrise de leur diffusion. Des nouveaux entrants comme la société Planet ont largement bénéficié de ce mouvement de fond. Planet a construit son modèle d'affaires sur l'exploitation de très petits satellites, de type Cubesats, fournissant à très bas prix des images certes moins précises que celles diffusées par les plus gros satellites, mais en quantité bien plus grande et avec l'objectif à terme de plusieurs revisites de sites par jour. Faisant le pari d'une demande en hausse de flux d'informations venant en complément d'images plus détaillées, Planet suscite d'abord l'intérêt du gouvernement américain et de ses services de renseignement qui constituent aujourd'hui son soutien économique le plus sûr. Confrontée à un marché commercial plus lent à décoller, la société compte d'abord sur ce flux d'affaires gouvernemental pour consolider son activité dans l'attente de l'essor progressif d'une activité plus intégrée dans le flux créé par la croissance des technologies de l'information. Cet exemple, s'il

reste unique, semble pouvoir faire école, comme pourraient le confirmer les nombreux projets qui tentent aujourd'hui de se faire une place.

Des efforts similaires sont en cours dans le domaine des télécommunications avec l'annonce de nombreuses « méga-constellations » constituées de plusieurs centaines, voire de plusieurs milliers de satellites en orbite basse. L'objectif serait de réduire la fracture numérique ou de servir des marchés en applications nouvelles basées, par exemple, sur l'Internet des objets. Échaudée par l'échec enregistré par de tels projets dans les années 1990, avec à la clé l'explosion d'une bulle spéculative, la communauté des télécommunications garde un avis mitigé sur le succès de telles entreprises.

Pour autant, aussi bien pour les télécommunications que pour l'observation de la Terre, deux facteurs majeurs sont venus transformer le paysage depuis vingt ans : l'existence d'une activité Internet qui génère d'énormes revenus publicitaires sur lesquels parient les entrepreneurs considérés, et, bien sûr, l'évolution des techniques qui permet désormais d'envisager des télécommunications opérées sur la base de satellites défilants (qui moins coûteux que les satellites géostationnaires permettent en outre une plus grande instantanéité des télécommunications) ou une prise d'image de plus en plus performante grâce à des objets dont le coût unitaire très réduit laisse envisager une possible multiplication de leur mise en orbite à très basse altitude.

Une étude récente d'un cabinet spécialisé américain montre que plus de 1 300 microsatellites (parmi lesquels 70 % de Cubesats) ont été lancés entre 2012 et 2018, avec une multiplication par 6 des satellites de ce type lancés en 2018 par comparaison avec 2012. Sur la même période, la moitié des satellites concernaient des charges commerciales avec environ 80 % de ces satellites destinés à l'observation de la Terre. Sur l'ensemble des petits satellites lancés sur la période, 36 % l'ont été aux États-Unis[4]. Les petits satellites ou les Cubesats, longtemps cantonnés dans un rôle purement expérimental, semblent donc trouver aux États-Unis une fonction désormais plus opérationnelle. Cette tendance n'a pas encore d'équivalent dans d'autres pays et correspond à l'éclosion du secteur dit du « New Space », qui, précisément, parie sur la production massive d'images ou de systèmes de télécommunications en relation avec un monde de l'information de plus en plus avide de données.

Ainsi, ce n'est pas un hasard si l'essentiel de ces nouveaux projets se sont d'abord concentrés aux États-Unis, plus exactement en Californie, à Palo Alto, et dans les environs de la Silicon Valley. Toujours selon le cabinet Bryce, entre 2000 et 2017, ce sont près de 17 milliards de dollars qui ont été investis dans plus de cent quarante *start-ups* créées, dans le même intervalle de temps, dans le monde entier, la Californie représentant à elle seule la moitié des deux cent cinquante investisseurs répertoriés. Le phénomène a connu une accélération avec deux tiers des montants investis au cours des cinq dernières années de la période précitée. Les stratégies d'investissement sont nombreuses et varient selon les types d'acteurs considérés, qu'il s'agisse de capital risque, des investisseurs souvent demandeurs d'un retour rapide sur investissement, ou des GAFA, qui y voient plus un possible investissement de moyen terme, ou encore de *Business Angels* qui sont, eux, plus prompts à aider de jeunes pousses prometteuses sur le plus long terme. Avec une moyenne de 2,5 milliards de dollars investis sur les toutes dernières années, les chiffres impressionnent vus de ce côté de l'Atlantique.

Pour autant, le « New Space » continue de ne représenter qu'une fraction des dépenses publiques qui continuent largement d'assurer la continuité des activités spatiales et de l'emploi qui y est associé.

La part écrasante de l'investissement militaire

L'explosion annoncée de la commercialisation des activités spatiales semble en fait au milieu du gué avec une administration qui paraît vouloir stimuler ce secteur tout en évitant de donner un rôle trop central à des acteurs comme Space-X ou Blue Origin. Une nouvelle directive publiée en mai 2018, complétée par la troisième du genre un mois plus tard[5], appelle à donner un rôle plus grand au Département du Commerce en matière d'organisation et de promotion de cette activité, notamment dans le domaine de la vie orbitale. Ces deux textes montrent une volonté réelle de faciliter l'accès du secteur privé à l'utilisation de l'espace.

Pour autant, aux États-Unis, la dépense militaire représente, depuis le milieu des années 1980, la plus grosse part de la dépense publique. Le budget spatial du Pentagone s'établirait autour de 20 milliards de dollars annuellement sans compter les programmes classifiés qui, de fait, ne sont pas comptabilisés dans le budget public. De ce point de vue, la présidence Trump, très prompte à afficher son volontarisme militaire, perpétue en réalité une tradition bien ancrée à laquelle son prédécesseur n'avait lui-même pas dérogé. Il faut en fait plutôt parler d'une relance depuis environ dix ans de programmes militaires intégrant une préoccupation stratégique nouvelle, qui est celle de la possibilité, pense-t-on outre-Atlantique, de la survenue d'un conflit militaire dans l'espace. L'insistance américaine à ériger la Chine en futur ennemi spatial depuis le test antisatellite réalisé avec succès par Pékin, le 11 janvier 2007, puis le constat fait du développement d'activités orbitales suspectes, aussi bien par les Chinois que par les Russes (qui sont en fait souvent similaires aux activités expérimentales menées du côté américain), ont, depuis lors, convaincu les administrations américaines successives de renforcer leurs capacités à défendre les satellites américains contre toute tentative d'attaque, voire à en prévenir la survenue possible.

