ÉTUDES
DE L'IFRI

CENTRE DES ÉTUDES DE SÉCURITÉ FOCUS STRATÉGIQUE n° 107

NOVEMBRE
2021

Le *cloud* défense

Défi opérationnel, impératif stratégique et enjeu de souveraineté

Clotilde BÔMONT

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

ISBN : 979-10-373-0447-6

Comment citer cette publication :
Clotilde Bômont, « Le *cloud* défense : défi opérationnel, impératif stratégique et enjeu de souveraineté », *Focus stratégique*, n° 107, Ifri, novembre 2021.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Focus stratégique

Les questions de sécurité exigent une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection ***Focus stratégique***, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, ***Focus stratégique*** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

Comité de rédaction

Auteur

Clotilde Bômont est chercheure au sein du centre de recherche et de formation GEODE (Géopolitique de la datasphère). Elle réalise actuellement une thèse de doctorat en géographie à l'Université Panthéon-Sorbonne, portant sur l'intégration du *cloud computing* dans les systèmes d'information militaires et les enjeux de souveraineté inhérents. Elle est également chercheure associée au Centre de recherche des Écoles de Saint-Cyr Coëtquidan (CREC).

Ancienne allocataire de la Direction générale des relations internationales et de la stratégie (DGRIS), Clotilde Bômont a également été rattachée à l'Institut de recherche stratégique de l'École militaire (IRSEM, 2016-2020). Elle a aussi été consultante pour la DGNUM (2018-2019) et chercheure invitée à l'Université Columbia (New York, 2019).

Résumé

Le ministère des Armées français a décidé de faire de l'informatique en nuage – ou *cloud computing* – l'un des piliers de sa transformation numérique. Recourir au *cloud* suppose néanmoins d'externaliser en partie la gestion des ressources informatiques, ce qui pose de nombreux défis d'ordre technique et culturel, mais aussi politique et industriel. À l'impératif de maîtrise technologique s'ajoutent en effet des enjeux stratégiques capitaux ayant trait à des questions d'autonomie et d'influence. Le *cloud* défense dépend donc autant de la capacité des armées à adapter la technologie à leurs exigences sécuritaires et opérationnelles, que des partenariats industriels mis en place par le ministère, et des politiques nationales sur le sujet.

De la RMA au *cloud* défense : en marche vers l'infogérance

À partir des années 1970 et dans un contexte de guerre froide, les agences américaines de défense investissent massivement pour développer les technologies informatiques et électroniques. Ces dernières bousculent profondément l'organisation et la conduite de la guerre, au point d'être parfois considérées comme une « révolution dans les affaires militaires ». Cette rupture a embrassé simultanément les champs de l'organisation bureaucratique (concept de *Transformation*) et de la doctrine d'emploi (*Network-Centric Warfare*). S'inspirant des stratégies américaines mais adoptant une approche plus progressive, les armées françaises entament elles aussi leur numérisation dès les années 1990 (numérisation de l'espace de bataille).

La numérisation s'opère par la mise en données du monde réel, soit sa transcription en langage informatique, et par la mise en réseau des divers récepteurs, soit l'interconnexion des décideurs, des effecteurs et des senseurs. Conséquences directes, la prolifération des données et la complexification des systèmes d'information et de communication (SIC) posent plusieurs défis tels que le stockage, l'exploitation et la discrimination des données, l'interopérabilité des systèmes, ou encore la maîtrise des compétences liées aux technologies de l'information et de la communication (TIC). Développé dans les années 2000 par le secteur civil, le *cloud* est alors apparu comme une réponse aux nouveaux besoins informatiques des armées.

Le *cloud* est un mode d'organisation des systèmes d'information (SI) qui repose sur l'infogérance, c'est-à-dire l'externalisation par l'utilisateur de la gestion de ses ressources informatiques (serveurs, plateformes, applications, données…) auprès d'un fournisseur de services. Ce dernier met alors ses capacités de stockage et de calcul à la disposition de son client, sur un principe de location. Ce fonctionnement présente de nombreux avantages pour le ministère des armées, tant sur le plan opérationnel, puisque le *cloud* contribue à augmenter la capacité informationnelle des forces (meilleure appréciation situationnelle, accélération de la boucle *Observe, Orient, Decide, Act* – OODA, mutualisation des informations) que sur le plan organisationnel (rationalisation et optimisation des ressources, augmentation de la productivité). Il est aujourd'hui considéré comme un prérequis à l'intégration d'autres technologies émergentes (internet des objets, intelligence artificielle, 5G/6G, etc.). Le *cloud* étant initialement une technologie civile, son adaptation aux besoins et aux exigences du ministère peut toutefois poser problème, notamment du fait des différences culturelles importantes entre les entreprises du numérique, « agiles » et fonctionnant sur des cycles courts, et le monde militaire, hiérarchique et bureaucratique.

Dans les années 1990-2000, la numérisation des armées se heurte à divers écueils : développement cloisonné des systèmes, méfiance à l'égard de l'externalisation, blocages culturels entre armées. Le ministère décide alors de créer en 2003 une organisation pour jouer le rôle d'opérateur unique et interarmées : la Direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI), qui portera les premiers travaux sur le *cloud* défense, dont le projet d'Infrastructure communicante adaptée sécurisée (INCAS). Le *cloud* défense tarde néanmoins à voir le jour et ce n'est qu'à partir de 2018 que les initiatives s'accélèrent, à la suite de l'annonce par le gouvernement d'une doctrine nationale sur le *cloud*. De nombreux chantiers sont alors initiés au sein du ministère et sont placés sous le pilotage de la Direction générale du numérique et des systèmes d'information et de communication (DGNUM), créée pour orchestrer la transformation numérique du ministère. L'annonce le 17 mai 2021 d'une nouvelle « Stratégie nationale pour le *cloud* » vient cependant bouleverser les travaux entrepris. La nouvelle stratégie se veut davantage en cohérence avec le projet européen GAIA-X et l'écosystème industriel national, mais apporte de profonds changements puisqu'elle prévoit le développement d'un *cloud* commun à l'ensemble de l'administration française, en lieu et place de solutions ministérielles harmonisées. Aussi son impact sur les démarches entamées par le ministère des Armées est-il encore incertain.

Adapter le *cloud* aux spécificités du ministère des Armées

Le ministère héberge, produit et manipule des informations dont la sensibilité peut être très élevée. La migration vers le *cloud* doit donc impérativement en tenir compte pour garantir la sécurité des données. Elle implique de repenser les systèmes de classification à l'aune des technologies numériques. L'infogérance pouvant présenter un risque pour la confidentialité, l'intégrité et la disponibilité des données, il convient également de définir les modalités d'externalisation (prestataire ou opérateur interne, infrastructures sur site ou hébergement distant, nature des SI externalisés, etc.).

La mise en place de solutions *cloud* communes à l'ensemble du ministère suppose également de prendre en compte la diversité et les spécificités des personnels, dont les besoins et les attentes vis-à-vis du *cloud* diffèrent selon leur métier (combat, administratif, santé, formation, restauration…) et dont les cultures numériques sont variables. La difficulté de recrutement dans les fonctions SIC pourrait cependant entraver le développement du *cloud* défense.

Le *cloud* pouvant contribuer à la capacité informationnelle des forces, il est aussi voué à intégrer l'infostructure de combat. Ce *cloud* tactique constitue alors le support technologique permettant l'interconnexion des différents systèmes déployés en opérations, des centres de commandement jusqu'aux terminaux embarqués, grâce à des dispositifs projetables sur les théâtres. La connectivité aléatoire, le besoin de mobilité des équipements, le déploiement des infrastructures en environnement hostile et le manque d'interopérabilité entre les plateformes sont autant de contraintes auxquelles le *cloud* tactique doit pouvoir faire face pour assurer la continuité des opérations et la sécurité des forces. Des projets de *cloud* de combat sont en cours au sein des trois armées, à l'image des nouvelles générations des programmes aérien (SCAF) et terrestre (SCORPION) dont les SI reposeront sur du *cloud*. Pour favoriser le combat collaboratif, le *cloud* a également vocation à être multi-domaines (programme de système d'information des Armées, SIA) et interalliés (*cloud* otanien).

Un *cloud* non souverain pour un ministère régalien ?

Si l'infogérance pose des enjeux techniques, culturels et organisationnels, elle présente également un risque géopolitique. Le marché mondial du *cloud* est largement dominé par les entreprises américaines (Amazon, Microsoft, Google…). Or le gouvernement

américain dispose de lois à portée extraterritoriale, telles que le *CLOUD Act*, lui permettant d'accéder aux données gérées par un fournisseur, y compris celles hébergées hors du territoire étatsunien, et celles relatives à des organisations ou des citoyens étrangers. Dans ces conditions, recourir à un prestataire soumis à une juridiction autre que la juridiction française (ou européenne) présente un risque important pour la sécurité des données du ministère des Armées et pose, en sus, des enjeux de souveraineté. Cependant, les entreprises françaises peinent à rivaliser avec les géants américains, techniquement performants et économiquement compétitifs. Les stratégies industrielles du ministère devront dès lors évaluer la part et la nature des risques acceptables. À la notion de fournisseur de technologies succède donc progressivement celle de partenaire stratégique.

La question industrielle est donc un élément central dans les stratégies *cloud*, ainsi que le démontre l'échec du projet américain JEDI (Joint Entreprise Defense Infrastructure), pendant du *cloud* défense français. JEDI devait permettre d'harmoniser les solutions *cloud* en proposant un socle architectural commun à l'ensemble du département de la Défense. Mais la concurrence entre les fournisseurs potentiels et les démêlés juridiques inhérents a conduit à l'annulation du projet qui, après révision, sera remplacé par le Joint Warfighter Cloud Capability.

En France, l'échec des initiatives pour développer des solutions *cloud* dites « souveraines » (Cloudwatt et Numergy) a montré les limites du marché local, et les réflexions stratégiques sont aujourd'hui conduites au niveau régional. Plusieurs démarches ont été entreprises dans ce sens, aussi bien par les institutions européennes que par les fournisseurs de services *cloud* eux-mêmes. Toutes les parties prenantes s'accordent effectivement sur le besoin d'ouvrir le marché du *cloud* à l'échelle européenne afin de permettre aux entreprises d'atteindre une taille critique. Cette dynamique a conduit au lancement en 2019 du projet européen GAIA-X qui vise à rendre aux Européens la « maitrise de leurs données » en facilitant le développement de la base industrielle européenne du *cloud*. La présence d'entreprises américaines et chinoises au sein du projet semble toutefois le rendre difficilement compatible avec les exigences du ministère des Armées.

Executive Summary

Cloud computing – or data management – is considered as one of the pillars of the digital transformation of the French Ministry of the Armed Forces. However, it requires to outsource the management of IT resources, which poses many technical and cultural as well as political and industrial challenges. In addition to the necessity of controlling the technology, there are major strategic issues relating to autonomy and influence. The defense cloud therefore depends as much on the capacity of the military to adapt the technology to its security and operational requirements, as on the industrial partnerships set up by the ministry, and national policies on the matter.

From RMA to Cloud Defense: Moving towards Outsourcing

From the 1970s and in the context of the Cold War, American defense agencies invested heavily in developing computer and electronic technologies. These profoundly shook up the organization and conduct of war, amounting for some to a “Revolution in Military Affairs”. This rupture simultaneously embraced the fields of bureaucratic organization (Transformation concept) and employment doctrine (Network-Centric Warfare). Inspired by American strategies but adopting a more progressive approach, the French military also began its digitization in the 1990s (battlefield digitization).

