note n°19/19

2 octobre 2019

Philippe Gros
Senior Research Fellow , Fondation pour la recherche stratégique

FONDATION pour la RECHERCHE STRATÉGIQUE

The "tactical cloud", a key element of the future combat air system

At the crossroads between operational requirement and technological opportunity, the tactical "cloud", or "combat cloud", is the latest manifestation of *Network Centric Warfare* (NCW), which for the past 20 years has conceptualised the information and decision-making superiority obtained by networking. It consists in bringing into the cockpit the most advanced capabilities of digital networks, based on commercial cloud technologies, in order to strengthen the efficiency, effectiveness and resilience of air power, whose operational functions will thus be transformed. The tactical cloud must become an essential part of a future air combat system and, beyond that, of all French armed forces, particularly in view of their limited format. But the architects of the combat cloud still have to overcome the enormous challenges associated with its development: cybersecurity (since the cloud increases the force's exposure to cyber-electronic threats); connectivity; interoperability; standards; information sharing.

The Future Combat Air System (FCAS) is the key project for French, German and Spanish air combat power from the 2040s onwards. As a reminder, its core will consist of a Next Generation Weapon System (NGWS), including the Next Generation Fighter (NGF), led by Dassault Aviation, which will take over from the Rafale, along with other new elements (drones, munitions, etc.). However, FCAS goes beyond the renewal of platforms and munitions. General Mercier, then French Air Force Chief of Staff, explained in 2015 that "[...] *for the future combat air system [FCAS] that the French Air Force is conceptualizing, the key word is indeed 'system'. Because it will not be a manned aircraft or a drone, but a system of systems integrating, within a real cloud, sensors and effectors of various types and different generations.*"[1]

This article will describe what this cloud notion means for FCAS, how it differs from current networking techniques, the incremental steps towards its completion and will present the potential added value but also the challenges faced to bring it to fruition.

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

The notion of the cloud

The notion of "cloud computing" basicallyillustrates varying degrees of outsourcing or pooling of a user's IT capacities. While the notion emerged with Amazon's leasing of its computing capabilities at the turn of the millennium, it refers to concepts and technologies that have actually been developed since the dawn of computing. There are multiple definitions of the "cloud" but the most common is the one given in 2011 by the U.S. National Institute of Standards and Technology: "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e. g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*"[2] The five characteristics are on-demand self-service, broad network access, resource pooling with other users, rapid elasticity and measured service. Service models refer to what is actually shared. The three main ones are:

- IaaS (Infrastructure as a service): sharing only includes the network and infrastructure (servers in particular). This is the most common model at the present time;
- PaaS (Platform as a service): sharing also extends to computer platforms, their operating systems and basic software;
- SaaS (Software as a service): finally, the sharing can involve the data itself and the applications used by the operator. This is technically the simplest model (cf. the use of a Gmail or Yahoo messaging service).

In the commercial sector, cloud computing mainly meets the same economic and managerial objectives as other outsourced services: the company no longer has to manage the evolution and security of its IT capacities, their "plasticity" according to the variability of its needs, a dedicated workforce of technicians, etc.

The cloud and the armed forces

The use of the cloud for military information and communication systems started around 10 years ago. The Americans were the first to make the move. Migration to the cloud is thus one of the pillars of the complete overhaul of the architecture of U.S. information and communication systems, the Joint Information Environment (JIE), conducted since 2010 through a vast federation of initiatives coordinated by the Chief Information Officer (CIO) of the Pentagon and the Defence Information Systems Agency. According to Teri Takai, the CIO who launched the project, the objective of the JIE is threefold: to make the defence sector more efficient, more secure against cyber threats and to reduce costs[3]. In concrete terms, efforts have focused on "consolidation", i.e. the massive reduction in the number of data centres, the development of a single security architecture and a common service base and the establishment of a single operational network management structure. However, the latest DoD strategy for cloud development shows, not surprisingly for observers of the U.S. defence sector, that the efforts made in recent years are far from satisfactory: lack of plasticity and therefore efficiency, extreme disparity and even unworkability of solutions, which have proliferated. The Pentagon's approach now is to develop a general-purpose IaaS/PaaS-type cloud, the Joint Enterprise Defense Infrastructure (JEDI), and specific (Fit-for-Purpose) clouds where necessary[4], an approach that has been challenged by Congress. The French Ministry of the Armed Forces has also developed its own private cloud, mainly for central administration tasks.[5]

The "tactical cloud"

These initial migrations to the cloud concerned fixed IT infrastructure of the major staffs, agencies, and possibly deployable command centres in the case of the U.S. Cloud development extending to the tactical level, that of units and platforms, also started to emerge. The U.S. forces have been experimenting with the latter for several years, and the French armed forces are at the conceptualisation stage. In its *Digital Ambition*, the French Ministry of the Armed Forces explains that "[ensuring operational

[2] Peter Mell (NIST), Tim Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology , September 2011 (translation by the author using Deepl translation service).