De nombreux programmes dits « contre-spatiaux » ont donc été engagés depuis plusieurs années qui visent aussi bien à accroître les capacités à surveiller de plus en plus précisément les mouvements spatiaux adverses qu'à durcir les satellites ou produire des systèmes offensifs pour contrer, le cas échéant, toute action préemptive. Les lignes budgétaires correspondantes ont été augmentées de près de 8 milliards de dollars sur cinq ans par l'administration Obama, geste confirmé depuis par l'administration Trump qui a réservé un montant du même ordre au titre des prochaines années.

Dans ce contexte, une quatrième directive spatiale vient d'être signée par le président américain, le 19 février 2019, qui annonce la création d'une « force spatiale ». Le mouvement est avant tout symbolique, jugé utile autant pour des raisons intérieures qu'extérieures, et qui, en dépit de réorganisations internes, n'affectera que peu le mouvement de fond déjà engagé[6]. Dans ce contexte, l'industrie spatiale américaine se voit bénéficier de débouchés assurés, et *a priori* pour longtemps. Elle peut compter sur des autorités chinoises ou russes, bien décidées à continuer à affirmer ou à réaffirmer leur présence dans l'espace, y compris sur le plan militaire, pour rester finalement ses meilleures « forces de vente ».

Xavier PASCO
Directeur de la FRS
x.pasco@frstrategie.org

Notes

1.Sierra Nevada, un autre challenger ayant, quant à lui, développé une navette spatiale pour le vol habité, a également vu son projet retenu dans sa version cargo pour assurer cette desserte.

2.Space Policy Directive-1 du 11 décembre 2017.

3.Sur ces points, voir Pasco X. (2017), *Le Nouvel Âge spatial, de la guerre froide au New Space*, Paris, CNRS Éditions, 192 p.

4.Bryce Space and Technology (2019), "Smallsats by the Numbers". Voir aussi l'étude plus détaillée de la Fondation pour la recherche stratégique, « Petits satellites, petits lanceurs », réalisée entre 2016 et 2018, avec le soutien du CSFRS et accessible à l'adresse suivante : https://www.csfrs.fr/sites/default/files/rapport_final_pspl_avril2018.pdf

5.Sapec Policy Directive-2 du 24 mai 2018 et Space Policy Directive-3 du 18 juin 2018.

6.En dépit du souhait de Donald Trump de créer une « sixième armée », la *Space Force* restera tout d'abord (et peut-être pour longtemps) placée sous l'égide de l'armée de l'air américaine…

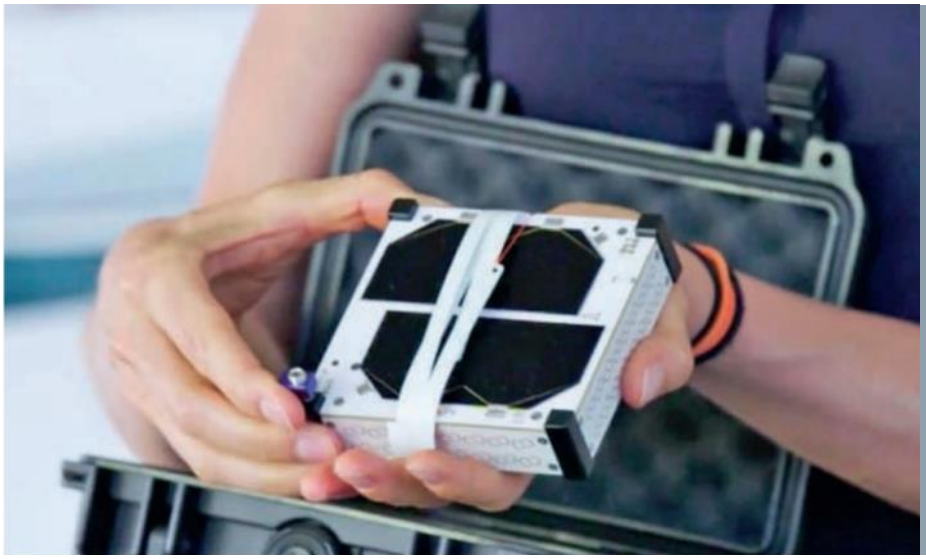


Photo © D.R.

Réalité et perspectives de l'IoT spatial

L'Internet des objets est considéré par de nombreux observateurs comme l'évolution naturelle du réseau Internet. Dans un futur proche, ce sont des milliards d'objets qui se connecteront au réseau pour accomplir de nombreuses tâches. Même si leurs capacités sont moindres, les petits satellites, en raison de leur faible coût, apparaissent comme des relais idéaux des communications avec les objets connectés, en particulier dans les lieux faiblement couverts par les réseaux terrestres. De nombreuses start-ups ont donc été créées pour bénéficier de l'avantage au premier entrant sur ce marché potentiel. Ce marché n'existe pas encore et pourtant plusieurs satellites ont déjà été lancés pour le servir. Cette course à l'IoT, qui a déjà fait mûrir le marché de la fabrication des petits satellites, pourrait pourtant ne jamais représenter une réalité économique structurante pour eux. En revanche, s'il devenait un marché viable, cette dynamique de rupture pourrait profondément modifier le secteur spatial actuel.