Digitization requires the transformation of real world into data, either through its transcription into computer language (code), and by connecting various receptors, including decision-makers, effectors and sensors. As a direct consequence, the proliferation of data and the increasing complexity of information and communication systems pose several challenges such as the storage, use and discrimination of data, the interoperability of systems, or the mastery of skills. Developed in the 2000s by the civilian sector, the cloud then appeared as a response to the new IT needs of the armed forces.

The cloud is a way of organizing information systems (IS) based on the outsourcing by the user of the management of its IT resources (servers, platforms, applications, data…) to a service provider. The latter makes the storage and computing capacities available to its client, on a rental basis. This has many advantages for the Ministry of the Armed Forces, on the operational level since the cloud increases the informational capacity of the military (better situational

assessment, acceleration of the Observe, Orient, Decide, Act loop, information sharing) and, as well as on the organization one (rationalization and optimization of resources, increased productivity). Cloud is a prerequisite for the integration of other emerging technologies (Internet of Things, artificial intelligence, 5G/6G, etc.). However, since the cloud was initially a civilian technology, its adaptation to the needs and requirements of the ministry is challenging, because of the significant cultural differences between digital companies, which are "agile" and operate on short cycles, and the hierarchical and bureaucratic world of the military.

In the 1990s-2000s, the digitization of the armed forces came up against various pitfalls: development of systems in silos, mistrust of outsourcing, and cultural blockages between the armed forces. In 2003, the Ministry created an organization to play the role of a single, joint operator: the DIRISI, which carried out the first work on the defense cloud, including the Secured Adapted Communicating Infrastructure project (INCAS). However, the defense cloud was slow to emerge, and it was not until 2018 that initiatives began to accelerate, following the government's announcement of a national doctrine on the cloud. Numerous projects were then initiated within the Ministry and placed under the guidance of the DGNUM, created to pilot the Ministry's digital transformation. However, the announcement on May 17, 2021 of a new "National Strategy for the Cloud" changed the course of this work. The new strategy is intended to be more consistent with the European GAIA-X project and the national industrial ecosystem, but it also brings about profound changes, since it provides for the development of a common cloud for the entire French administration, instead of harmonized departmental solutions. Its impact on the steps taken by the Ministry of the Armed Forces is therefore still uncertain.

Adapting the Cloud to the Specificities of the Ministry of the Armed Forces

The Ministry hosts, produces and handles very sensitive information. Migration to the cloud must therefore guarantee data security, which implies to rethink classification systems in the light of digital technologies. As outsourcing present a risk to the confidentiality, integrity and availability of data, it is also important to define the outsourcing methods (service provider or internal operator, on-site infrastructures or remote hosting, nature of the outsourced IS, etc.).

The implementation of cloud solutions common to all departments of the Ministry also requires considering the diversity and specificities of the personnel, whose needs and expectations with regard to the cloud differ according to their profession (combat,

administrative, health, training, catering, etc.) and whose digital cultures vary. However, the difficulty of recruiting for communication and information systems functions could hinder the development of the defense cloud.

As the cloud contribute to the informational capacity of the military, it should also integrate the combat information structure. This tactical cloud is the technological support that enables the interconnection of the different systems deployed in operations, from command centers to onboard terminals, thanks to devices that can be projected on the field. Random connectivity, the need for equipment mobility, infrastructure deployment in hostile environments and the lack of interoperability between platforms are all constraints that the tactical cloud must be able to cope with to ensure continuity of operations and security for the forces. Combat cloud projects are underway within the French Army, Air Force and Navy, as the new generations of air (SCAF) and land (SCORPION) programs whose information systems will be based on the cloud show. To promote collaborative combat, the cloud is also intended to be multi-domain and inter-allied (NATO cloud).

A Non-sovereign Cloud for a Sovereign Ministry?

In addition to the technical, cultural and organizational challenges, outsourcing also presents a geopolitical risk. The global cloud market is largely led by American companies (Amazon, Microsoft, Google, etc.). However, the American government has laws with extraterritorial reach, such as the CLOUD Act that allows to access data managed by a provider, including data hosted outside the United States, and data relating to foreign organizations or citizens. Under these conditions, using a provider subject to a jurisdiction other than French (or European) presents a significant risk for the security of the Ministry of the Armed Forces' data and seems hardly compatible with sovereignty. However, French companies are struggling to compete with the technically efficient and economically competitive American giants. The Ministry's industrial strategies will therefore have to evaluate the share and nature of acceptable risks. The notion of technology supplier is gradually being replaced by that of strategic partner.

Hence the industrial aspect is key to cloud strategies, as demonstrated by the failure of the American JEDI (Joint Enterprise Defense Infrastructure) project. JEDI was supposed to improve cloud solutions through a common architectural foundation for the entire Department of Defense. But competition between potential suppliers

and the inherent legal wrangling have wrecked the project, which is replaced by the Joint Warfighter Cloud Capability.

In France, the failure of initiatives to develop so-called "sovereign" cloud solutions (Cloudwatt and Numergy) exemplified the limits of the local market, and strategic thinking is now conducted at the regional level. Several steps have been taken in this direction, both by European institutions and by the cloud service providers themselves. All stakeholders agree on the need to open the cloud market to the European scale, so that companies can reach critical mass. This dynamic led to the launch in 2019 of the European GAIA-X, which aims to give Europeans "control over their data", through the development of the European cloud industrial base. However, having American and Chinese companies in the project seems hardly compatible with the requirements of the Ministry of the Armed Forces.

Sommaire

Introduction

Le 17 mai 2021, le gouvernement français annonçait la réorientation de sa stratégie *cloud*[1], formalisée pour la première fois en 2018. Poursuivant les efforts amorcés trois ans plus tôt, la nouvelle doctrine de l'État – dite « *cloud* au centre » – réaffirme la systématisation du recours au *cloud* dans les administrations, mais se veut davantage tournée vers les projets européens et prévoit une plus grande mutualisation des solutions techniques au niveau interministériel. Cette réorientation, si elle atteste de l'actualité du sujet, montre également que la France tâtonne et que les défis techniques, politiques et industriels que pose le *cloud* n'ont pas encore été relevés. Ces difficultés de positionnement au niveau politique impactent le ministère des Armées qui tente depuis une dizaine d'années de développer son *cloud* défense[2].

Le *cloud* est un mode d'organisation des systèmes d'information et de communication (SIC) qui peut effectivement permettre au ministère de faire face aux difficultés liées à sa numérisation (augmentation massive des données, multiplication des SI…). Entamée dans les années 1990, la numérisation du ministère de la défense français s'est inspirée des réflexions conduites au sein du département de la Défense américain, qui contribuait alors largement au développement des technologies informatiques. Durant les décennies suivantes, l'accélération fulgurante et la démocratisation des innovations dans le domaine numérique ont contribué à extraire les nouvelles technologies de l'information et de la communication (NTIC) du champ exclusivement stratégique et militaire. Elles sont aujourd'hui essentiellement développées par des entreprises privées, multinationales et dont le poids économique est tel qu'il influe sur les relations internationales. Le *cloud* fait partie de ces technologies qui se sont un temps émancipées des cercles de réflexions étatiques. Si son intégration dans les SIC du ministère des Armées pose des problèmes d'ordre technique, culturel, structurel et opérationnel, elle soulève également des enjeux politiques et stratégiques capitaux ayant trait à des questions d'autonomie, de sécurité et d'influence.

1. Le terme « *cloud* » est la contraction de « *cloud computing* », que l'on traduit en français par « informatique en nuage ». L'expression anglaise est couramment usitée, y compris dans les documents officiels français. Les trois termes sont donc ici employés de façon équivalente.
2. Le terme « *cloud* défense » désigne l'ensemble des solutions *cloud* utilisées par le ministère des Armées français.

La construction du *cloud* défense est donc multidimensionnelle et multiscalaire. Aussi doit-elle être analysée à plusieurs niveaux :

- au niveau ministériel, le *cloud* devant prioritairement répondre aux besoins du ministère des Armées ;
- au niveau des politiques nationales, puisque le *cloud* pose des enjeux géopolitiques importants et peut constituer une faille dans la souveraineté de l'État, notamment du fait de la répartition des principaux fournisseurs de services *cloud* et de l'extraterritorialité du droit, en particulier étatsunien et chinois ;
- au niveau européen, puisque l'échelle régionale apparaît comme la seule permettant l'émergence d'un secteur industriel capable de proposer des alternatives convaincantes aux entreprises américaines et chinoises. C'est également au niveau européen que se décident plusieurs standards techniques, notamment dans le cadre du projet GAIA-X.

Il apparaît alors que le *cloud* défense, pourtant un objet technique, est indissociable du contexte politique, économique et social au sein duquel il est déployé. Cette étude s'emploie donc à démontrer que, si son développement a d'abord été envisagé au niveau organisationnel et dans la continuité des efforts de numérisation du ministère, le *cloud* défense est aujourd'hui contingent des projets et des postures stratégiques gouvernementales dans le domaine numérique, et des partenariats industriels que pourra mettre en place le ministère des Armées.

Pour comprendre la place du *cloud* dans les armées françaises, il convient de revenir sur ses origines et sur les raisons qui ont conduit le ministère des Armées à en faire l'un des piliers de sa transformation numérique (I). Les spécificités du ministère complexifient néanmoins la migration de ses systèmes d'information et de communication (SIC) vers l'informatique en nuage, et impliquent de repenser les modèles traditionnels de *cloud* (II). Pour garantir que cette transition ne présente aucun risque pour la sécurité des données, le choix des partenaires industriels avec lesquels le ministère s'associera est crucial. Bien qu'il s'agisse d'un ministère régalien et en dépit des risques relatifs à la maîtrise des données, le ministère des Armées pourrait être amené à recourir à des fournisseurs non nationaux (III).

De la RMA au *cloud* défense : en marche vers l'infogérance

En une quarantaine d'années, les technologies de l'information et de la communication (TIC) se sont imposées sur les théâtres d'opérations militaires, bousculant profondément l'organisation et la conduite de la guerre. Leur développement s'est accompagné d'évolutions doctrinales et a généré de nouveaux besoins informatiques, qui ont progressivement conduit à l'adoption du *cloud computing*. Si les promesses du *cloud* sont nombreuses, son intégration dans les SIC du ministère des Armées n'a d'abord pas été une priorité. Les intérêts de cette technologie étant aujourd'hui mieux compris, le *cloud* fait l'objet de réflexions stratégiques aux plus hauts niveaux du ministère et de l'État.