[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, August 2016, p.14.

superiority and information control in theatres of operations] *requires a significant transformation of our operational architectures to place data at the heart of the future combat cloud. Expertise in the end-to-end architectures of functional chains should ensure interoperability, resilience and digital security (cybersecurity) of all systems and the sharing of information between all military personnel.*"[6] Again, there is no single definition of a "combat cloud" or "tactical cloud" (a misnomer, since multiple nodes are located far from the tactical edge). In reality, as with current networks, it all depends on the organisations and operational specificities of the various environments, even if many of the concepts and technical solutions can be transposed from one force component to another.

Concerning air operations, the focus of FCAS, the most vehement promoter of the cloud has been retired Lieutenant General David Deptula, member of the planning team for *Desert Storm*, inventor of the *Effects-Based Operations* concept and tireless advocate for air power at the head of the Mitchell Institute. In 2013, he set forth the notion of the "combat cloud" as an "*ISR/Strike/Manoeuvre/ Sustainment complex with the potential to usher in an entirely different architecture for the conduct of war*". Deptula considered this cloud to be the driver not only of air power but also of cross-domain synergy, which has been the mantra of American operational concepts for the past 10 years.[7]

In 2016, the U.S. Air Force's Air Combat Command developed an initial concept of operation for the air power combat cloud. It defined it as "*an overarching meshed network for data distribution and information sharing within a battlespace, where each authorised user, platform or node transparently contributes and receives essential information and is able to utilise it across the full range of military operations.*"[8] As the U.S. Navy, itself very advanced — possibly the most advanced — on the subject, explains, the tactical cloud does not consist in the outsourcing of data storage and the hosting of applications, or in server virtualisation, characteristic of a commercial cloud, even if these elements can be implemented. Above all, it is about storing and accessing a massive volume of data, hosted on multiple and disparate sources in a common environment, and providing the tools to extract meaning, to correlate data from multiple domains, using *big data* techniques and artificial intelligence in particular. **The tactical cloud must thus allow platforms and units to access a tool that was previously only available to operators at the strategic level.**[9]

The tactical cloud, a new expression of the vision behind the *Network Centric Warfare* concept

In light of these definitions, the tactical cloud appears to be nothing more or less than the continuation of the implementation of the *Network Centric Warfare* (NCW) concept developed in 1998 by Admiral Cebrowski and John Gartska, which became the central concept for the "Transformation" of U.S. forces over several years. NCW assumes that the networking of sensors, command and control (C2) elements and effectors offers a decisive advantage in combat.

In 2004, the Pentagon redefined a new set of rules characterisation network-centric joint combat:

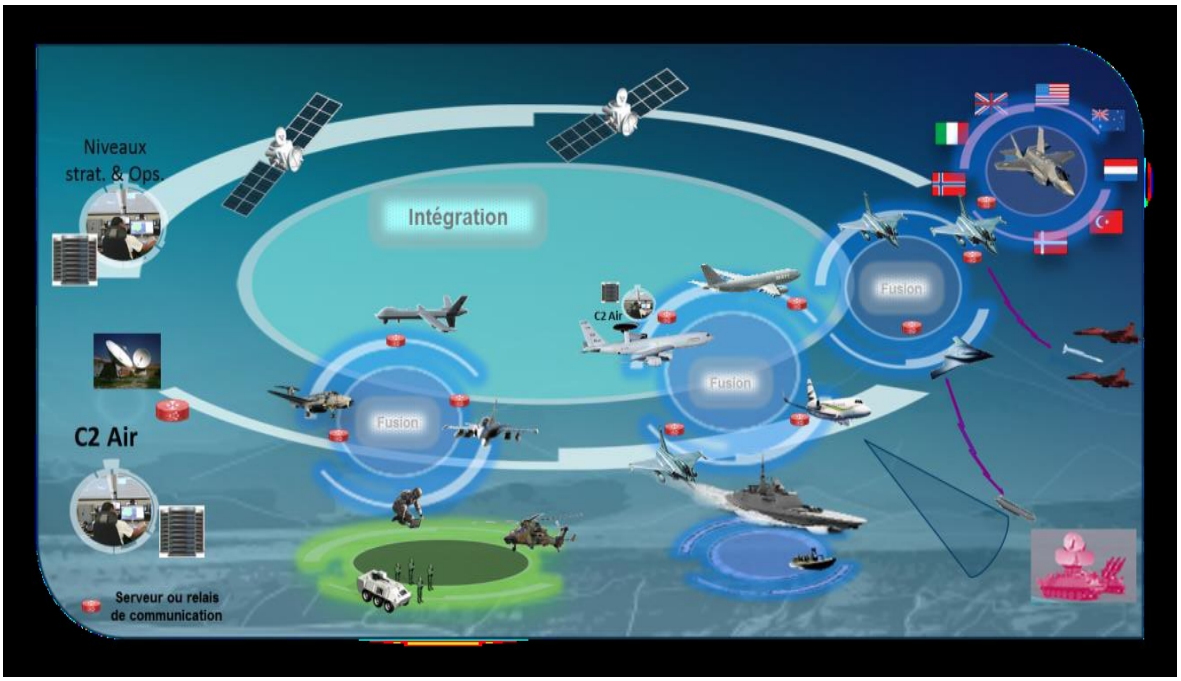
- "*Fight First for Information Superiority*": Paramount quest for information superiority over the enemy;
- "*High-Quality Shared Awareness*": Development of **common understanding and situational awareness** across the spectrum of participants;
- "*Dynamic* ***Self-synchronisation***" of low-level forces through exploitation of shared awareness;
- More rapid execution of **non-linear operations**, achievement of desired effects by a dispersed and "demassed" force;
- Compression of levels of war resulting from the integration of operations, intelligence (specifically Intelligence, Surveillance, Reconnaissance, ISR) and sustainment and the fusion of joint capabilities at the lowest tactical level (recently redesignated "multidomain" operations);

[6] MINARM, *Ambition numérique du ministère des Armées,* DICoD - Bureau des éditions - December 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*, cited in: 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.



Overall view of combat air system as seen by French Air Force – source: David Pappalardo, "Combat collaboratif aérien connecté, autonomie et hybridation Homme-Machine : vers un 'Guerrier Centaure' ailé ?", DSI, January-February 2019, p.71

♦Rapid **speed of command** by compressing sensor-to-decision-maker-to-shooter timelines, which turns information advantage into **decision superiority** over the adversary.[10]

It is true that the pumped-up implications of networking envisaged by the proponents of the "Revolution in Military Affairs" sank into the sands of Iraq and Afghanistan. Nevertheless, at the tactical level, many of these assumptions have been amply confirmed by the facts. From that time on, NCW's promoters conceived another information management cycle: Task, Post, Process, Use (TPPU), in which mission-oriented sensors post their data on the network; users take them, process them and use them according to their specific needs. This is more or less what is envisaged in tactical clouds.

Current TDLs allow for an initial implementation of NCW but constitute a constraint on information sharing

Current networking of air assets is based on tactical data link (TDL) systems, mainly the well-known link 16 (L16) which allows multinational interoperability, even if the U.S. has several other TDLs. L16 has already truly transformed air operations. It has thus made it possible to identify all friendly aircraft so equipped and to build up a single image of the air situation in a theatre. It makes the conduct of these operations much more flexible. For more than 10 years now, Western pilots have routinely received critical information about their mission, or even changes in target assignment, while in flight.

Exchanges, however, remain limited in many respects. Link 16 actually covers two different things: on the one hand, a transmission network (linking the on-board terminals on the different platforms) but also a catalogue of about 50 formatted operational messages (J-series messages, giving platform position, alerting, track monitoring, mission control and assignment, etc.)[11] and a "free text" capability depending on the platforms.[12]

Link 16, however, was conceived in the 1970s. It is true that it has undergone many improvements: extension of its range by satellite communications, multi-network gateways with other TDLs, *Network Enabled Weapons* (NEW, the inclusion of munitions on L16 for guidance onto moving targets), etc. However, an L16 network remains very complex to plan for each engagement and requires meticulous management by the *Joint Data Link Management Cell*.[13] It is therefore not a *Mobile Ad Hoc Network* like our telephone networks, for example. Its bandwidth is also very limited and its latency high. The exchange capacities offered by these TDL messaging systems are also limited. General Breton, who heads the FCAS programme, explains that "*an important aspect of innovation in FCAS will be networking: currently on the Rafale* [in its

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

[11] Not including those dedicated to network management.

[12] See the exceptional Wikipedia entry in French, written by a tactical datalink specialist.