L'Internet des objets, plus connu sous son sigle anglais « IoT », pour *Internet of Things*, est un sujet brûlant pour l'évolution du réseau Internet. Parfois défini comme la suite logique du Web social qui caractérise la structure actuelle du réseau, l'IoT repose sur la supposition que de nombreux objets viendront se connecter à Internet dans un futur proche pour des applications variées. Ce type d'évolution fait écho à la vision développée par Mark Weiser dans les années 1990 : des milliards d'objets connectés au réseau auraient le potentiel de changer profondément l'usage d'Internet en le rendant omniprésent dans la vie quotidienne (Weiser, 1991).

Des objets connectés ont déjà commencé à émerger dans notre vie quotidienne : les compteurs Linky, les scooters en libre-service ou les enceintes connectées en sont des exemples.

Certains observateurs anticipent l'existence de 20 milliards d'objets connectés d'ici à 2020 (Hung, 2017), contre environ 7 milliards aujourd'hui (Lasse Lueth, 2018). Ce marché pourrait ainsi représenter à cette échéance plus de 450 milliards de dollars (Columbus, 2018). Certains analystes anticipent l'apport des technologies spatiales pour ce type d'applications. L'objectif affiché par de nombreuses start-ups consiste à trouver une niche au sein du marché de l'IoT, mettant en avant le caractère global des télécommunications par satellite.

La « course » à l'IoT spatial

Le secteur des télécommunications par satellite a historiquement favorisé l'usage de l'orbite géostationnaire pour des raisons d'économie : les satellites sont en effet des appareils coûteux et lourds, leur poids se mesurant en tonnes. L'altitude de l'orbite dite « géostationnaire », située à 35 687 km de la surface terrestre, permet à un satellite d'apparaître fixe dans le ciel, un seul satellite offrant donc un relais de télécommunications couvrant une large partie du globe (Clarke, 1945). En orbite basse, les satellites « défilent » au-dessus de la surface, un nombre important de ceux-ci est donc nécessaire pour assurer une couverture globale. Un ensemble de satellites est traditionnellement décrit comme une « constellation ».

Les évolutions techniques dans la miniaturisation électronique ont permis depuis le début du XXIe siècle de réduire considérablement le poids et la taille des satellites, et par conséquent leur coût de production à l'unité. Le standard « Cubesat » inventé en Californie est devenu particulièrement répandu : une unité (u) est constituée d'un cube de 10x10x10 cm. Un Cubesat 3u est un parallélépipède de 30x10x10 cm. Ces petits satellites peuvent désormais être produits en masse de façon relativement économique, ce qui était impossible pour des satellites lourds. Cela permet d'envisager la réalisation de constellations de satellites en orbite basse pour un coût raisonnable.

Ces satellites sont cependant beaucoup moins performants que les satellites géostationnaires. Ils sont incapables de transmettre les débits d'informations nécessaires à la diffusion d'images télévisées de bonne qualité ou à une connexion Internet pour un utilisateur humain. De plus, leur caractère défilant signifie qu'à moins d'en déployer des centaines voire des milliers, une couverture totale et permanente du globe ne peut être garantie.

*Article publié dans *Réalités industrielles*, Mai 2019, Annales des Mines, pp.73-76

L'IoT constitue potentiellement un cas d'usage dans lequel un débit faible et une latence importante ne sont pas des facteurs limitants. Certains objets connectés ont en effet des besoins de connexion modestes : un relevé par jour constitué d'un message court peut suffire à certaines applications (Holmes, 2018). Les petits satellites apparaissent particulièrement adaptés à un tel usage, car leur faible coût permet, avec un risque minime, de se positionner sur ce marché.

Ainsi, les entreprises Aerial & Maritime, AisTech, Analytical Space, Astrocast, Blink Astro, eightyLEO, Commsat, Fleet Space Technologies, Helios Wire, Hiber Global, Hongyan, Guodian Gaoke, Kepler Communications, Kineis, Lacuna Space, Myriota, NSL Comm, OQ Technology, Swarm Technologies, Spire Global, Sky and Space Global, SAT4M2M et Xingyun ont été fondées pour atteindre ce marché émergent.

À ces nouveaux entrants, il convient d'ajouter les acteurs traditionnels de la communication de machine à machine (M2M) : Iridium, Globalstar, Inmarsat, Thuraya et Orbcomm, qui connectent déjà des millions d'objets par satellite, mais pour un coût plus élevé. Eutelsat et Telesat, deux opérateurs de satellites de télécommunications géostationnaires, ont également annoncé leur décision de se lancer sur ce marché (Holmes, 2018). La nouvelle version des balises Argos, appelée Argos Neo, proposera vraisemblablement des applications IOT, gérées par la société Kineis (Cabirol, 2018).

Les projets des start-ups présentent certains points communs : la plupart utilisent des satellites basés sur le format Cubesat, prévoient des constellations en orbite basse terrestre et proposent des services basés sur un flux de données faible et intermittent à un coût nettement inférieur aux solutions actuelles (Crisp, 2018). Certaines différences pourraient cependant les départager dans cette nouvelle course à l'espace.

La seule entreprise à avoir opté pour l'intégration verticale de sa production de satellites est Swarm Technologies. Celle-ci a conçu des satellites originaux : ils sont en effet au format 0,25u, soit un quart de Cubesat. Ce format est à l'origine d'un scandale qui a affecté l'entreprise en 2018. La FCC avait en effet refusé d'autoriser le lancement de satellites-tests de ce format, par crainte que les radars de surveillance de l'espace soient incapables de suivre ces objets de si petite taille. Le lancement a pourtant eu lieu malgré cette interdiction (Harris, 2018). Swarm Technologies a dû renoncer au vol suivant et s'acquitter d'une amende de 900 000 dollars auprès du régulateur américain (Henry, 2018), ce qui n'a pas empêché l'entreprise de lever 25 millions de dollars en janvier 2019 (Pressman, 2019).