Conduire la guerre à l'ère informationnelle

La révolution informationnelle des Armées

L'intégration du *cloud* dans les armées s'inscrit dans un processus d'évolution du domaine militaire initié dès les années 1970-1980, et parfois présenté comme la dernière révolution dans les affaires militaires (*Revolution in Military Affairs*, RMA). À cette époque, les technologies électroniques et informatiques connaissent un essor important, notamment grâce au soutien à la recherche et au développement apporté par les agences américaines de défense, au premier rang desquelles la Defense Advanced Research Projects Agency (DARPA). Ces innovations technologiques sont de plus en plus intégrées au sein des forces étatsuniennes, tant dans leurs armements (GPS, télécommunications, lasers, etc.) que dans la planification des opérations. Elles sont censées apporter aux troupes américaines, alors affaiblies par l'échec de la guerre du Vietnam, un avantage qualitatif pour compenser, dans la perspective d'une guerre de haute intensité en Centre-Europe, la supériorité quantitative des troupes soviétiques[3]. Constatant la portée des avancées américaines,

3. J. Henrotin, *La Technologie militaire en question. Le cas américain et ses conséquences en Europe*, Paris, Economica, 2013, p. 14.

le maréchal soviétique Nikolai Ogarkov est le premier à souligner leur caractère révolutionnaire. Il insiste sur l'importance pour l'URSS des technologies électroniques et informatiques qui, aux côtés des technologies nucléaires, sont selon lui « l'une des principales sources du développement des affaires militaires en général[4] ». S'inspirant de la « révolution scientifique et technique » à l'œuvre en URSS depuis les années 1960, Ogarkov parle ainsi, dès le début des années 1980, d'une « révolution technique militaire ».

Ce n'est que durant la première moitié des années 1990 que la « technologisation » progressive des armées est perçue par les Américains, *a posteriori*, comme une « révolution dans l'art de la guerre », ainsi que l'affirme en 1992 le secrétaire à la Défense Dick Cheney[5]. Ce tournant conceptuel fait suite à la victoire de la coalition conduite par les États-Unis lors de la guerre du Golfe. La fulgurance de la bataille, qui s'est déroulée du 17 janvier au 28 février 1991, ainsi que le rôle central des nouvelles technologies dans l'issue du combat poussent certains analystes américains à évoquer un changement de paradigme. En 1993, Andrew Marshall, alors responsable de l'Office of Net Assessment (ONA), reprend ainsi le concept d'Ogarkov et introduit le terme de *Revolution in Military Affairs* (RMA)[6].

Selon Marshall, une RMA correspond à un changement majeur dans la nature de la guerre et la conduite des opérations, causé par l'utilisation de nouvelles technologies et l'introduction de nouveaux concepts doctrinaires et organisationnels accompagnant leur intégration[7]. Une RMA est donc bien « le produit d'un ensemble d'innovations dans les domaines technologique, doctrinaire et organisationnel[8] ». Elle n'en demeure pas moins un « processus de transformation socio-technique » ; elle ne peut être décorrélée du contexte social, économique et politique qui conditionne son existence, soit parce que ce contexte est à l'origine des évolutions dans les affaires militaires, soit parce qu'il en permet la réalisation (forces économiques et industrielles, évolution des instances administratives de l'État, etc.)[9].

4. N. Ogarkov, *Vsegda v gotovnosti k zashchite otechestva*, Moscou, Voyenizdat, 1982, p. 36. Cité par D. Herspring, « Nikolay Ogarkov and the Scientific-technical Revolution in Soviet Military Affairs », *Comparative Strategy*, vol. 6, n° 1, 1987, p. 29-59.
5. J. Henrotin, *La Technologie militaire en question*, *op. cit.*, p. 15.
6. C. Wasinski, « Créer une Révolution dans les affaires militaires : mode d'emploi », *Cultures & Conflits*, n° 64, 2006, p. 149-164.
7. J. McKitrick *et al.*, « The Revolution in Military Affairs », *in* B. Schneider et L. Grinters (dir.), *Battlefield of the Future: 21st Century Warfare Issues*, Maxwell AFB Alabama, Air University Press, 1998, p. 65-97.
8. T. Balzacq, « Bienvenue dans la guerre *high-tech* », *in* T. Balzacq et A. De Nève (dir.), *La Révolution dans les affaires militaires*, Paris, Economica, p. 15-29.
9. *Ibid.*

Aussi la RMA des années 1990 est-elle directement liée aux progrès des technologies informatiques, qui ont entraîné l'avènement d'une « société informationnelle » au sein de laquelle « la création, le traitement et la transmission de l'information deviennent les sources premières de la productivité et du pouvoir[10] ». Selon Alvin et Heidi Toffler, ces évolutions sociétales ont conduit à une nouvelle forme de guerres qu'ils qualifient de guerres de la « troisième vague ». À la suite des « guerres agraires » du néolithique, puis des « guerres industrielles » du XIXe siècle, les guerres contemporaines seraient « informatiques ». Reprenant l'expression de Peter Drucker, les époux Toffler parlent de « guerres de la connaissance » (*knowledge warfare*) au sein desquelles la maîtrise des TIC est primordiale[11]. Grâce à l'informatique et la microélectronique, la RMA amorcée dans les années 1970-1980 se caractérise donc par une augmentation significative de la précision des frappes, et par des progrès conséquents en matière d'acquisition et de traitement de l'information[12]. Les capacités de renseignement, de surveillance, d'acquisition d'objectifs et de reconnaissance (ISTAR) sont ainsi décuplées, et les systèmes de commandement et de contrôle (C2) sont progressivement informatisés afin de leur permettre de traiter une quantité grandissante de données.

De la Network-Centric Warfare *américaine au développement incrémentiel français*

Bien que l'impact des NTIC sur les affaires militaires soit communément reconnu, la notion de RMA ne fait pas toujours consensus. Sa pertinence même est débattue, les changements observés dans les affaires militaires étant parfois perçus comme relevant davantage de l'évolution que de la révolution[13]. Sa traduction opérationnelle a également été pointée du doigt, même si ce sont en réalité les interprétations de la RMA et les décisions prises par certains dirigeants qui sont décriées. Les principales critiques portent notamment sur la réduction des effectifs sur les théâtres à la suite de l'intégration de nouvelles technologies[14], et sur l'absence

10. M. Castells, *La Société en réseaux. L'ère de l'information*, Paris, Fayard, 1996, p. 43.
11. A. Toffler et H. Toffler, *Guerre et contre-guerre : Survivre à l'aube du XXIe siècle*, Paris, Fayard, 1993.
12. É. de Durand, « Révolution dans les affaires militaires : 'révolution' ou 'transformation' ? », *Hérodote*, n° 109, 2003, p. 57-70.
13. En France, voir B. Tertrais, « Faut-il croire à la 'Révolution dans les affaires militaires' ? », *Politique étrangère*, n° 63, 1998, p. 611-629 ; P. Braillard et G. Maspoli, « La 'Révolution dans les affaires militaires' : paradigmes stratégiques, limites et illusions », *AFRI*, vol. III, 2002, p. 630-645.
14. Cette critique fut notamment formulée à la suite de la guerre d'Irak (2003-2011). Fort de l'idée selon laquelle la supériorité informationnelle et les armes de précision améliorent l'efficacité et la puissance des forces, le secrétaire à la Défense américain Donald Rumsfeld avait privilégié le déploiement sur les théâtres irakiens d'un nombre limité de combattants équipés de

d'anticipation quant à l'adaptation des États rivaux des États-Unis et de leurs ennemis non étatiques à ces nouvelles « guerres informationnelles[15] ».

Cette représentation d'une guerre centrée sur la technologie et l'information a tout de même guidé les évolutions du département de la Défense américain (DoD) depuis la fin des années 1990, et continue d'influencer les politiques de défense américaines comme étrangères. Elle a donné lieu aux États-Unis au concept de « transformation » des forces. Le terme fait son apparition pour la première fois en 1999, lorsque le chef d'État-major de l'US Army, le général Eric K. Shinseki, annonce la parution du document stratégique *Army Vision 2010*[16]. Il souligne alors la nécessité de transformer en profondeur l'armée américaine pour répondre aux évolutions du contexte des opérations[17]. Ce besoin de transformation des forces est également souligné pendant la campagne présidentielle de 2000 et se traduit sous la présidence de Georges W. Bush par la création le 29 octobre 2001 du Bureau pour la transformation des forces (Office of Forces Transformation, OFT), placé sous la direction du vice-amiral Arthur Cebrowski. La « transformation » des forces devient alors un concept opératoire pour mettre en œuvre cette « révolution socio-technique » au sein de l'organisation militaire.

La « transformation » peut ainsi être vue comme la mise en application de la RMA par le DoD. La RMA bouleversant profondément l'ensemble de l'organisation militaire, la « transformation » doit s'opérer dans tous les secteurs du département. Elle comporte donc trois volets : l'organisation interne du département de la Défense, la collaboration avec les agences extérieures et les partenaires multinationaux, et la conduite du combat[18]. Vingt ans après les débuts de la « transformation », le *cloud computing* intervient dans chacun de ces volets, que l'on retrouve également dans les stratégies actuelles du ministère des Armées français.

Parmi ces trois volets, c'est d'abord sur le plan doctrinal et dans la conduite des opérations que l'intégration des technologies informatiques a été pensée. Pour traduire sur les théâtres

hautes technologies. Néanmoins, le besoin d'accroître les effectifs sur le terrain pour contrôler la situation post-conflit a invalidé l'idée d'une Révolution qui permettrait de réduire drastiquement le nombre de combattants. Pour autant, du fait des progrès des nouvelles technologies, et en particulier des systèmes télé-opérés, télé-supervisés ou autonomes, ce débat est toujours d'actualité et l'équilibre reste à trouver.

15. E. Cohen, « Change and Transformation in Military Affairs », *Journal of Strategic Studies*, vol. 23, 2004, p. 395-407.

16. *Army Vision 2010*, Department of Defense, Department of the Army, Washington D.C., 1999.

17. Association of the United States Army, *How "Transformational" Is Army Transformation?,* Torchbearer National Security Report, Institute of Land Warfare, 2003.

18. « The Implementation of Network-Centric Warfare », Office of Force Transformation, Washington D.C., 2005.

d'opérations les caractéristiques de l'âge informationnel, le vice-amiral Arthur Cebrowski et John Garstka proposent dès 1998 le concept de Network-Centric Warfare (NCW)[19]. La NCW est un mode de gestion du champ de bataille qui place l'information au cœur de la stratégie et qui suppose le déploiement de moyens techniques et organisationnels pour optimiser sa collecte et son partage. Reprenant l'idée de l'amiral William Owens d'un « système de systèmes[20] », la NCW prône donc une mise en réseau de l'ensemble des entités intervenant dans une opération (décideurs, effecteurs et senseurs) afin de créer un environnement informationnel commun, fiable et substantiel. L'augmentation de la capacité informationnelle des forces doit à son tour permettre l'amélioration de la puissance de combat[21].

Ces concepts américains n'ont pas manqué d'exercer une influence importante au sein des pays alliés des États-Unis. La NCW s'est notamment déclinée dans les années 2000 au Royaume-Uni et au sein de l'Organisation du traité de l'Atlantique nord (OTAN) sous le terme de Network-Enabled Capacity (NEC), en Allemagne en tant que Netzwerkgestützte Operationsführung (NetOpFü), en Suède en tant que Network-Based Defence (NBD), ou encore en Australie sous son nom originel de Network-Centric Warfare. En France, elle a donné lieu au concept d'opération réseau-centrées (ORC), dont les héritages se retrouvent par exemple au sein de l'armée de Terre dans les principes de combat collaboratif et de « bulle opérationnelle aéroterrestre » (BOA).