[13] For general background, see CICDE, Les liaisons de données tactiques (LDT), Publication interarmées PIA -3.50_LDT(2017), N° 109/DEF/CICDE/NP dated 13 June 2017.

present configuration] *the pilot mainly uses his own sensors and some information provided by the network*"[14]. Thus, much of the data obtained by the aircraft is not shared, such as data from the Spectra system or the optronics sensor.[15]

The tactical cloud: an architecture focused on operational data

The cloud again raises this NCW issue in the era of much-vaunted "big data", characterised by the five Vs: volume, "velocity" (speed of transmission in continuous flow), variety (of formats), veracity and value. Tactical users run the risk of being overwhelmed by the "data tsunami", mentioned by General Ferlet, Director of French Military Intelligence. This extension of big data to the tactical level is explained by the diffusion of several technologies down to the level of platforms and deployed units:

- Sensor capabilities;
- Increased volume of transferable data at identical signal frequencies;
- Greater flexibility in the use of the electromagnetic spectrum through "software defined" techniques;
- Increasing capacity of information storage on a given volume;
- Software for the extraction and automated processing of data increasingly based on artificial intelligence using *machine learning*. This will allow (in theory at least and in the long run...) "predictive" analyses of the operational situation;
- Tools and architectures for the "fusion" of heterogeneous data, no longer based on simple correlation or mixing of information but on the integration of raw data from embedded or remote sensors. This is the "*fusion warfare*" already used by flight groups of fifth generation aircraft (F-22 and F-35) ... in isolation;[16]
- The diversity and speed of application development.

These technologies lead to a paradigm shift: from a logic where the network dictates the volume but also the format of the data exchanged to a logic where it is the data, in its extreme variety, that becomes the main parameter. In 2010 in the U.S., the *Chairman of the Joint Chiefs of Staff*, then General Dempsey, highlighted the transition to a *data-centric* environment.[17] The U.S. Air Force now prefers to speak of a "*data-to-decision*" cycle rather than a "*sensor-to-shooter*" cycle.[18]

If we extrapolate the conceptions involved in testing of the U.S. Navy's Data Focused Naval Tactical Cloud[19], the data that would be exchanged within an air combat cloud would be as follows:

- Sensor data (not only from radars, but also from warning systems, electronic support measures, andoptronic sensors) from the different platforms;
- Previously developed intelligence products;
- Other critical data on the operating environment (weather, topography, etc.);
- Data on the availability and instantiated performance of cloud participants' systems (status of units and platforms, sensors, weapons, etc.);
- "Historical" data relating to intelligence, the environment or previous operations. For example, we can mention the thematic bases for producing temporal GEOINT (geospatialisation of an activity, etc.);
- Open source data related to the operation, e.g. posted on social networks.

As the third V of big data indicates, data are no longer necessarily extracted from sources and then formatted specifically to be transferred to a TDL system. To exploit relevant information in a wide variety of formats, the Americans have been working for years on data strategies. The Air Force, for example, articulates its strategy around the registration of authoritative data sources,

[14] General Breton cited in Yves Pagot « Le SCAF raconté par ses concepteurs », *Portail Aviation*, 31 January 2019.
[15] Conversation with a manufacturer.
[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 Institute 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.

information cataloguing and access management, the development of relational databases between information based on metadata characterisation these available sources, and of course the development of interoperability and data protection measures.[20] The Navy's testing is based on the *Unified Cloud Model* used in the commercial sector, which combines the use of metadata for source identification with the analysis of content according to generic data models and ontologies, subsequently allowing user requests to be answered more precisely.[21]

The NGF, the future FCAS combat aircraft, a node of the cloud at the extreme tactical edge, would thus comprise:

♦Various applications designed for its different operational functions;

♦Automated analysis tools, possibly shared with other systems, implemented through its applications;

♦Common services also shared with other systems, operating transparently for the pilot;

♦Storage of large amounts of data;

♦Connection to the communication network with other platforms and units, a "self-forming & self-healing" MANET network.

This information system would operate with a large degree of automation and even autonomy because its increasing complexity will no longer be manageable by a crew, especially in a combat situation. General Breton explains that "*on FCAS* [...] *The management of data transfer by the network will be performed independently of the pilot, who will see the fused data. He will thus supervise the overall process.*"[22]
To describe empirically what this cloud allows and its ease of usage for the operator, one **often finds the comparison with the use of the smartphone, supplemented by increased automation of tasks,** in the explanations of its designers and architects, from U.S. generals to French General Breton.

Incremental progress towards the tactical cloud

Construction of the cloud will not be completed at a single stroke because technological building blocks are currently under development or even already implemented. This is obviously the case in the United States: i.e. the data fusion capabilities of fifth-generation aircraft (*fusion warfare* being the hallmark of the F-35) or the architectures being implemented step by step as of today by the U.S. Navy (*Cooperative Engagement Capability*, then *Naval Fire Control - Counter Air*, then its extension to other missions).