Les autres start-ups ont majoritairement décidé de confier la fabrication de leurs microsatellites à des entreprises établies. Le tableau ci-dessous résume les choix effectués par certaines d'entre elles. Certaines initiatives utilisent la station spatiale internationale comme segment spatial. Ainsi, la NASA a eu recours à une charge utile fabriquée par Digi-international, société américaine spécialisée dans les communications et la technologie de la machine à la machine, pour surveiller le fonctionnement de son dispositif exo-brake (Roberts, 2017). La start-up SAT4M2M, soutenue par l'ESA, a fait le même choix. Kineis est, quant à elle, une société française issue de l'entreprise CLS, qui souhaite capitaliser sur les acquis du projet Argos, notamment en utilisant la plateforme Angels pour développer sa constellation de vingt satellites. Ceux-ci seront des Cubesats 12u construits par Thales Alenia Space, Nexeya et Syrlink (Henry, 2018). Les architectures diffèrent donc, mais ces entreprises ont un objectif commun : être parmi les premières à offrir des services IoT depuis l'espace.

Start-ups	Fabricant de satellites	Origine du constructeur
Kepler Communications NSL Comm	AAC Clyde	Grande-Bretagne
Astrocast	Airbus	Europe
Helios Wire Lacuna Space	Astrodigital	Etats-Unis
Hongyan	CASC	Chine
Xingyun	Casic	Chine
Aerial & maritime AisTech Hiber Global Sky and Space Global OQ Technologies	GomSpace	Danemark
Blink Astro	Nanoavionics	Lituanie
Kineis	Thales Alenia Space, Nexeya et Syrlink	France
Fleet Space Technologies	Pumpkin Space Systems	Etats-Unis
Myriota	SpaceQuest	Etats-Unis

Un marché présentant un réel potentiel, mais immature

La plupart de ces entreprises se concentrent sur les réseaux *Low Power Wide Area* (LPWA), qui comprennent les réseaux SigFox, LoRa et NB-IoT. Comme dans la plupart des offres de télécommunications, il existe une concurrence entre les offres spatiales et les offres terrestres, les coûts affichés par ces dernières jouant généralement en leur faveur. Il semble que l'IoT ne fasse pas exception à cette règle.

En conséquence, les applications de l'IoT spatial sont essentiellement liées à des lieux peu couverts par les réseaux terrestres − soit 80 % de la surface du globe !. Les espaces maritimes et désertiques sont particulièrement concernés. Bien que cette proposition puisse avoir du sens pour certaines applications, particulièrement celles

liées à la logistique et à la connectivité des zones isolées (plateformes pétrolières, industrie minière, militaires en opération), certains analystes se montrent réservés sur la capacité de ces start-ups à proposer des services adéquats à leurs clients, étant donné la présence sur le marché de concurrents historiques offrant des services certes plus onéreux, mais également plus performants et fiables. Ainsi, si Northern Sky Research prévoit bien l'émergence d'un segment de marché couvert par des petits satellites, celui-ci serait limité à seulement 5,1 % du marché de l'IoT spatial (Crisp, 2018).

Par ailleurs, le grand nombre de constellations programmées nécessiterait, pour espérer un retour sur investissement, l'émergence d'un marché de millions d'objets connectés par constellation. Si tous les projets annoncés étaient menés à leur terme, ce serait plus de 1 600 satellites qui seraient lancés, ce qui, d'après certains analystes, est un nombre bien trop important au regard du marché potentiel.

Tim Farrar de TMF Associates explique ainsi que s'il est aisé pour la plupart des start-ups de lever 10 millions de dollars pour pouvoir prouver la viabilité technique de leur concept, il est beaucoup plus difficile pour elles de lever suffisamment de fonds pour développer leur business model (Higginbotham, 2018).

Face à l'anticipation de ce que seront les futurs marchés, il est logique de voir se multiplier les investissements dans différentes infrastructures et une forme de course à l'IoT spatial se mettre en place, incluant le lancement de satellites -tests prouvant la viabilité technique des projets envisagés, et ce malgré l'absence de clients. Il est également presque certain que toutes ces start-ups ne survivront pas et que les prochaines années verront une consolidation de cette industrie (Harris, 2018).

Une conséquence de cette course à l'IoT spatial est cependant déjà notable. Les commandes passées par ces start-ups auprès de fabricants de microsatellites comme GomSpace ou AstroDigital ont contribué à l'arrivée à maturité de ce secteur, qui cherche désormais à concevoir des satellites de plus en plus performants pour le compte de clients toujours plus exigeants. Ainsi, GomSpace a-t-il été sélectionné par l'ESA pour la construction d'un Cubesat qui, dans le cadre de la mission HERA, sera envoyé vers un astéroïde. Les forces aériennes colombiennes ont également fait appel à eux pour la fabrication d'un satellite d'observation de la Terre. AAC Clyde est, pour sa part, passé de la construction de sous-systèmes pour Cubesats à la fabrication et à l'intégration de microsatellites complets pour ses clients. Cette course à l'IoT spatial a donc eu pour effet de dynamiser le secteur de la construction de satellites, alors que le marché qu'il souhaite atteindre n'existe pas encore. La pérennité du secteur industriel des microsatellites apparaît donc largement dépendante de l'évolution des besoins de l'IoT en termes de connectivité spatiale.

Les besoins de l'IoT semblent correspondre aux capacités des petits satellites, il est donc compréhensible que des entreprises se positionnent sur ce marché potentiel pour bénéficier de l'avantage du premier entrant. Il est tout à fait envisageable aujourd'hui que l'IoT ne s'élève jamais à la hauteur de son potentiel estimé. Dans ce cas, les investissements consentis auront été relativement modestes. Si, en revanche, l'IoT devient un marché massivement desservi par les satellites, les ruptures technologiques engendrées par l'industrie des petits satellites auront des conséquences importantes sur le secteur spatial, surtout au regard de la période de fragilité qu'il traverse actuellement.