Les réflexions stratégiques américaines ont beaucoup influencé les forces françaises qui, conscientes de l'importance de maîtriser ces nouvelles technologies, ont entamé leur numérisation dès le début des années 1990, tout en cherchant à se réapproprier les doctrines américaines alors perçues comme un outil de suprématie des États-Unis[22]. Les armées françaises ont d'abord considéré les NTIC comme un adjuvant capacitaire et non comme un changement radical dans la façon de conduire la guerre. C'est ce qui explique que le processus de numérisation des forces a été incrémentiel[23] et n'a été que peu

19. A. Cebrowski et J. Garstka, « Network-Centric Warfare: Its Origins and Future », *Proceedings of the U.S. Naval Institute*, vol. 124, 1998. John Garstka était alors directeur de la technologie (CTO) au sein de la direction des systèmes C4 (*Command, Control, Communications & Computers*) de l'État-major. Lors de la création de l'OFT en 2001, il devient sous-directeur des concepts et des opérations au sein du bureau.

20. W. Owens, « The Emerging U.S. System-of-systems », *INSS Strategic Forum*, n° 63, 1996, p. 1-4.

21. D. Alberts, J. Garstka et F. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, Washington D.C., CCRP, 1999.

22. P. Gros *et al.*, « Du *Network-Centric* à la stabilisation : émergence des 'nouveaux' concepts et innovation militaire », *Études de l'IRSEM*, IRSEM, n° 6, 2010.

23. En informatique, le terme « incrémentiel » désigne l'accroissement de la valeur d'une variable à chaque phase de l'exécution d'un programme. Il signifie ici que la numérisation des

théorisé, à l'exception de l'armée de Terre qui a rapidement avancé le concept de « numérisation de l'espace de bataille » (NEB).

Si la NEB diffère dans certains aspects de sa mise en œuvre du concept américain[24], elle reste bien une déclinaison de la NCW, et les objectifs poursuivis sont les mêmes. Bonne illustration de ce développement incrémentiel, la NEB a connu plusieurs évolutions. Initiée, comme pour les autres armées, dans les années 1990, la numérisation des forces terrestres conduit au développement de divers systèmes (SICF, SIR, SIT[25]) et équipements (FELIN[26], radio PR4G) déployés lors de la phase d'expérimentation, dans les années 2000. Les retours d'expérience mitigés[27] ont néanmoins entraîné, à partir des années 2010, une réorientation des projets et le lancement du programme SCORPION. Ce dernier prévoit le remplacement d'une grande partie des systèmes développés lors de la première phase de la NEB (1990-2010) et l'évolution, voire le remplacement, de nombreux équipements utilisés durant la décennie précédente.

La faible conceptualisation doctrinale dans les autres armées françaises ne signifie pas pour autant que la numérisation n'a pas eu lieu, ainsi que le rappelle l'amiral François Moreau, sous-chef d'état-major chargé des plans et des programmes de l'état-major de la Marine nationale, qui souligne lors de son audition à l'Assemblée nationale en 2018 que « la Marine [...] opère des systèmes numérisés depuis trente ou quarante ans », aussi bien sur les bâtiments que dans l'environnement et le soutien de la flotte[28]. Cette faible « montée en doctrine » peut toutefois être interprétée comme un défaut d'anticipation et comme la conséquence d'un manque de vision stratégique et politique sur le sujet, vision qui se précise depuis trois ans seulement. En effet, bien que le cyber apparaisse dans les deux *Livre blanc de la défense et de la sécurité nationale* de 2008[29] et 2013[30], et dans la *Revue stratégique* de 2017[31], et qu'ait été publiée en

armées s'est déroulée de façon progressive, par adjonctions et adaptations successives de matériels et de logiciels.

24. P. Gros *et al.*, « Du *Network-Centric* à la stabilisation : émergence des "nouveaux" concepts et innovation militaire », *op. cit.* La NEB française adopte, par exemple, « une architecture hiérarchique (niveau tactico-opératif, division, brigade, groupement tactique interarmes...) » alors que l'architecture du modèle américain est, elle, « fonctionnelle (manœuvre, renseignement, logistique...) ».

25. Système d'information pour le commandement des forces (SICF), système d'information régimentaire (SIR), système d'information terminal (SIT).

26. Fantassin à équipement et liaisons intégrés (FELIN).

27. C. Bedez, « De la numérisation de l'espace de bataille à l'info-valorisation : gagner la confiance des utilisateurs tactiques », *Pensées mili-terre*, Centre de doctrine et d'enseignement du commandement, 2018.

28. O. Becht et T. Gassilloud (rapporteurs), *Rapport d'information sur les enjeux de la numérisation des armées*, Rapport n° 996, Paris, Assemblée nationale, mai 2018, p. 215.

29. *Livre blanc de la défense et de la sécurité nationale*, Paris, Ministère de la Défense, 2008.

30. *Livre blanc de la défense et de la sécurité nationale*, Paris, Ministère de la Défense, 2013.

31. *Revue stratégique*, Paris, Secrétariat général à la Défense et à la Sécurité nationale, 2017.

2018 la *Revue stratégique de cyberdéfense*[32], l'intégration des NTIC n'est essentiellement traitée que sous le prisme de la sécurité numérique et de leur usage en situation conflictuelle (lutte informatique défensive et offensive)[33]. Le processus de numérisation des armées en tant que tel, s'il s'est opéré *de facto*, semble donc n'avoir été que peu formalisé dans les réflexions stratégiques avant 2017 (voir schéma n° 2). L'année 2017 est effectivement marquée par la parution du document *Ambition numérique du ministère des Armées*[34] qui expose la démarche ministérielle de « transformation numérique ». Depuis, de nombreuses initiatives ont été entreprises afin d'accélérer la numérisation des forces et semblent faire l'objet de réelles réflexions en amont de leur mise en œuvre, comme en témoigne la mise en place de divers groupes de travail à haut niveau hiérarchique (DGA, DGNUM, EMA, etc.). Le document *Ambition numérique* atteste également d'une perception globale de la numérisation, qui doit se concevoir autant au niveau des différentes armées qu'à l'échelle du ministère dans son ensemble.

Le cloud computing *en réponse aux nouveaux besoins informatiques*

La numérisation des armées suppose l'articulation de deux dynamiques concomitantes : la mise en données et la mise en réseau[35]. La mise en données – également désignée sous le néologisme « datafication[36] » – correspond à la transcription du réel en langage informatique, afin d'en systématiser l'analyse. La mise en réseau consiste en l'établissement de connexions entre les diverses parties prenantes afin d'échanger ces données. Sur les théâtres d'opérations par exemple, cette mise en données et en réseau s'est traduite par une multiplication des capteurs[37] et une plus grande interconnexion entre les décideurs, les effecteurs et les capteurs.

Ces deux dynamiques entraînent logiquement une augmentation des volumes de données produites et échangées sur les différents réseaux. Elles occasionnent également la complexification des SIC,

32. *Revue stratégique de cyberdéfense*, Paris, Secrétariat général à la Défense et à la Sécurité nationale, 2018.
33. A. Dabila, « L'intégration numérique des armées : de l'incorporation tactique à la conjonction stratégique », *Note de recherche*, Institut d'études de stratégie et de défense, mai 2020.
34. *Ambition numérique du ministère des Armées*, Paris, DICoD, novembre 2017.
35. A. Cattaruzza et S. Taillat, « Les enjeux de la numérisation du champ de bataille », *Dynamiques internationales*, n° 13, 2018.
36. V. Mayer-Shönberger et K. Cukier, *Big data. La révolution des données est en marche*, Paris, Robert Laffont, 2014.
37. Un capteur est un dispositif technique qui détecte un signal et le retranscrit. Les capteurs peuvent être thermiques, mécaniques, optiques, chimiques, ioniques… Ils sont les principales sources de données « brutes » à la base des informations circulant sur les SI militaires.

toujours plus nombreux et interconnectés. Or la prolifération des données et la complexification des systèmes posent plusieurs défis et leur gestion devient un enjeu en soi. Le premier défi concerne le stockage, l'exploitation et la discrimination des données collectées et partagées. En 2009 déjà, les drones américains survolant l'Irak et l'Afghanistan ont collecté en un an l'équivalent de 24 années de vidéo[38]. Le système embarqué de surveillance terrestre en temps réel ARGUS de la DARPA collectait lui en 2013 plus de 40 gigabits par seconde[39]. Ces capacités croissent à une vitesse inédite : entre 2001 et 2011, les volumes de données amassées par les drones de surveillance américains auraient augmenté de 1 600 %[40]. Pour gérer ces quantités colossales de données, dont la croissance s'accélère de façon exponentielle, de nouvelles architectures des SI doivent être envisagées afin d'augmenter les capacités de stockage et d'assurer le bon fonctionnement des systèmes en évitant leur saturation. Cette augmentation massive des données manipulées par les personnels de la défense génère également de nouveaux besoins en matière de technologies de traitement de données. Ces dernières peuvent effectivement permettre d'extraire un maximum d'information de ces *big data*, et doivent faciliter la discrimination afin d'éviter que les personnels ne soient submergés.

Le second défi de la numérisation réside dans l'interopérabilité des systèmes. Un système est dit interopérable lorsqu'il est capable de communiquer et de fonctionner avec d'autres systèmes. Cela suppose la compatibilité des standards et des programmes utilisés par ces systèmes. Au sein du ministère des Armées, les SI sont nombreux et très hétérogènes. Afin de les rendre interopérables, un effort de standardisation est donc nécessaire et le développement de plateformes « universelles » communes à plusieurs systèmes pourrait faciliter leur communication et le partage de données.

Enfin, le troisième défi que pose la transformation numérique des forces concerne les compétences nécessaires pour gérer ces nouveaux systèmes et les flux de données y circulant. Avec la démocratisation de l'informatique, de nouveaux métiers sont apparus et portent aussi bien sur les infrastructures informatiques (architectes infrastructures, ingénieurs systèmes et ingénieurs réseaux, techniciens cybersécurité, etc.) que sur les données numériques (développeurs, ingénieurs et architectes data, *data scientists*, etc.). Ces nouvelles fonctions sont indispensables à la bonne marche des

38. S. Graham, « Drone: Robot Imperium », *TNI Working Papers*, Transnational Institute, 2016.
39. N. Couch et B. Robins, « Big Data for Defence and Security », *RUSI Occasional Paper*, RUSI, septembre 2013.
40. T. Shanker et M. Richtel, « In the New Military, Data Overload Can Be Deadly », *The New York Times*, 16 janvier 2011, disponible sur : www.nytimes.com.

systèmes du ministère mais ne représentent pas le cœur de métier de l'organisation et peuvent être difficiles à acquérir.

Initialement développé dans le domaine civil, le *cloud computing* s'est rapidement imposé durant la seconde moitié des années 2000 en réponse à ces nouveaux enjeux et est apparu comme une solution face aux besoins informatiques générés par la numérisation des armées. En effet, le *cloud* est un mode d'organisation des SI qui permet justement d'augmenter les capacités de stockage d'une organisation par la mise à disposition de ressources supplémentaires, et qui facilite la mutualisation des données grâce à leur mise en commun. Il est également un support particulièrement intéressant pour le développement de technologies de traitement de données comme le *big data analytics* ou l'intelligence artificielle, voire un prérequis pour d'autres innovations telles que l'internet des objets (IoT). Le *cloud* permet en outre de confier la gestion des SI à un prestataire, ce qui peut pallier en partie au manque de compétences en interne et soulage les personnels de certaines tâches fastidieuses et accaparantes.

Un tournant socio-technique impulsé par le secteur civil

Continuité technologique, révolution des pratiques

Pour bien saisir les enjeux posés par l'intégration du *cloud* au sein des SIC militaires, il convient de comprendre comment fonctionne la technologie, et ce qui se cache derrière cette dénomination éthérée. Souvent présenté comme une innovation et une technologie de rupture, le *cloud* s'inscrit pourtant dans une continuité technologique. Il bouleverse en revanche profondément les pratiques liées à l'informatique.

