note n°8/19

19 juin 2019

FONDATION pour la RECHERCHE STRATÉGIQUE

Philippe Gros
Maître de recherche, Fondation pour la recherche stratégique

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

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].

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

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].

[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 Entrerprise for the Future Conflicts of Tomorrow, 5 May 2014, p.2

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, plate-forme ou nœud autorisé contribue et reçoit en toute transparence l'information essentielle et est en mesure de l'utiliser dans toute la gamme des opérations militaires* »[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.

[4] *DoD Cloud Strategy*, December 2018.

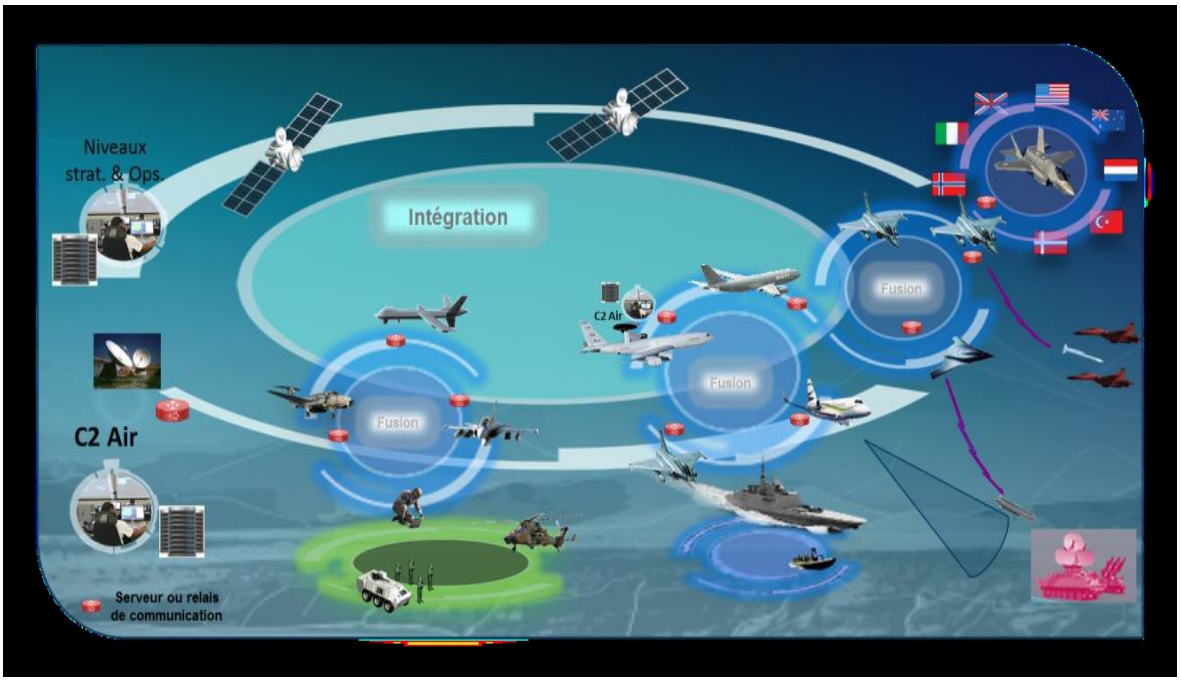
[5] Axel Dyèvre, Pierre Goetz et Martin de Maupeou, *Emploi du Cloud dans les Armées, Première approche des concepts et contraintes*, Les notes stratégiques, CEIS, août 2016, p.14.

[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.



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

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)

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

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

[11] Sans compter ceux destinés à la gestion du réseau
[12] Voir sur ce plan l'exceptionnelle fiche wikipédia française, élaborée par un spécialiste de la LDT
[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.

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,

[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*.

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

[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.

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

[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.

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

[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.

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.

[30] Defense Intelligence Agency, *China Military Power*, January 2019, p.86.
[31] Bilal Khan, « "LINK-17" – PAKISTAN'S HOMEGROWN DATA-LINK SYSTEM », 05 April 2016, *Quwa*.
[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 sur le https://www.dote.osd.mil/.

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**.

rmes, 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**.

Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.

La Fondation pour la Recherche Stratégique est une fondation reconnue d'utilité publique. Centre de recherche indépendant, elle réalise des études pour les ministères et agences français, les institutions européennes, les organisations internationales et les entreprises. Elle contribue au débat stratégique en France et à l'étranger.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643