The French Air Force has also adopted an incremental approach to developing this cloud, with milestones in 2025 and 2030, designed to prepare for the arrival of FCAS. This is the Connect@aero programme that goes hand in hand with the deployment of the F4 standard on the Rafale. It aims in particular at the introduction of a higher-speed communication system and additional connectivity ramifications, including munitions f thus appying the NEW concept. The objective of this programme is to "detect enemy air defence systems with greater precision" and "collaboratively adapt the trajectories and manoeuvres" of effectors and their munitions, in a degraded positioning, navigation and timing (PNT) environment. The aim is to implement a "global air combat system" within the next decade.[23] Furthermore, the concepts do not envisage the emergence of a tactical cloud that would immediately encompass all air power tasks. The cloud will — again incrementally — assume the different operational functions, probably starting with shared situational awareness (improving what current TDLs allow) and moving towards predictive analytics, that will massively exploit intelligence manipulate the most complex objects and the largest amounts of data, thus requiring the most sophisticated tools.[24]

Benefits of the cloud: the example of a close air support mission

Let us consider the example of a close air support (CAS) mission. Notionaly, mission participants include the "effector" aircraft; the *Joint Terminal Attack Controller* (JTAC), embedded within the ground unit to request support and then coordinate or guide the strike or support action and possibly the forward observer if the JTAC is not present in the area; the combined arms commander, in

[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] General Breton cited in Yves Pagot *op cit.*
[23] David Pappalardo, « Combat collaboratif aérien connecté, autonomie et hybridation Homme-Machine: vers un 'Guerrier Centaure' ailé ? », *DSI*, January-February 2019, p 70-75.
[24] Navy test procedure, *Data Focused Naval Tactical Cloud* and conversation with a manufacturer.

his command centre; the "air control" network, which extends from the JTAC to the air operations centre or air support operations centre and includes officers positioned at the interface with the land force command echelons to collect CAS requirements at the planning stage and distribute aircraft for conduct of operations.

The process is as follows: at the request of his unit leader, his own observations or those of the observer, the JTAC makes a request for support with a recommendation for an air strike that the combined arms commander validates. The JTAC issues a request to the operational centre, which assigns the aircraft if this has not already been done at the planning stage. Once in the area, the aircraft contacts the JTAC; the latter provides the pilot with a formatted brief (the "*9 Line brief*" specifying the heading the aircraft needs to follow, distance from the target, elevation, description and coordinates of the target, friendly forces in the area, the type of marking the JTAC will perform) and additional remarks: air defence threats, coordination measures (e.g. if artillery fire is being carried out concurrently), desired method of attack. The pilot reads back part of the brief. Then the JTAC and he correlate their perception of the situation and verify the acquisition of the target. The pilot carries out his approach, and the JTAC clears him to fire.

In practice, **in the "all-radio" era that we are gradually leaving**, this dialogue between the JTAC and the pilot can sometimes last tens of minutes to be sure that the pilot hits the right target without collateral damage. However, it can still be a source of error or even impossible in the event of linguistic misunderstanding.

Current practice involves Digitally Aided CAS (DACAS), in other words the use of TDLs to reduce these risks of misunderstanding and error and accelerate the decision loop, even if radio remains necessary to clear or abort the mission. The JTAC communicates his request using the *Variable Message Format*, a TDL chosen by land forces because it can be broadcast on conventional radio network devices. The support operations centre validates and assigns the aircraft using L16. The elements of the *9 Line brief* are dispatched either by VMF message if the aircraft are equipped with this TDL (which is not the case for most USAF aircraft) or through several L16 messages. To prepare the engagement, the aircraft will extract the position of the friendly forces by interrogating, via L16, the *Blue Force tracking* server (the precise position of ground forces in the area) verified by the ground force command centre, usually at brigade level. Digitisation also allows the aircraft to receive the above-mentioned brief and other information from the JTAC even before contact is made. When contact is made, digitisation allows the JTAC to annotate an image transmitted by the aircraft's targeting pod to mark the target and allow the aircraft to communicate its aim point to the JTAC for confirmation before the attack. However, DACAS still faces multiple obstacles: different security levels between the JTAC and the aircraft (Secret level of the L16 vs. mission restricted level of the tactical ground network) that prevent the pilot from automatically integrating the data into his nav/attack system, requiring him to use a separate tool; correlation of data extracted from servers and emanating from the JTAC in the terminal phase, etc.[25]