Le *cloud computing* est effectivement le produit des évolutions successives de l'informatique depuis l'ordinateur à transistor d'IBM au début des années 1960 jusqu'à nos jours. Il s'appuie sur des technologies et des concepts qui lui préexistent, tels que la virtualisation, le calcul à la demande (*utility computing*), le web (et son évolution 2.0), ou encore l'informatique en grille (*grid computing*)[41]. Son apport majeur consiste en la réunion de ces technologies qu'il fait fonctionner ensemble et dont il adopte les

41. R. Krutz et R. D. Vines, *Cloud Security. A Comprehensive Guide to Secure Cloud Computing*, Idianapolis, Wiley Publishing, 2010.

principales caractéristiques (ressources en libre-service, accès distant, rassemblement des dispositifs, etc.[42]).

Le *cloud* est un modèle d'architecture des SI qui repose sur le principe d'infogérance, c'est-à-dire sur l'externalisation par l'utilisateur de la gestion de ses ressources informatiques (serveurs, logiciels, applications, données…) auprès d'un prestataire. L'utilisateur peut ainsi se délester de l'acquisition et de l'entretien (frais de fonctionnement, mises à jour, etc.) d'une partie des infrastructures, des équipements et des applicatifs nécessaires au fonctionnement de ses systèmes. Le prestataire, appelé fournisseur de services, met alors ses propres ressources, soit ses capacités de stockage et de calcul, à la disposition de l'utilisateur, sur un principe de location. Cela présente de nombreux avantages pour l'utilisateur qui peut théoriquement, en fonction de ses besoins, déployer des capacités de stockage (élasticité horizontale) et de traitement (élasticité verticale) supplémentaires à distance, sur simple demande et de manière quasi instantanée. Cela permet par exemple de faire face à un pic de demandes imprévu tout en maintenant la qualité de service, et sans avoir à investir au préalable dans des dispositifs supplémentaires dont l'usage resterait exceptionnel. L'élasticité technique se double parfois d'une facturation à l'usage qui permet à l'utilisateur de ne payer que pour les ressources réellement utilisées.

Ce fonctionnement contribue à la servicisation de l'informatique, déjà anticipée dans les années 1960 par quelques précurseurs[43] : l'accès aux ressources numériques devient bien un service auquel souscrire, et n'est plus conditionné par la détention en propre des dispositifs. Cette servicisation s'est accompagnée d'une délocalisation des ressources numériques qui ne sont plus hébergées chez l'utilisateur ou dans les locaux d'une organisation, mais au sein de centres de données – ou *data centers*. Ces ressources sont alors accessibles *via* le réseau internet, ou un réseau intranet dans certains cas particuliers. La délocalisation des dispositifs explique que le *cloud* paraisse intangible pour nombre d'utilisateurs qui n'ont en effet besoin que d'un simple terminal et d'une connexion au réseau pour y accéder.

Il existe dans le *cloud* plusieurs niveaux de services, qui constituent autant de degrés d'externalisation. On en distingue généralement trois :

- Le IaaS (Infrastructure as a Service), où le prestataire met à la disposition de son client l'espace de stockage et la puissance de traitement de son infrastructure informatique et se charge uniquement de la gestion des composants de l'infrastructure

42. P. Mell et T. Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, US Department of Commerce, 2011.
43. D. Parkhill, *The Challenge of Computer Utility*, Boston, Addison-Wesley, 1966.

(serveurs, connexions réseau, résilience, bande passante…) ;

- Le PaaS (Platform as a Service), où le prestataire fournit également au client les systèmes d'exploitation et les logiciels de traitement de bases de données lui permettant de développer et/ou de gérer les applications et les outils de son choix sans avoir à se soucier de la mise en place et de la maintenance des plateformes nécessaires à une telle opération ;
- Le SaaS (Software as a Service), où le prestataire gère l'ensemble du dispositif informatique, jusqu'aux applications qu'il héberge lui-même et qu'il rend disponibles pour son client.

Le IaaS est à la base du *cloud* et correspond au niveau minimal d'externalisation auquel un utilisateur peut souscrire. Le PaaS repose ainsi sur le IaaS et, dans une logique d'externalisation croissante, le SaaS est lui-même construit sur le PaaS.

En sus du niveau de services, l'utilisateur peut aussi décider du mode de déploiement du *cloud* qui peut être public, privé, communautaire ou hybride. Dans le cas d'un *cloud* public, les offres de services proposées sont accessibles au grand public, les ressources sont partagées et sont hébergées dans les locaux du fournisseur. Dans le cas d'un *cloud* privé, le client souscrit à un ensemble de services dont il a l'usage exclusif. Le dispositif peut être géré par le client, un tiers ou les deux, sur site ou non. Sur le même principe, un *cloud* communautaire est simplement un *cloud* privé partagé volontairement par plusieurs organisations. Un *cloud* hybride, enfin, est composé de plusieurs environnements *cloud* différents liés par des standards technologiques qui permettent la portabilité des applications et des données.

Le cloud*, outil d'économie et de performance pour les Armées*

Si les évolutions technologiques et l'histoire de leur intégration dans les organisations militaires expliquent le développement du *cloud* défense, s'attarder également sur ses usages potentiels au sein du ministère des Armées permet de comprendre les intérêts qu'il suscite.

En cohérence avec les évolutions doctrinales et à une époque où le concept de guerre en réseau faisait florès, le *cloud* a d'abord été envisagé comme un élément incontournable de l'infrastructure informationnelle de combat – appelée « infostructure » par les théoriciens de la NCW. Il est effectivement un adjuvant dans la maîtrise de l'information, puisqu'il facilite sa mutualisation et fournit des capacités de stockage et de traitement de données permettant d'augmenter quantitativement et qualitativement le niveau d'information. En concourant à la mise à disposition des forces

d'informations riches et mutualisées quasiment en temps réel, le *cloud* apparaît comme un outil de mise en œuvre de la NCW et son utilisation sur les théâtres pourrait, *in fine*, apporter des avantages opérationnels non négligeables. L'augmentation de la capacité informationnelle des forces promise par le *cloud* contribuerait par exemple à une meilleure connaissance du terrain et une plus grande appréciation situationnelle, réduisant de fait l'incertitude et le brouillard de la guerre. Il pourrait également permettre davantage de collaboration et une plus grande capacité d'autonomie des forces, accélérant en principe la boucle OODA (*Observe*, *Orient*, *Decide*, *Act*)[44]. Les opérations gagneraient ainsi en amplitude et les frappes en précision, ce qui garantirait une plus grande efficacité de la mission[45].

Outre son utilisation en combat, le *cloud* présente des intérêts organisationnels indéniables qui, s'ils ne sont pas propres au ministère des Armées, pourraient grandement accélérer sa transformation numérique.

L'utilisation du *cloud* entraîne le rassemblement, au sein de *data centers*, des ressources informatiques *hardware* et *software*. Une fois ces ressources rassemblées, leur gestion peut être :

- **Rationalisée**, le partage des ressources permettant de réduire le nombre d'infrastructures et d'identifier les applicatifs redondants. Cette rationalisation faciliterait également l'évolution du « *legacy*[46] », entraînant ainsi un meilleur fonctionnement de l'ensemble de l'infostructure du ministère.
- **Mutualisée**, la mise en commun des capacités *hardwares* et *softwares* induisant le partage des ressources humaines, matérielles et immatérielles (logiciels, données…), ce qui occasionne d'importantes économies et permet de profiter d'effets d'échelle.
- **Optimisée**, puisque le rassemblement des ressources au sein d'un nombre limité d'infrastructures partagées permet une meilleure supervision du parc informatique. Les besoins sont ainsi mieux identifiés et la sécurité s'en trouve renforcée (automatisation des procédés de sécurité et leur application à grande échelle et en profondeur, meilleure résilience des systèmes grâce à la redondance facilitée par la virtualisation, disparition progressive des équipements obsolètes et mises à jour des logiciels permettant de limiter les risques inhérents).

44. La boucle OODA est un concept décrivant l'enchaînement des processus itératifs permettant la conduite d'une action sur le champ de bataille. Elle a été imaginée par le pilote de chasse américain John Boyd dans les années 1960.
45. « The Implementation of Network-Centric Warfare », Office of Force Transformation, *op. cit.*
46. Le *legacy* désigne l'ensemble des matériels et logiciels obsolètes d'une organisation, qui continuent pourtant d'être employés, essentiellement parce que leur remplacement est coûteux et contraignant.

Le *cloud* est donc également progressivement introduit au niveau du réseau d'entreprise[47] du ministère des Armées. Il semble être un levier pour la numérisation de l'environnement et du soutien des forces, et pourrait contribuer à combler l'écart d'avancement entre la numérisation des systèmes d'armes, « déjà très poussée », et celle des fonctions organiques du ministère, « moins avancée[48] ».

Cette recherche de rationalisation et d'optimisation des SIC s'est traduite au sein du ministère des Armées par le projet INCAS (Infrastructure communicante adaptative sécurisée). Lancé en 2008, INCAS a permis la mise en place de structures d'hébergement mutualisées (SHEM) qui réunissent les données et les SI des divers services du ministère. Cette démarche a permis de diviser par dix le nombre de sites d'hébergement[49]. Elle a pour cible, à l'horizon fin 2021, le maintien de seulement quatre *data centers* principaux (à Suresnes, Bordeaux, Rennes et Toulon), appuyés par une douzaine d'hébergements auxiliaires. L'actualisation du projet en 2016 prévoit de compléter cette rationalisation par le développement d'infrastructures hyperconvergées[50], la virtualisation des réseaux (en plus de celle des machines) et la mise en place d'une plateforme de services – autant d'éléments qui confirment que le projet INCAS constitue une première étape dans la construction du *cloud* défense[51].

Enfin, l'élasticité technique du *cloud* et la possibilité qu'il offre de recourir à des compétences externes apportent une grande flexibilité au ministère des Armées dans la gestion de ses SI. Cette flexibilité, conjuguée aux usages et aux avantages précédemment identifiés, est porteuse d'efficacité et de productivité[52], et semble être un gage de performance et d'économie supplémentaire.

Une technologie civile dans les SI militaires

Bien que le *cloud* semble être une solution particulièrement avantageuse pour le ministère des Armées, il n'a pas été conçu pour ce

47. En informatique, un réseau d'entreprise désigne le réseau interne à une organisation. Dans le cas du ministère des Armées, l'expression comprend les équipements utilisés en métropole et dans les DROM-COM.
48. O. Becht et T. Gassilloud, *Rapport d'information sur les enjeux de la numérisation des armées*, *op. cit.*
49. Entretien avec un ingénieur de la DIRISI, novembre 2018.
50. L'« infrastructure hyperconvergée » est une infrastructure informatique dont la gestion est facilitée grâce au rassemblement des fonctions de traitement, de stockage, de mise en réseau ou de virtualisation sur une plateforme prête à l'emploi.
51. « Stratégie du système d'information de l'État : Synthèse des contrats de progrès ministériels 2013-2015 », Direction interministérielle des systèmes d'information et de communication (DISIC), décembre 2013.
52. O. Becht et T. Gassilloud, *Rapport d'information sur les enjeux de la numérisation des armées*, *op. cit.*

type d'organisation. Comme la majorité des récentes innovations dans le domaine numérique, le *cloud* a initialement été développé par le secteur civil pour répondre à des besoins sociétaux. En effet, les problèmes de massification des données et de complexification des SIC rencontrés par les organisations de défense l'ont également été par la société civile, qui a su y faire face plus rapidement. Les premières solutions *cloud* sont apparues durant la seconde moitié des années 2000, et se destinaient essentiellement à des entreprises. En une décennie à peine, l'informatique en nuage s'est démocratisée et est utilisée aujourd'hui par la quasi-totalité des internautes, généralement au travers d'applicatifs (niveau SaaS) tels que des messageries électroniques (Gmail, Outlook, Thunderbird…), des outils de bureautique en ligne (Google doc, Framapad…), des plateformes collaboratives (Slack, Teams…), etc.