Paul WOHRER
Chargé de recherche, FRS
p.wohrer@frstrategie.org

Références bibliographiques

Cabirol M., « Le CNES confie le futur système Argos à Thales », *La Tribune*, 14 mai 2018.
C. Clarke, Arthur, « Extra-Terrestrial Relays », *Electronics World*, 119 (1924):14, avril 2013.
Columbus L, « 2017 Roundup of Internet of Things Forecasts », *Forbes*, 10 décembre 2017.
CORDIS, « Space IoT takes off », *CORDIS*, 9 juillet 2018.
Crisp A., *The bottom Line. The ROI challenge of IoT Smallsats*, Northern Sky Research, 3 octobre 2018.
GOMSPACE, « The Colombian Air Force Orders its second advanced Nanosatellite platform from GomSpace », *PRS Newswire*, 1er décembre 2017.
GOMSPACE, « ESA and GomSpace Sign Contract for Advanced Nanosatellite to join the HERA mission », *PRS Newswire*, 21 janvier 2019.
Harris M., « SpaceX's Next Launch Will Spark A Space Internet Showdown », *Politico*, 27 novembre 2018.
Harris M., « Why Did Swarm Launch Its Rogue Satellites? », *IEEE Spectrum*, 20 mars 2018.
Henry C., « EightyLEO Details Vision for IoT SmallSat Constellation », *Via Satellite*, 22 octobre 2015.
Henry C., « FCC fines Swarm $900,000 for unauthorized smallsat launch », *SpaceNews*, 20 décembre 2018.
Henry C., « French IoT company plans $139 million smallsat constellation », *SpaceNews*, 10 septembre 2018.
Higginbotham S., « Lacuna is bringing the internet of things to space », *Stacey on IoT*, 23 octobre 2018.
Hill J., « Saceflight to Launch Fleet Space Centauri I on ISRO's PSLV This Year », *Via Satellite*, 3 juillet 2018.
Holmes M., « Eutelsat Exec Discusses Possibility of Full LEO Constellations », *Via Satellite*, 9 mars 2018.
Holmes M., « Telesat and LEO: Goldberg Answerse the Burning Question », *Via Satellite Digital*, Janvier 2018.
Hung M., *Leading the IoT*, Gartner, 2017.
Jones A., « China to launch first Hongyan LEO communications constellation satellite soon », *GB Times*, 13 novembre 2018.
Lasse Lueth K., « State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating », *IoT Analytics*, 8 août 2018.
Nyirady A., « Luxembourg Companies to Test IOT Technology », *Via Satellite*, 21 septembre 2018.
ONEWEB, « Keyshot Module », site web de Oneweb, 2019.
ORBCOMM, « ORBCOMM Surpasses Two Million Subscriber Communicators in The Industrial IoT Market », site d'Orbcomm, 28 novembre 2017.
Man A., « Exclusive: Satellite Startup Swarm Raises $25 Million For Space-Based Internet Plan », *Fortune*, 24 janvier 2019.
Reichert C., « Satellite IoT start-up Myriota raises $15m », *ZDNet*, 26 mars 2018.
Roberts F., « NASA looks to bring IoT to space with wireless comms test », *Internet of Business*, 6 mars 2017.
SAT4M2M, « SAT4M2M », site web de SAT4M2M, 2019.
Weiser M., « The Computer for the 21st Century. Scientific American », vol. 265, septembre 1991, pp. 94-104.

Europe et cybersécurité : quelle(s) base(s) industrielle(s) ?

Dans un contexte marqué par d'importantes évolutions technologiques, le paysage industriel européen de la cybersécurité connaît une structuration progressive, suite notamment à différentes vagues de consolidation. Cependant, une diversité des profils compose ce que l'on peut appeler une « base industrielle et technologique de cybersécurité » (BITC). La présence d'industries de défense aux côtés d'entreprises issues du monde du numérique aux *business models* différents complique ainsi la lecture du secteur. En matière de concurrence, les BITC européennes font face à l'hégémonie des groupes de cybersécurité américains, la structuration d'une filière tournée vers l'innovation en Israël et l'émergence de nouveaux acteurs (Chine notamment). Les défis européens sont alors multiples : création d'un leadership international, soutien à l'innovation, structuration d'un marché unique, etc. Fondé sur une approche comparée des bases nationales de cybersécurité en Europe et à l'étranger (Etats-Unis et Israël), cet article propose de revenir, dans un premier temps, sur les acteurs composant une base industrielle et technologique de cybersécurité ainsi que sur les éléments clés à l'origine de son développement. Dans un second temps, il tente d'éclairer les capacités européennes en la matière et ses spécificités.

Une BITC composée d'acteurs aux profils variés

L'offre de cybersécurité recouvre des solutions très diverses et la demande est caractérisée par une forte disparité, allant du citoyen-consommateur jusqu'aux ministères de la Défense. Le périmètre de la cybersécurité est en effet très large. Pour être appréhendé, il nécessite de recourir à plusieurs segmentations de marché, que ce soit selon les solutions[1] ou les clients[2].

Eu égard à ce large périmètre, plusieurs profils d'entreprises composent la BITC. Parmi les acteurs pivots, les fabricants de matériels et d'équipements informatiques et électroniques ont vu l'apparition des grands systémiers-intégrateurs (IBM, Microsoft, HP, Cisco, Dell, etc.) aux côtés d'équipementiers (Qualcomm, ST Microelectronics, Schneider Electrics, Siemens, etc.). Les éditeurs de logiciels spécialisés (Symantec, CheckPoint, Kapersky, etc.) et les entreprises de services du numérique (ESN) jouent également un rôle majeur, ces dernières profitant de la proximité clients pour déployer une large gamme de solutions de cybersécurité (Atos, Capgemini, Sopra-Steria etc.). Si une partie des opérateurs de télécommunication et des groupes de défense ont fait le choix de se positionner sur ce marché, leur entrée est plus tardive et elle s'est faite principalement par opérations de croissance externe.