With a mature tactical cloud, the speed and richness of information sharing and the exploitation of each stakeholder would potentially increase. It is conceivable that the JTAC would share at an early stage not only the elements of the request and the 9 Line Brief but also the representation of 3D volumes (the distribution of airspace volumes), environmental elements (topography, civilian environment, etc.) and a computer simulation of the proposed tactical approach. The JTAC would post all this information on the cloud and then update it. Once the assigned aircraft is known, he could automatically obtain the status and capabilities of its sensors and weapons in the current situation, allowing the strike to be prepared. On the assigned aircraft, the pilot would launch an application that would automatically remove and update these elements from the servers, and the elements would be integrated into his navigation and attack system which would provide him with recommended courses of action based on his approach heading. Once on-zone, his nav/ attack system data would be correlated with those of the JTAC, providing him, for example, with complementary perceptions from his sensors, or even from the drone that he might utilise (*manned-unmanned teaming*), allowing the pilot and the JTAC to share a better view of the situation.

We can also imagine the potential added value of this data contribution for dynamic

[25] Ideas taken from the technico-operational study for the implementation of digital exchanges during air support missions, written in 2014-2015 with contributions from the author.

interdiction missions, such as SCAR (*Strike Coordination and Reconnaissance*) missions. Making better use of existing analyses, or even the ability to make one's own correlations based on historical and situational data, can make a powerful contribution to the assessment of adverse courses of action currently in progress and to the direction of the mission execution. This type of analysis is currently carried out, at best, only in intelligence support of mission planning.

The cloud: a major factor in FCAS effectiveness, resilience and efficiency

The cloud is theoretically a significant factor in increasing FCAS effectiveness. Brigadier General (ret.) Jean-Michel Verney, FCAS operational advisor at Airbus, believes that "*for the first time, the need for information on board an air platform will supplant the need for speed in the fighter pilot's mantra.*"[26]

The shared situational awareness enabled by the cloud will be a factor in increasing or strengthening information superiority over the adversary, and the resulting decision-making superiority, as postulated by NCW. In addition, its interconnections, as well as the shared situational awareness thus generated, potentially enable **the full transition from connected combat to collaborative combat,** as called for by Caroline Laurent, Director of Strategy at the French defence procurement agency (DGA)[27], for which the French Air Force intends to achieve incrementally through the Connect@aero programme. Collaborative combat means that the capabilities of the different platforms are implemented as a single system to improve the detection of enemy systems and generate the desired effect more quickly and effectively, in action and in reaction. Thus, for example, weapons could be delivered by one platform based on integrated data from sensors on other platforms (as prefigured by NEW). The gain in effectiveness is not only reflected in the speed of execution of the OODA loop. As is apparent from the CAS example, better exploitation of intelligence, finer shared knowledge, in real time, of the operational capabilities of units engaged in a given situation, along with collaborative combat capability will increase the **precision of the desired effects.**

The implementation of such a combat cloud **should also lead to the transformation of the C2 function of operations,** an issue that has been the subject of much debate for several years. Air operations traditionally follow a dual doctrinal principle:

- control (planning, development of the *Air Tasking Order* choreographing the "ballet" of operations over 24 hours, the dynamic conduct of these 24 hours of operations, then their assessment) is centralised at the level of the combined air operations centre (CAOC) in order to best manage limited resources;

- execution is decentralised, i.e. partly carried out at the CAOC and partly delegated to "*battle management*" platforms such as AWACS, effectors (etc.), in order to guarantee the freedom of action necessary to deal with tactical contingencies.

With their modern sensors, recent combat aircraft have already become both effectors and ISR platforms. With the situational awareness and processing capabilities provided by the cloud, these aircraft and their successors will have the ability to take the initiative, allowing them, in the eyes of many observers, to assume an increased share of local control of operations, well beyond the current decentralised execution, i.e. to receive some of the authorities currently retained at the CAOC level. This is the concept of "distributed control."[28] The use of American F-35s and F-22s as "quarterbacks" for 4th generation aircraft is said to foreshadow this development despite the limited connections with other aircraft. However, the impact on the doctrine and organisation of the C2 function is still limited. Some stakeholders in the US even, consider a "Disaggregated C2" concept, a much larger distribution of control involving thoroughly overhauled decision-making cycles and possibly the disappearance of the CAOC as it exists, or the AWACS[29], which is perceived as a "extreme" view by many. Conversely, since some delegations of control may already exist in practice, others minimise the scope of this concept of "distributed control".

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

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

[28] See for example, 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.