Le *cloud* est emblématique de cette nouvelle dynamique d'innovation selon laquelle ce n'est plus le secteur militaire qui entreprend le développement de nouveaux équipements qui irriguent finalement le monde civil, mais bien le secteur civil qui est à l'origine de l'émergence de nouvelles technologies ensuite intégrées à l'organisation militaire.

Cette inversion du sens de l'innovation a plusieurs conséquences. D'abord, elle occasionne l'émergence de nouveaux acteurs privés qui, dans le cas du numérique et du spatial, sont devenus extrêmement puissants et concurrencent largement les programmes étatiques[53]. Dans le secteur du *cloud*, on peut notamment citer les américains Amazon (AWS), Google, Microsoft, IBM, Cisco ou encore Salesforce, et les chinois Alibaba et Huawei. Ensuite, cette nouvelle dynamique a causé une diminution de l'implication et du soutien du ministère dans le développement des innovations technologiques « au motif que ces technologies étaient financées par le secteur civil[54] ». Or, les technologies civiles ne sont pas forcément compatibles avec les équipements militaires et les modes de fonctionnement de l'organisation. L'adaptation *a posteriori* de ces technologies aux besoins du ministère peut en outre être compliquée par les différences culturelles importantes entre les entreprises du numérique, « agiles » et fonctionnant sur des cycles courts, et le monde militaire, hiérarchique et bureaucratique. Tous ces éléments ont conduit, enfin, à une intégration relativement tardive et disparate du *cloud* dans les SIC militaires, comme ce fut le cas aux États-Unis, voire à une omission stratégique, comme évoqué précédemment pour la France.

53. C. Perrin et J.-N. Guérini (rapporteurs), *Rapport d'information fait au nom de la commission des Affaires étrangères, de la Défense et des forces armées par le groupe de travail sur l'innovation et la défense*, Rapport n° 655, Paris, Sénat, juillet 2019.
54. O. Becht et T. Gassilloud, *Rapport d'information sur les enjeux de la numérisation des armées*, *op. cit.*

Construire une stratégie *cloud* pour le ministère des Armées

L'entrée discrète du cloud *dans la transformation numérique*

À la fin des années 1980, les trois armées entrent dans la numérisation et se dotent de systèmes propres qu'elles conçoivent et exploitent de façon autonome[55]. Ce développement parallèle des systèmes pose de sérieux problèmes d'interopérabilité. C'est pourquoi le ministère lance durant la décennie 1990-2000 divers projets pour faciliter la communication entre armées et coordonner les SIC au niveau ministériel, dont le programme *Socrate* initié en 1991, et la création du Directoire des SIC en 1998[56]. Ces initiatives, empêchées par les divergences culturelles et la diversité des matériels, tardent néanmoins à porter leurs fruits. Inspiré par l'expérience britannique, le ministère envisage alors d'externaliser certaines tâches. Ce sont cependant les difficultés liées à l'externalisation qui sont mises en exergue dans les conclusions des études préliminaires, et le choix est fait d'y renoncer, même s'il est aujourd'hui admis que ces blocages étaient avant tout culturels et liés à l'*habitus* militaire.

Émerge alors l'idée de créer une organisation qui jouerait le rôle d'opérateur unique et interarmées pour le ministère. Elle est concrétisée en 2003 avec la création de la Direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI), confirmant par la même occasion l'institutionnalisation progressive de la numérisation des armées françaises. Si sa création a soulevé quelques réticences au sein des armées, la DIRISI s'est progressivement imposée, passant d'un effectif de 300 personnes en 2003 à plus de 7 000 en 2015. Ses missions se sont également précisées, au prix de nombreux chantiers et plans de transformation. Actuellement, elles portent aussi bien sur la gestion des réseaux et des infrastructures numériques du ministère en métropole et en opérations, que sur la sécurité des SI, et sur l'achat de services, de matériels et de logiciels. C'est donc naturellement que la DIRISI est apparue comme un acteur essentiel de la construction du *cloud* défense.

Du fait de ses nombreuses promesses, le *cloud* a été identifié dès 2010 comme une cible à atteindre pour l'architecture des SIC du ministère. L'élaboration d'un *cloud* défense a alors constitué l'un des principaux axes du projet « Dirisix » de transformation de la DIRISI.

55. Direction des réseaux d'infrastructure et des systèmes d'information, *Une aventure humaine : au cœur des opérations et de la vie de la défense*, 2014.
56. *Ibid.*, p. 11. En 1998, le Directoire des SIC « rassembl[ait] l'EMA, la DGA et le SGA, responsables respectivement des systèmes d'information opérationnels et de communication (SIOC), des systèmes de l'informatique scientifique et technique (SIST), des systèmes d'information d'administration et de gestion (SIAG). »

Le directeur central de la DIRISI, le général de corps d'armée Patrick Bazin, affirme rétrospectivement que « l'adoption [du nuage informatique] était inéluctable » mais admet qu'elle « s'appuy[ait] sur des ruptures technologiques encore en devenir[57] ». Ce n'est donc qu'en 2014, au travers du projet INCAS, que les premières infrastructures du futur « *cloud* défense » ont été inaugurées. À l'image de la « transformation » du DoD américain, le ministère des Armées entamait alors sa modernisation.

Cette démarche s'accélère à partir de 2017 lorsque la ministre des Armées Florence Parly inscrit la transformation numérique du ministère dans la Loi de programmation militaire 2019-2025, et la formalise dans le document *Ambition numérique du ministère des Armées*[58]. L'objectif de cette transformation est triple. Elle doit garantir la supériorité opérationnelle et la maîtrise de l'information sur les théâtres d'opérations, renforcer l'efficience des soutiens et faciliter le quotidien du personnel, et améliorer la relation au citoyen et l'attractivité du ministère. Si les potentiels apports du *cloud* pour mener à bien cette transformation paraissent aujourd'hui évidents, ils ne sont encore que timidement identifiés en 2017. L'importance de l'informatique en nuage est reconnue mais reste mal comprise puisqu'elle ne semble être considérée que comme une technologie supplémentaire à maîtriser, au même titre que l'intelligence artificielle (IA), le *big data* ou l'internet des objets. Le fait que le *cloud* soit à la base du socle numérique en train de se mettre en place et qu'il soit un préalable au développement d'autres innovations technologiques est néanmoins suggéré dans le document officiel[59]. Pour les opérateurs du ministère des Armées, le *cloud* semble toujours, en 2017, se limiter à ses capacités d'hébergement, même si une volonté de se tourner davantage vers des offres de service élargies est exprimée[60].

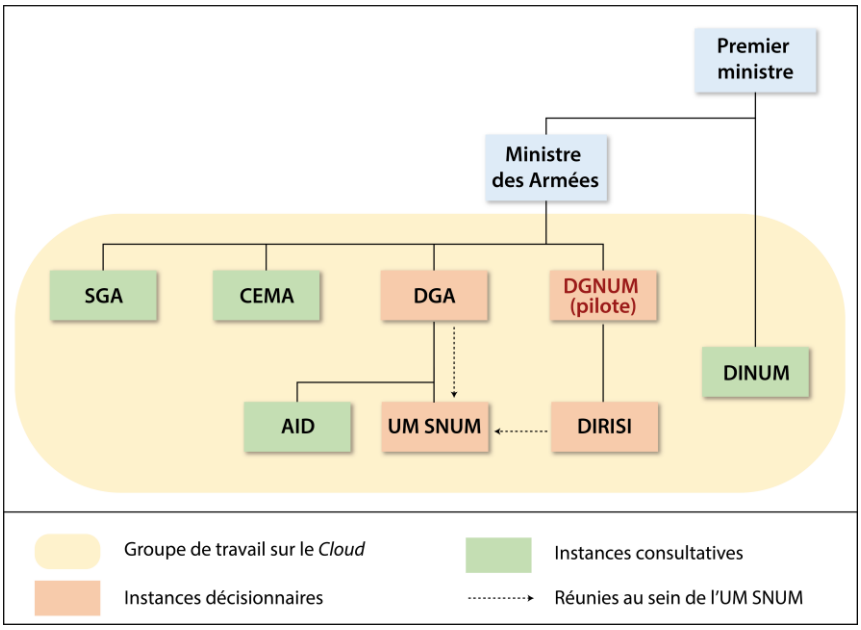
Vers un cloud *défense français ?*

Les représentations que les différents acteurs ont du *cloud* évoluent significativement fin 2018[61], lorsque paraît la première stratégie nationale sur le *cloud*[62]. Prenant la forme d'une doctrine d'utilisation,

57. Direction des réseaux d'infrastructure et des systèmes d'information, *Une aventure humaine : au cœur des opérations et de la vie de la défense*, *op. cit.*, p. 35.
58. *Ambition numérique du ministère des Armées*, *op. cit.*
59. *Ambition numérique du ministère des Armées*, *op. cit.*
60. Allocution du GCA Blaire, Directeur central de la DIRISI, à l'occasion de la Saint-Gabriel au Fort du Kremlin-Bicêtre, le 6 octobre 2017.
61. Sur la question des représentations, voir C. Bômont, « Le poids des représentations dans la construction du *cloud* défense », *in* A. Aglan, Y. Richard et P. Vermeren (dir.), *Guerre de près et de loin*, Paris, Éditions de la Sorbonne, à paraître.
62. Circulaire du Premier Ministre n° 6049/SG du 8 novembre 2018, portant sur la Doctrine d'utilisation de l'informatique en nuage par l'État.

cette stratégie ne s'adresse dans un premier temps qu'aux services de l'État et reste succincte puisqu'elle n'est déclinée que sur trois pages. Elle n'en est pas moins ambitieuse puisqu'elle vise à « développer massivement l'utilisation de l'informatique en nuage au sein de l'administration et à terme à en faire le principe par défaut ». Impulsée par le cabinet du Premier ministre, cette stratégie s'inscrit dans la démarche interministérielle de transformation numérique initiée un an plus tôt dans le cadre du plan « Action Publique 2022 », et dans laquelle est impliqué le ministère des Armées. Un groupe de travail sur l'informatique en nuage est alors mandaté par la ministre des Armées pour réfléchir à la déclinaison de cette doctrine au sein du ministère. Ce groupe est piloté par la Direction générale du numérique et des systèmes d'information et de communication (DGNUM)[63]. Créée en juin 2018, la DGNUM remplace la DGSIC, qui avait elle-même succédé en 2006 au secrétariat du Directoire des SIC, et étend son champ d'action. La DGNUM a pour mission « d'assurer la cohérence globale des [SIC] du ministère [...] et d'améliorer les conditions dans lesquelles sont conduits les projets[64] ». Directement rattachée à la ministre, elle orchestre la transformation numérique du ministère et est en charge de la gouvernance des divers chantiers y concourant.