Le tableau ci-après offre une vision d'ensemble des écosystèmes impliqués dans la cybersécurité et permet d'illustrer les différentes stratégies de positionnement des entreprises. On notera néanmoins, pour les acteurs pivots issus de la défense ou du monde du numérique, que les stratégies de positionnement tendent à se lisser en raison d'une logique de plus en plus partagée d'intégration verticale des activités.

BITC et quête d'innovation

Les spécialisations des BITC nationales, qu'elles soient orientées plutôt produits/solutions, spécialisées dans un sous-secteur, etc. sont héritières des politiques industrielles spécifiques menées dans différents secteurs (défense, électronique, semi-conducteurs, informatique, etc.), essentiellement dans les années 1970-2000. Ainsi, le développement d'une capacité nationale de cybersécurité s'appuie-t-elle d'abord sur la présence au préalable d'une industrie de défense, du logiciel, de l'informatique hardware (PC & composants, calculateurs, cartes et puces électroniques, etc.), des télécommunications, du conseil, etc.

Les stratégies nationales dédiées à la cybersécurité, et incluant un volet industriel, sont quant à elles assez récentes. Une analyse de ces dernières, menée dans les principaux pays leaders du secteur, nous permet de retenir des conditions de succès communes :

- Prise de conscience des risques cyber par les acteurs publics ;
- Maturité des marchés domestiques de la cybersécurité (public et privé) ;
- Grands groupes leaders, têtes de pont de filière ;
- Adoption d'un arsenal juridique contraignant (objectif de susciter la demande) ;

*Article publié dans la revue *RDN*, avril 2019.

Principales stratégies de positionnement	Marchés ciblés
Groupes de défense	
Entrée sur le marché : diversification des activités au profit de la cybersécurité, dans un contexte de contraction des commandes via *« spin-in »* de technologie de défense et politique de croissance externe. Consolidation des activités : création d'une B.U. cyber et/ou création d'une filiale cyber pour conserver/créer une « marque » forte (via regroupement des activités et/ou croissance externe). Logique de partenariat : intégration de solutions leaders sur le marché/développement conjoint d'offres avec les acteurs leaders mondiaux (systémiers intégrateurs, éditeurs de logiciels, prestataires de services).	Marché : Défense (marché et activités historiques) + Diversification des clients au profit des acteurs « civils » : administrations publiques et grands groupes. Ventes directes, en qualité de systémiers-intégrateurs.
Fabricants de matériels et d'équipements	
Systémiers intégrateurs Entrée sur le marché : presque exclusivement tous américains, des fabricants ayant privilégié une diversification des activités au profit d'une offre de services, suivant une stratégie d'intégration verticale. Fourniture d'offres packagées. Consolidation des activités de services et édition logicielle via une stratégie d'acquisition agressive. Le cas échéant, intégration des solutions de sécurité reconnues comme leaders du marché.	Marchés : Grands comptes prioritairement (administrations publiques, grands groupes).
Equipementiers – pure player Entrée sur le marché : sécurisation *by-design* et développement d'offres de services de sécurité associées. Développement de solutions sécurisées *by design* grâce à une politique de R&D soutenue. En recherche de taille critique pour réaliser des économies d'échelles. Logique de partenariats : services et intégration de solutions sécurisées.	Marchés : intermédiaires (systémiers-intégrateurs) via partenariats + Renforcement de la relation directe avec les clients finaux.
Éditeurs de logiciels	
Grands groupes Acteurs historiques positionnés sur le marché de la cybersécurité, presque tous non européens et cotés en bourse. Intégration permanente de mécanismes et solutions de sécurité dans leur offre. D'une logique de licence à une offre SaaS. Très forte logique marketing (référencement des solutions, etc.). Croissance externe via l'acquisition ciblée d'éditeurs de logiciels disposant de briques technologiques, soutenue par des réserves de cash importantes.	Canaux de ventes indirects *via* ESN et systémiers-intégrateurs. Vers le développement de relations directes avec les clients finaux (vente de services associés).
Start-ups, PME Recherche d'une croissance interne rapide soutenue par la quête de financement (levées de fonds, cotation en bourse, etc) en vue d'assurer une bonne commercialisation des solutions (certification, catalogage, marketing, etc.).	Développement des canaux de vente indirects en B2B *via* les ESN.
Prestataires de services	
Entreprises de services du numérique (ESN) à rayonnement mondial Entrée sur le marché : proximité clients assurée grâce à la multiplication d'établissements secondaires et/ou croissance externe. Logique d'intégrateur : sélection des offres de sécurité les plus réputés du marché (bénéficiant d'une reconnaissance auprès du client final grâce à un bon catalogage/référencement) et/ou des acteurs en mesure de déployer des solutions à l'échelle mondiale. Développement d'offres de sécurité managées autour de SOC.	Marchés : Grands comptes prioritairement et administrations publiques. + Développement vers les marchés Défense (liés principalement aux activités de soutien général).
Cabinets de conseil à rayonnement local/régional Proximité Client/Offre en matière d'audit et de conformité : accent mis sur le développement des ressources humaines (consultants).	Marchés : PME-ETI et collectivités territoriales.
Prestataires de services de R&D Entrée sur le marché : généralement issus de laboratoires de recherches publics ou privés (spin-off). Modèle basé sur la licence de brevets. Concentration des efforts RH dans la R&D et multiplication des projets de recherche menés dans l'écosystème local.	Marchés : Fabricants de matériels et d'équipements essentiellement, en vente directe et indirecte (royalties issus des brevets).
Opérateurs télécom	
Entrée sur le marché : Intégration de solutions de sécurité au sein des offres « classiques » de communication via des partenariats avec des entreprises spécialisées et/ou développement de solutions en interne. Développement d'une offre de cybersécurité en interne (création d'une B.U.) ou par croissance externe ciblant des prestataires de services spécialisés.	Clients historiques + Marchés liés aux prestations de services en matière de cybersécurité (en concurrence avec les ESN notamment).