Collaborative combat and these possible reorganisations of operations control are believed to confer **an increased degree of resilience and flexibility to air power** in the face of integrated air defence systems with redundant detection and interception capabilities, by guaranteeing the versatility and distribution of the actors in the "kill chain". This is the adage that it takes one network to fight another network. It also makes it possible **to optimise the performance, the efficiency of the air power used**. This is a particularly important point. The French air power is certainly the largest in Europe, along with that of the UK, but it still shows signs of weakness. This is the case for airborne ISR capabilities. This is also true for engagement/combat capabilities. The planned force structure of 225 combat aircraft (Air Force and Navy) must be able to deploy 45 aircraft (including the naval aviation group) under the operational contract for a major engagement. In practice, the French Air Force has struggled in recent years to permanently deploy about fifteen aircraft. Moreover, to do so, it has had to focus most of its sustainment resources on them, making it difficult for it to regenerate capacities. In other words, the French Air Force can perform well in long-distance raids and can provide limited support over time, but is no longer able to carry out a campaign alone. At the same time, it has been apparent for several years that U.S. participation in French engagements has gone from something that could be taken for granted to a worrying variable. A limited coalition action without the enormous resources of the U.S. Air Force becomes perfectly plausible. If the transition from the current system to FCAS follows the trend seen in all the generational shifts experienced by French air forces and those of its partners, there is a risk that the inventory will be reduced again, even if the incorporation of drones may be able to compensate for this continuing decline. In this context, the contributions of the cloud will be all the more critical.

Finally, at present, **only the Western and Israeli air forces have demonstrated their expertise in networked air operations. However, this advance is not set in stone** within the timeframe of FCAS. Thus, L16 has been distributed to all U.S. partners (including Saudi Arabia, the UAE, Japan, South Korea, Pakistan and Taiwan). The Chinese Air Force is naturally thought to have developed its own TDL[30], and the Pakistan AF, too[31]. We are therefore witnessing a gradual levelling of the playing field in networked operations.

However, the development of big data and associated processing capabilities, including artificial intelligence, is a fairly universal phenomenon. It is therefore mechanically accessible to many countries, not only to Western nations and their richest partners. Not developing this capacity means taking the risk of facing a situation of information inferiority against an opponent in the long term. Admittedly, the French forces have already encountered such situations, especially in irregular warfare environments, but rarely in tactical confrontation itself and never in the air domain. **The cloud therefore appears to be an essential milestone in military competition.**

The main risk: increased exposure to cyber-electronic threats

The move to the cloud is not without risk. The main one is obviously the threat of cyber-electronic attacks (i.e. the convergence of electronic warfare and cyber warfare, already widely recognised in doctrinal terms and the focus of technological development).[32] A distinction must be made here between jamming threats to the communications network and sensors, and threats classified as offensive cyber warfare that could potentially affect the entire cloud.

Until recently, L16 was considered quite secure against jamming. However, here again, rapid advances in information technologies can reshuffle the cards. It is true that functional distribution in the C2 and ISR domains helps to counter jamming actions on a particular system and to reduce the impact of these actions on a given node. The use of low probability of detection and intercept (LPD/LPI) TDLs will prolong and even increase the difficulty of jamming these communications. However, these new TDLs must not rely on timing from GNSS systems (such as GPS), which are vulnerable to jamming, as a synchronisation tool. In any case, use of the cloud will become a challenge in an electromagnetic environment strongly contested by an adversary who has himself adopted "adaptive electronic warfare" processes that flexibly distribute his efforts.

The offensive cyber warfare threat,

[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] See Philippe Gros, *Les opérations en environnement électromagnétique dégradé*, note n°1 de l'observatoire des conflits futurs, FRS, April 2018.

whether or not it involves this exploitation of the electromagnetic spectrum, appears even more problematic in the long term. Reports by the Pentagon's Director Operational Test & Evaluation regularly reflect the "cyber vulnerabilities" of many U.S. systems, including recent systems that have in theory taken this threat into account, such as the F-35.[33] However, the multiplication of interconnections increases the potential for electronic intrusions into the cloud and increases the risk of systemic effects. Moreover, by coupling a large part of the competitive advantage of air power to this deep and extensive networking, the cloud also increases the criticality of this vulnerability. In other words, with a tactical cloud insufficiently secured against an effective opponent, there is a potential **risk of systemic paralysis** of air power.

Major challenges relating to connection, interoperability and information sharing

The first major challenge for the cloud will therefore probably be **its ability to function in this extremely constrained electromagnetic environment, in which operations could often be degraded or even denied,** conditions which are far removed from the solid mesh of fibres and relay towers that underlie telephone networks. Operating procedures will have to be adapted to this intermittent connection, such as, for example, compensation by searching for TDL throughput, strengthening asynchronous transmissions, massive storage of data in mission planning, and collaborative combat models that can be executed without a connection.