Schéma n° 1 : Organigramme du groupe de travail sur le *cloud* au ministère des Armées



Source : Clotilde Bômont, réalisation : Clotilde Bômont et Guilhem Marotte, 2021.

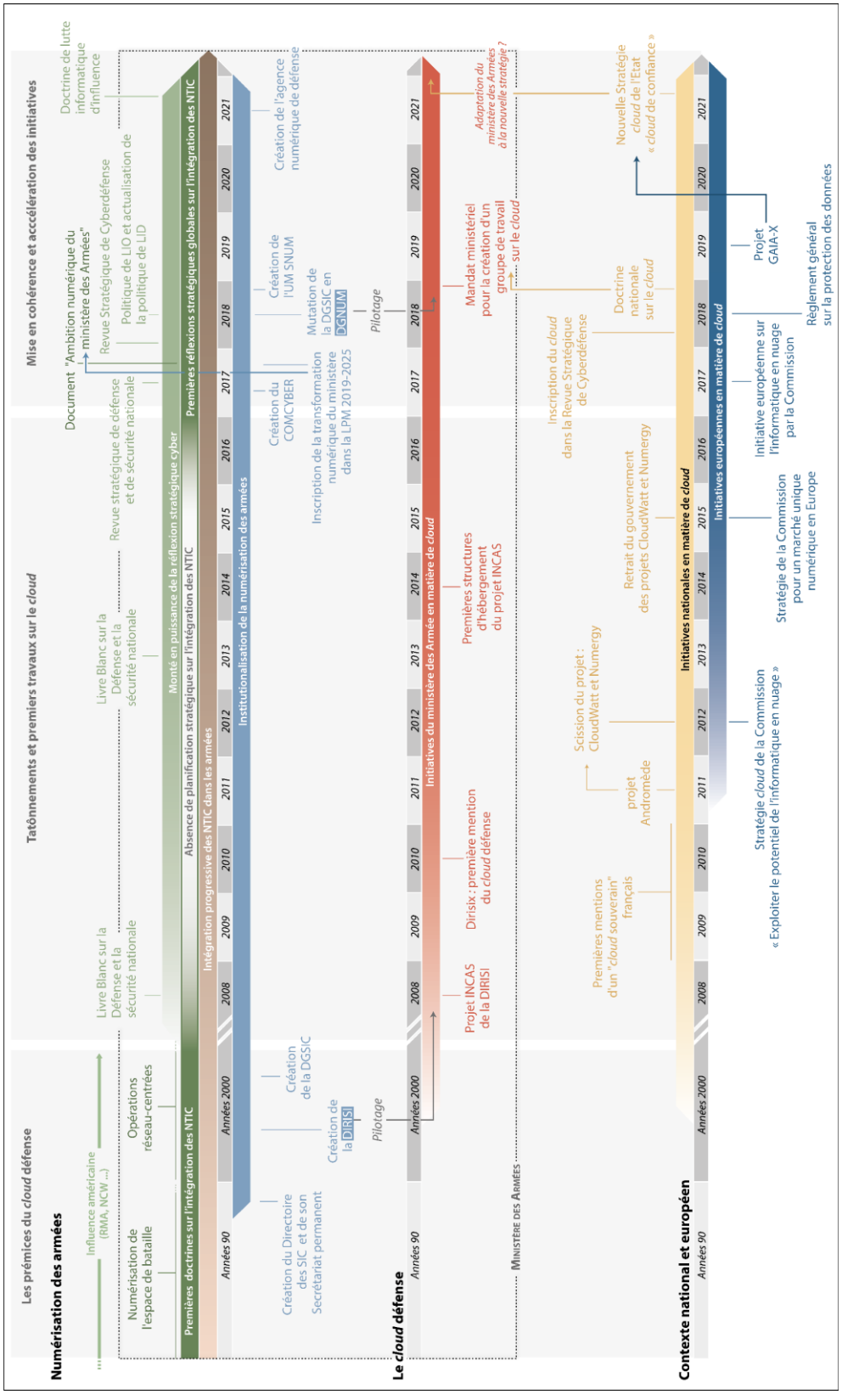
63. La DGNUM, créée au premier semestre 2018, remplace la DGSIC et étend son champ d'action.
64. Ministère des Armées, *Orchestrer la transformation numérique du ministère des Armées*, *op. cit.*

Dans ses travaux sur le *cloud*, elle est appuyée par la Direction générale de l'armement (DGA) et la DIRISI, réunies au sein d'une unité de management mixte, l'Unité de management du socle numérique (UM SNUM). Les travaux sont conduits en consultation avec l'état-major des armées (EMA), le Secrétariat général pour l'administration (SGA), l'Agence d'innovation de la défense (AID) et la Direction interministérielle du numérique (DINUM)[65] (voir schéma n° 1). Cette dernière veille à l'harmonisation des démarches conduites au sein des différents services de l'État. Les chantiers initiés dans le cadre de ce groupe de travail sont pour beaucoup toujours en cours[66].

La conduite des projets *cloud* du ministère des Armées se voit cependant bouleversée par l'annonce de la nouvelle stratégie « *cloud* » de l'État le 17 mai 2021[67] (voir schéma n° 2). Présentée comme la « mise à jour de la doctrine [de 2018][68] », cette nouvelle stratégie nationale, appelée « doctrine '*cloud* au centre'[69] », poursuit l'effort de transition de l'administration vers le *cloud* et se veut davantage en cohérence avec les projets menés au niveau européen, dont GAIA-X, et avec l'écosystème industriel national (soutien aux « projets industriels de développement de technologies[70] »). Elle apporte tout de même de profonds changements puisqu'elle prévoit le développement d'un *cloud* commun à l'ensemble de l'administration française, en lieu et place de solutions ministérielles harmonisées. Aussi, même si elle semble insister davantage sur les bonnes pratiques à adopter que sur les aspects techniques, son impact sur les démarches entamées par le ministère des Armées est encore incertain. Elle pourrait le contraindre à revoir sa copie, alors même que les premières réflexions commençaient à se formaliser et les chantiers à être lancés.

65. En 2018, la DINUM portait encore le nom de DINSIC. Elle devient officiellement la DINUM en octobre 2019.
66. Déclaration de Madame Florence Parly, ministre des Armées, sur le numérique au sein du ministère des Armées, à Bordeaux le 29 avril 2021.
67. *Stratégie nationale pour le* cloud, Dossier de presse, Paris, mai 2021, disponible sur : www.numerique.gouv.com.
68. A. de Montchalin, ministre de la Transformation et de la Fonction publiques, lors de la présentation de la stratégie nationale pour le *cloud*, à Paris le 17 mai 2021.
69. Circulaire du Premier Ministre n° 6282/SG du 5 juillet 2021, portant sur la Doctrine d'utilisation de l'informatique en nuage par l'État (« *cloud* au centre »).
70. *Stratégie nationale pour le* cloud, mai 2021, *op. cit.*

Schéma n° 2 : Le *cloud* défense français, un développement erratique



Source : Clotilde Bômont, réalisation : Clotilde Bômont et Guilhem Marotte, 2021.

L'intégration du *cloud computing* dans les systèmes du ministère des Armées paraît aujourd'hui bien amorcée. Il aura néanmoins fallu une dizaine d'années avant que ne soit mise en place une réelle stratégie en matière de *cloud*, et sa réalisation effective pourrait encore prendre plusieurs années. Elle dépendra de l'évolution des positionnements politiques français sur le sujet, mais aussi de la capacité du ministère à adapter la technologie à ses spécificités et à surmonter les enjeux internes (ressources humaines, cultures antagonistes, exigences sécuritaires, *legacy*, etc.) et externes (partenaires industriels, souveraineté) que pose son intégration.

Adapter le *cloud* aux spécificités du ministère des Armées

La migration d'une architecture informatique vers le *cloud* suppose une adaptation des équipements, de l'organisation des ressources numériques et des pratiques. Pour comprendre le bouleversement que peut représenter le *cloud*, le cas du ministère des Armées est intéressant à plusieurs égards. Ce dernier est effectivement confronté à des problèmes structurels et culturels que rencontrent également la plupart des administrations, voire certaines entreprises, cherchant à migrer vers le *cloud*. Comprendre les enjeux qui se posent au sein de ce ministère permet ainsi de les appréhender dans d'autres organismes. Parallèlement, le ministère des Armées présente des spécificités qui exacerbent ces enjeux (sensibilité des données, diversité des personnels, fonction combattante), et dont la prise en compte conditionne la réalisation même du *cloud* défense.

La sensibilité des données à l'épreuve du *cloud*

Les trois piliers de la sécurité informatique

Le ministère des Armées héberge, produit et manipule des informations dont la sensibilité peut être très élevée. Son infrastructure informatique doit donc être particulièrement sécurisée et robuste, afin d'assurer la confidentialité, l'intégrité et la disponibilité des données, qui sont les trois piliers de la sécurité informatique.

La confidentialité permet de garantir que les données ne sont accessibles qu'aux individus ou appareils autorisés. Elle peut être renforcée grâce à des mesures techniques (comme le chiffrement) ou organisationnelles (comme l'authentification). Au niveau stratégique comme aux niveaux opérationnel ou tactique, la rupture de cette confidentialité peut être lourde de conséquences, d'autant qu'il est souvent difficile de s'apercevoir de l'existence d'une brèche. Pendant la Seconde Guerre mondiale par exemple, le décryptage par les Alliés des messages codés par la machine allemande Enigma a joué un rôle important dans l'issue du conflit et est à ce titre considéré comme le

premier grand succès de la cryptanalyse. Plus récemment, les révélations d'Edward Snowden et de Julian Assange ont montré à la fois l'étendue des pratiques de certaines agences de renseignement et les conséquences politiques de la publication d'éléments classifiés.

En informatique, l'intégrité est un principe permettant d'assurer qu'une donnée n'est pas altérée, que cette altération soit volontaire ou accidentelle. Cela signifie que la donnée reste identique et entière durant tout son cycle de vie, ce qui garantit sa fiabilité. Il faut y ajouter le principe d'authenticité, qui permet de confirmer qu'une donnée émane d'une source reconnue et autorisée. L'altération de l'intégrité des données peut par exemple être utilisée dans le cas de manœuvres de déception. La modification, même infime, ou l'ajout de données peuvent alors falsifier l'information transmise. Il est aisé d'imaginer les conséquences dramatiques qu'une telle manipulation peut avoir sur un champ de bataille[71]. Le cas des systèmes d'armes létales autonomes (SALA) illustre bien l'importance de l'intégrité des données. Si de tels systèmes venaient à être déployés, la corruption des flux d'informations leur parvenant pourrait être un moyen de les détourner de leur objectif afin de servir un autre but. De manière plus insidieuse, l'exemple du ver informatique Stuxnet montre comment, en corrompant seulement l'intégrité de certaines données choisies, les États-Unis et Israël ont ralenti le programme nucléaire iranien. Stuxnet est un *malware* qui s'est attaqué aux systèmes de contrôle et d'acquisition des données (SCADA) de la centrale de Natanz en charge de la régulation de la vitesse des centrifugeuses, ce qui a entraîné un dysfonctionnement des turbines et a ainsi causé des dommages matériels au sein de la centrale.