- Mise en place d'une politique de R&D dédiée (plan d'investissements, feuilles de routes industrielles) ;
- Formations universitaires adaptées de qualité et en nombre suffisant (accompagnant la croissance du secteur) ;
- Soutien au développement des entreprises technologiques à travers l'afflux de financements privés adaptés (capital-risque) ;
- Regroupement des activités de cybersécurité au sein de clusters réunissant l'ensemble de l'écosystème (industriels, centres de R&D, laboratoires de recherche, pôles de formation, clients finaux, capitaux-risqueurs).

La pérennisation de l'activité des start-ups, et plus généralement des acteurs innovants en matière de cybersécurité, est aujourd'hui une des priorités des Etats qui affichent une ambition dans le secteur. Le regroupement sous forme de cluster est désormais privilégié dans l'ensemble des stratégies nationales avec pour objectif, entre autres, d'attirer les financements privés en capital-risque. En effet, l'émergence des start-ups est marquée par une phase de développement de solutions adaptées à des défis de sécurité spécifiques. Avantage compétitif déterminant dans le secteur, cette stratégie de niche peut leur offrir une forte croissance (identification sur le marché en tant que pionnier). Ces start-ups font alors souvent l'objet d'acquisition par des grands groupes (systémier-intégrateur et éditeurs de logiciels essentiellement). Pour accompagner cette hyper-croissance, la présence en nombre et en volume des différents investissements en capitaux-risques, encouragés par des fonds d'investissements publics amorceurs adaptés, est donc primordiale.

Parmi les leaders mondiaux, le cas israélien illustre bien cette problématique. Avec près de 420 entreprises[3] (contre 148 en 2011), la BITC israélienne profite de la présence d'acteurs têtes de pont, notamment dans les secteurs de l'édition logicielle (CheckPoint et CyberArk) et de la défense (Elbit Systems). Mais elle se distingue par le nombre de créations de start-ups (depuis 2014, moyenne >65 start-ups cyber par an) et de PME récentes positionnées sur des segments relais de croissance (SCADA industriels, Objets connectés, Renseignement d'origine cyber, etc.). Ces start-ups bénéficient, pour réussir leurs levées de fonds, de l'accompagnement par de très nombreux investisseurs. En 2018, elles ont ainsi capté plus de 1 Md$ d'investissements en capital-risque, soit près de 20 % du total mondial réalisé dans le secteur de la cybersécurité[4] (2e place derrière les États-Unis qui en concentrent ~50 %). Ce montant, qui a augmenté de manière exponentielle ces dernières années, coïncide avec l'inauguration du cluster CyberSpark situé à Beersheva. Signe de son attractivité, le cluster accueille près d'une cinquantaine de centres de R&D étrangers tels qu'IBM, Intel, Microsoft, Siemens, etc., qui profitent notamment de l'écosystème national de recherche et de soutien publics[5].

Quelles actions européennes en matière de renforcement des capacités industrielles de cybersécurité ?

La Commission européenne s'est emparée des sujets numériques et *in fine* de la cybersécurité, ses initiatives s'inscrivant dans le cadre de la « Stratégie de cybersécurité de l'Union européenne »[6]. Elle affiche parmi ses objectifs le développement de ressources industrielles et technologiques en matière de cybersécurité. La communication relative à la création d'un « marché numérique unique »[7] rappelle également ces enjeux. Elle montre surtout que les initiatives de la Commission européenne visent une meilleure structuration du marché européen, et ce, à travers une évolution du cadre réglementaire[8]. Sur le plan de la structuration de l'offre, les avancées paraissent plus modestes. La mise en place d'un partenariat public-privé pour la cybersécurité (PPP) est toutefois notable. Il s'est matérialisé en juin 2016 par la création de l'*European Cybersecurity Organisation* (ECSO), composée d'acteurs et associations d'industriels, clusters, administrations publiques, clients et opérateurs. L'ECSO est censée générée, d'ici 2020, 1,8 Md€ d'investissements dans le secteur de la cybersécurité, l'UE s'engageant à consacrer 450 M€ dans le cadre du programme cadre de recherche et développement H2020 (financement qui doit susciter en théorie des investissements 3 à 4 fois supérieurs par les membres d'ECSO).

En Europe, des capacités concentrées en France, au Royaume-Uni et en Allemagne

A l'image du marché, les BITC européennes restent fragmentées. Une analyse des principales bases industrielles (françaises, britanniques et allemandes) fait par ailleurs ressortir la problématique de l'ancrage des BITC à un domaine d'action public plus large (sécurité, industrie 4.0, numérique, etc.).

En France, les dernières données communiquées par l'association d'industriels ACN[9], font état d'une BITC composée de près de 850 acteurs, principalement des PME et microentreprises. Elle réalise un chiffre d'affaires (CA) national hors export cumulé de 9 Mds€ pour environ 60 000 emplois. Ces données intègrent les activités issues de la sécurité numérique et ce, au sens très large, avec la vente de matériels et d'équipements tels que ceux liés à la biométrie, détection, terminaux de paiement, etc. Les leaders en la matière sont par exemple Idemia (ex Morpho - Oberthur Technologies), Gemalto ou Ingenico. La BITC française se trouve ainsi écartelée entre le monde du numérique et celui de la sécurité.

En Allemagne, la BITC est caractérisée par la position dominante d'entreprises intervenant en particulier sur le segment des infrastructures réseaux (Siemens, Deutsche Telekom, Secunet, etc.), et plus généralement, par la présence d'un tissu dense de PME et ETI. Représentée par les associations *Bitkom* et *Teletrust*, la BITC allemande fait partie intégrante du projet d'industrie 4.0, lancé en 2011 par le gouvernement.

Selon la dernière étude publiée par les autorités nationales[10], la BITC britannique regroupe 846 acteurs dont Sophos, le premier éditeur de logiciel spécialisé en Europe (CA total de 641M£ ; 3 300 employés). L'ensemble des entreprises du secteur emploie 31 000 personnes pour un CA cumulé de 5,68 Mds£. Pleinement intégrée au monde du numérique, la BITC est représentée par l'association d'industriels *TechUK*, qui agit comme interface privilégiée avec le gouvernement dans le cadre des initiatives de partenariat public-privé en la matière.