Then there is the question of interdependence between players in the cloud. Achieving this interdependence requires, first and foremost, an unprecedented level of interoperability. However, for the long-time observer, most of the current presentations promoting the future arrival of this system of systems, with perfectly fluid exchanges of information between actors (etc.), vividly recall the emphasis on digitisation and NCW that has been prominent in the literature and in briefings for 25 years: the gloomy assessment of current performance is always followed by the same objectives. This repetition, year after year, or on the occasion of each new project aimed at advancing integration, actually demonstrates the highly elusive nature of these objectives. Experience in the United States shows that the setting of standards is not sufficient to guarantee interoperability between systems acquired in an institutional landscape with multiple decision-makers, who adapt these standards and/or develop their roadmap according to their own architectural timelines.

Interoperability has certainly made progress, as shown by the TDLs mentioned above. Simply, it has so far been achieved when an organic or operational authority has sufficient weight to impose its standards on the actors under its control (see, for example, the history of Blue Force Tracking, L16 or missile defence architecture); when partners of this authority fully agree to adopt these standards in the smallest detail, even the equipment that goes with them (the allies with L16, for example); and finally, and to a lesser extent, when convergence is sought on certain missions whose criticality is recognised (example of DACAS given above). In other words, interoperability is achieved through a bottom-up process, within the elements of a given armed force and possibly its direct partners, or an agency. However, this is changing today with the spread of information systems relying on modular open architectures that can be upgraded in theory in a much more flexible manner and are intended to replace the juxtaposition of "customer" systems. It remains to be seen whether these new systems will represent real progress in this area.

This raises the question of the standard-setting authority for the design of the FCAS cloud. At first sight, two options appear to be possible. The first one would be integration into the U.S. air power "cumulonimbus" (based on the F-35, the Joint Aerial Layer Network and its multi-network gateways, its conception of the C2 function, etc.) which the Americans will mechanically seek to impose within NATO. This option again raises the issue of French strategic autonomy principle. It also raises the question of the survival of a significant part of the French defense industrial and technological base. The second, in which the French Ministry of Defence is committed as mentioned earlier, is therefore to develop its own "cumulus". In this case, the question of interoperability with the U.S. and probably NATO architecture will arise. Unless the technologies currently under development allow flexible links, on demand, between the two systems. In any case, this calls for incremental development of a French cloud, concomitantly with the one currently being

[33] DOT&E reports are available at https://www.dote.osd.mil/.

developed by the Americans, without which this issue of standards is likely to be definitively resolved when FCAS will reach maturity.

Second, assuming that technologies and standards are in place, interdependence requires **a symmetrical and open policy of information sharing, particularly in the case of FCAS which is built on an international partnership.** However, facilitating access to intelligence products will be a permanent challenge, as will "fusion warfare" between sensors on aircraft from different countries. This is particularly true of electronic support sensors, whose data inputs into SIGINT are among the most sensitive in the intelligence system. In practice, this type of policy for sharing (or more precisely policy for exchange, in the intelligence field) is not self-evident and is only implemented if the highest authorities specify it. It therefore poses the challenge of training with limited information access and the risk, in operations, of having an asymmetric cloud.

Finally, there is the question of the perimeter of the cloud. **One of the main fears that can be raised about the FCAS tactical cloud is the extent to which the cloud will really take account of the other domains,** currently presented as belonging to the second "outer" circle. It should be noted that the vision promoted by General Deptula is that of a multi-domain cloud, not only dedicated to air forces, possibly including space and cyber (the multi-domain approach of many other air power actors), but also to land and naval forces. This vision is all the more relevant to the French forces, precisely because of the limited volume of the forces of each service. Thus, the cloud should be built not only as a function of typical air power missions, but for joint force missions. Regarding the example of CAS mentionned above, the cloud should typically encompass the broader fire support in its entirety, of which CAS is only one process and which would also include land and naval artillery fires. In other words, the FCAS cloud should aim for integration with the Scorpion combat cloud. Of course, this ambition would plunge us even further into the turmoil of interoperability described above. However, **maintaining the French military power at the forefront of Europe, in a high-risk strategic environment, and the ambition to remain a framework nation within limited coalitions, requires this ability for integrated joint force operations, of which the cloud must be an essential part.**

The opinions expressed here are the responsibility of the author alone.

The Foundation for Strategic Research is an independent research centre and a leading French think tank on defence and security issues. It conducts studies for French government departments and agencies, European institutions, international organisations and companies. It contributes to the strategic debate in France and abroad.

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