Des acteurs de niche sont également présents en Italie, Finlande, Espagne, Suède ou encore en Estonie.

Les groupes de défense européens, acteurs pivots des BITC nationales ?

Structurant des capacités sur plusieurs segments, les groupes de défense européens sont devenus progressivement des acteurs pivots au sein des BITC nationales.

Ce positionnement privilégié des principaux groupes de défense européens est principalement le fruit d'opérations de rachats d'entreprises menées au cours des dix dernières années, avec pour cœur de cible les acteurs spécialisés de cybersécurité, généralement des PME, ETI ou filiales de grands groupes. Le britannique BAE Systems a ainsi initié une politique de croissance externe particulièrement dynamique entre 2008 et 2014, investissant près de 1 Md£ dans l'acquisition de six entreprises spécialisées (Detica, Stratesc, ETI A/S, pôle Intelligence Service Group de L-1 Identity Solutions, Norkom Technologies, Silversky). Airbus a réalisé en 2012-2013 les acquisitions successives d'Arkoon et Netasq, quand le français Thales procédait au rachat des activités cyber d'Alcatel Lucent (2014), Vormetric (2015), Guavus (2017) et Gemalto (initié fin 2017). L'allemand Rohde & Schwarz a repris cinq entreprises entre 2014 et 2017 (GateProtect, Adyton Systems, Sirrix AG, R&S Cybersecurity HSM et DenyAll). En revanche, Leonardo a essentiellement tiré profit de technologies de défense pour développer son offre de cybersécurité, à travers notamment les activités de sa filiale électronicienne Selex[11]. Le groupe italien va aussi renforcer ses activités de cybersécurité à travers l'acquisition de l'entreprise de défense Vitrociset (janvier 2019).

La stratégie de croissance externe déployée par les principaux groupes de défense aura permis d'étoffer rapidement leur portefeuille de solutions de cybersécurité et d'étendre leur positionnement vers les marchés civils (administrations publiques et grands groupes). Leur CA généré dans le secteur de la cybersécurité les place désormais parmi les leaders nationaux. Ce rôle d'acteurs pivots au sein des BITC leur offre une place prédominante dans l'écosystème d'innovation, plutôt porté par des entreprises au profil civil[12]. Dans ce cadre, les groupes de défense ont multiplié les alliances stratégiques avec les leaders mondiaux, grands groupes civils et acteurs spécialisés (Airbus-Atos, Thales-Cisco, BAE Systems-02, Rohde&Schwarz-Radisys etc.). En structurant leur coopération, ils nouent également des relations privilégiées avec les start-ups spécialisées. A titre d'exemple, Thales est devenu, en 2017, partenaire référent de l'incubateur Station F pour la cybersécurité quand BAE Systems a étendu, fin 2016, son partenariat avec le cluster londonien CyLon puis lancé en 2018 *The Intelligence Network*[13], renforçant ses liens avec le monde de l'innovation civile dans le domaine de la cybersécurité.

Le concept de base industrielle et technologique de cybersécurité (BITC) est récent et fait référence à une pluralité d'acteurs. Au niveau européen, il suscite des problématiques spécifiques comme celle liée à la création d'un marché unique, condition pour une meilleure consolidation du secteur. La convergence des politiques dédiées entre Etats détenteurs d'une BITC apparaît également déterminante dans le contexte de la présence sur le marché européen d'acteurs étrangers aux positions dominantes.

KÉVIN MARTIN
Chargé de recherche, FRS
k.martin@frstrategie.org

Notes

1.Familles de solutions proposées (matériel, softwares, services), fonctions de sécurité assurées (pare-feu, antivirus, chiffrement surveillance réseau, etc.), niveau de sécurité offert (IoT, secret Défense, etc.), systèmes sécurisés (infrastructures fixes, équipements de mobilités, bases de données, systèmes industriels, etc.).

2.Approche sectorielle (banque, finance, santé, e-administration, etc.), Défense, Civils (administrations publiques, gestionnaires d'infrastructures vitales, grands groupes, ETI, PME consommateurs), géographique (maturité des marchés, règles juridiques, labels, etc. selon pays/régions).

3.Start-Up Nation Central, *Israel cybersecurity industry in 2017*, 2018.

4.« A look back at the Israeli cyber security industry in 2018», *Techcrunch*, 30 janvier 2019.

5.Ministry of Economy and Industry, State of Israel, *R&D Centers – Investments models in Israel,* 2017.

6.Communication de la Commission européenne*, Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé,* 7 février 2013.

7.Communication de la Commission européenne, *Stratégie pour un marché unique numérique en Europe*, 6 mai 2015.

8.Par exemple règlement EIDAS, RGPD ou de la directive NIS. La mise en place de certificats européens de cybersécurité pourrait être une étape supplémentaire en vue de réduire les barrières à l'entrée engendrées notamment par les coûts de certification et de labellisation nationaux.

9.Alliance pour la confiance numérique, *L'observatoire de la filière de la confiance numérique en France*, 2017.

10.Department for Digital, Culture, Media & Sport, Margot James MP, *UK Cyber Security Sectoral Analysis*, 30 octobre 2018.

11.Depuis septembre 2015, la filiale a fusionné avec le groupe.

12.Élément rappelé par la ministre des Armées, Florence Parly, dans le cadre de la création de l'Agence de l'innovation de défense : *« La nouvelle agence de l'innovation aura donc pour mission d'organiser les échanges avec cet écosystème de l'innovation, qui est plutôt civil* ». *Cf.* « Entretien de la ministre des Armées », *Usine nouvelle*, 31 mai 2018.

13.« BAE Systems Proposes a New Collaborative Approach to Cybersecurity », *CBR*, 9 juillet 2018.

FONDATION pour la RECHERCHE STRATÉGIQUE

www.frstrategie.org

ISSN : 2274-598X