La disponibilité, enfin, permet de garantir l'accessibilité d'une donnée en un temps limité. Elle suppose d'œuvrer à la résilience des systèmes d'information et de prévenir la destruction des données[72], en prévoyant par exemple leur redondance et en protégeant les réseaux permettant de les acheminer afin de maintenir une bonne connectivité. L'indisponibilité des données entrave l'action ; elle pourrait par exemple empêcher la synchronisation des unités, ou l'achèvement d'une mission. Relativement faciles à mettre en œuvre et produisant des effets très contraignants, les attaques informatiques restreignant l'accès aux données sont de plus en plus courantes et prennent souvent la forme de déni de service distribué (DDoS) et de rançongiciels (*ransomwares*).

71. L. de Rochegonde et É. Tenenbaum, « Cyber-influence : les nouveaux enjeux de la lutte informationnelle », *Focus stratégique*, n° 104, Ifri, mars 2021.
72. Les données peuvent être détruites logiquement, par une manœuvre informatique, ou physiquement, à la suite de l'endommagement – volontaire ou non – des infrastructures les hébergeant. Plusieurs entreprises ont ainsi définitivement perdu certaines de leurs données lors de l'incendie de l'un des *data centers* de l'entreprise OVHcloud en mars 2021.

Pendant longtemps, la sécurité informatique a été envisagée de façon périmétrique, c'est-à-dire en concentrant les protections autour des SI, sur un modèle dit « de château fort[73] ». Cette vision de la cybersécurité semble aujourd'hui obsolète à divers titres[74] : il devient difficile de délimiter le périmètre des systèmes, ces derniers ont une plus grande porosité, et les attaques sont de plus en plus sophistiquées. Du fait de sa nature ubiquitaire, le *cloud* achève de montrer les limites de l'approche périmétrique et suppose une adaptation des règles de sécurité. C'est l'une des raisons pour lesquelles il est parfois pointé du doigt par certains personnels du ministère des Armées, qui le jugent inadapté à l'infostructure militaire parce qu'insuffisamment sécurisé. Si ces craintes doivent être relativisées, la migration vers le *cloud* ne doit évidemment pas déroger aux trois principes de disponibilité, d'intégrité et de confidentialité des données. Elle implique de tenir compte de la classification des informations et de correctement définir les modalités de l'externalisation.

Traduire la sensibilité des données dans le cloud

Suite à la révision, en juillet 2021, de l'instruction générale interministérielle sur la protection du secret de la défense et de la sécurité nationale n° 1300 (IGI 1300), il existe actuellement deux niveaux de classification, « secret » et « très secret », auxquels s'ajoutent diverses mentions permettant d'indiquer une sensibilité particulière : « spécial France », des spécifications – « confidentiel médical », « confidentiel industrie »… – et « diffusion restreinte » pour les documents non classifiés. Ces classifications portent sur des informations « dont la divulgation […], l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités[75] » du ministère des Armées. L'avènement du numérique soulève néanmoins quelques interrogations quant à la notion « d'informations ».

S'il est facile de décider du niveau de classification d'un document, cela s'avère beaucoup plus complexe pour les données numériques. Les données sont la forme la plus élémentaire de l'information ; elles sont des éléments de description d'une réalité (un objet, un événement, un phénomène, etc.) et c'est leur agrégation qui permet la création d'informations. Ces données se caractérisent par

73. C. Leuprecht, D. Skillicorn et V. Tait, « Beyond the Castle Model of Cyber-Risk and Cyber-Security », *Government Information Quaterly*, vol. 33, n° 2, 2016, p. 250-257.
74. *Revue stratégique de cyberdéfense*, SGDSN, Paris, février 2018.
75. Instruction ministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015, relative à la protection des systèmes d'information sensibles.

leur nature (métadonnées, données brutes, données issues de traitements…), leur source (senseurs, sources ouvertes…) et par leurs usages (organique/administratif, technique/fonctionnel et opérationnel). Une donnée en elle-même peut donc ne pas être sensible, mais le recoupement de données en apparence anodines peut permettre d'obtenir des informations beaucoup plus critiques. Prenons l'exemple d'un militaire qui commande de nouvelles bottes de combat sur la plateforme *e-Habillement*, qui est excusé à une réunion suite à une convocation médicale, qui est renseigné sur l'Annudef comme ingénieur infrastructure au sein de la DIRISI et dont les horaires de publication sur Twitter changent subitement dans les jours suivants. Si ces éléments considérés isolément ne présentent pas une grande sensibilité, leur recoupement peut indiquer qu'une opération est probablement en cours de préparation – le déploiement des infrastructures SIC ayant souvent lieu en amont des opérations – et des hypothèses peuvent être émises sur la zone géographique en déterminant le fuseau horaire grâce aux tweets.

La mise en place du *cloud* suppose donc de repenser les systèmes de classification « à l'aune des nouvelles technologies[76] ». Le récent travail de refonte du système de classification devrait conduire à la simplification des différents niveaux et ainsi faciliter leur prise en compte.

La confidentialité et la criticité des données ne pouvant ainsi être évaluées directement, leur sensibilité est déterminée en fonction du SI sur lequel elles reposent. La classification des SI dépend, quant à elle, des réseaux qui les supportent (Intraced, Intradef, Internet, FROPS…). Ces niveaux de classification doivent être retrouvés dans les différentes solutions *cloud* à la disposition du ministère.

La question de la classification amène celle de l'externalisation et du recours à des fournisseurs de services *cloud* extérieurs. Sans même encore aborder l'enjeu du choix des fournisseurs, la migration vers le *cloud* suppose de repenser l'organisation des SI et de distinguer les tâches qui peuvent être externalisées de celles qui doivent être maintenues en interne. Parce qu'elle suppose l'implication d'opérateurs autres que la DIRISI, la transition vers le *cloud* va à l'encontre d'une tendance forte au sein du ministère. Les réticences relatives à l'externalisation des télécommunications et de la gestion de l'infostructure sont effectivement nombreuses et anciennes puisqu'elles ont notamment conduit à la création de la DIRISI[77]. En 2011, le piratage des réseaux de l'entreprise Lockheed Martin, premier industriel de défense américain, a conforté la position des détracteurs de la sous-traitance en révélant l'étendue des

76. C. Villani, *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, Mission parlementaire, Paris, mars 2018.
77. DIRISI, *Une aventure humaine*, *op. cit.*

vulnérabilités auxquelles sont exposés les SI militaires. L'industriel s'occupait de l'électronique de nombreux armements américains comme les missiles *Trident* ou les chasseurs F-35, et gérait également plusieurs réseaux satellitaires au profit du DoD. Cette attaque s'est soldée par un échec mais sa complexité et sa subtilité ont surpris, et elle a mis en exergue l'importance d'étendre les questions de sécurité dans le *cloud* à l'ensemble des acteurs de la base industrielle et technologique de défense (BITD).

Les modalités de déploiement du *cloud* défense devront donc répondre à ces contraintes. Les premières réflexions du ministère des Armées, en cohérence avec la doctrine de 2018[78], se sont portées sur l'articulation entre deux solutions de *cloud* privé – appelées cercle 1 – et une solution dite de *cloud* dédié – appelée cercle 2. Les solutions privées avaient vocation à recevoir les SI classifiés, ou de criticité élevée dans le cas par exemple d'un soutien direct aux opérations. Les données devaient être hébergées dans les *data centers* du ministère des Armées, et l'exploitation devait être assurée par les personnels du ministère, suppléés en métropole par un prestataire extérieur. La solution dédiée prévoyait un hébergement et une gestion davantage externalisés.

Cette organisation a toutefois été entièrement revue avec l'annonce de la nouvelle stratégie « *cloud* » de l'État du 17 mai 2021. Le cercle 2 sur lequel travaillait particulièrement le ministère des Armées n'existe plus, et le cercle 1 évolue en un *cloud* interministériel. Comme son nom l'indique, ce dernier a vocation à être utilisé de façon conjointe par l'ensemble des ministères français qui devront renoncer à disposer d'infrastructures *cloud* en propre. Les besoins des administrations non couverts par le *cloud* interministériel pourront l'être au travers d'offres labellisées. D'après les premières communications, il semble qu'une exception soit faite pour le ministère des Armées qui pourra conserver des infrastructures en interne, en raison de la criticité de ses données et des exigences particulières liées à sa fonction combattante.

Comprendre la diversité des personnels

Afin de mener à bien la construction du *cloud* défense, il est également nécessaire de prendre en compte le facteur humain, trop souvent écarté dans le contexte d'innovations technologiques. Un outil, numérique ou non, ne sera jamais pleinement intégré si les utilisateurs ne perçoivent pas son utilité, vivent son utilisation comme une contrainte, ou ne lui

78. La doctrine de 2018 prévoyait trois types de *cloud*, appelés « cercles », qui correspondaient à différents niveaux de sensibilité des données. Les données les plus sensibles devaient être hébergées sur le cercle 1, les données moins sensibles, sur le cercle 3.

font pas confiance[79]. Il convient donc de comprendre l'environnement social dans lequel est développé le *cloud*, et d'admettre que les changements de pratiques (délocalisation et servicisation), ainsi que la refonte de l'architecture des SI qu'il implique constituent un bouleversement important pour les personnels du ministère.

Des besoins et des attentes variés

Le ministère des Armées se caractérise par la grande diversité des personnels qu'il emploie. Cette diversité est d'abord le fait des nombreux métiers représentés : le ministère compte environ 270 000 agents civils et militaires qui exercent plus de 200 métiers différents dans des secteurs aussi variés que la santé, l'hôtellerie restauration, la formation et l'enseignement, la conduite des opérations et la préparation des forces, l'habillement[80]… Les évolutions de l'infostructure ministérielle doivent tenir compte de cette variété pour répondre au mieux aux différents besoins des personnels. Au niveau des directions de systèmes d'information (DSI) des métiers[81], les besoins convergent néanmoins et sont similaires à ceux que l'on retrouve dans toute organisation ayant entamé sa transformation numérique, tels que la recherche d'agilité et de réactivité. Les divergences se traduiront surtout au niveau des types de *cloud* utilisés – privé ; interministériel – et au niveau des applicatifs.

Les attentes et les représentations vis-à-vis du *cloud* peuvent également varier en fonction des métiers et du rôle joué dans la migration vers l'informatique en nuage. Les perceptions diffèrent selon que l'on se place du point de vue des décideurs tels que la DGNUM, la ministre des Armées ou le Premier ministre ; des opérateurs tels que la DIRISI, la DGA ou les partenaires industriels ; ou des futurs utilisateurs, soit l'ensemble des directions et du personnel du ministère des Armées. Aussi les décideurs semblent-ils envisager le *cloud* comme un gage de modernité et un atout, alors que les utilisateurs, plus partagés quant aux apports de la technologie, expriment une inquiétude face aux potentielles difficultés liées à la transition. Les concepteurs et les opérateurs, eux, voient le *cloud* comme une opportunité de modernisation et un gain d'efficacité et de facilité, mais aussi comme un bouleversement important, qui

79. A. Cattaruzza et S. Taillat, « Les enjeux de la numérisation du champ de bataille », *op. cit.*
80. Direction générale du numérique et des systèmes d'information et de communication, *La Transformation numérique du ministère des Armées. Concepts clés*, Paris, Défense Connect, 2020.
81. « Les "métiers" correspondent à l'ensemble des entités du ministère hors fonctions SIC. », *Schéma directeur de la Transformation numérique. Volet Stratégique*, Paris, Défense Connect, 2018.

nécessite une adaptation des personnels et implique une charge de travail supplémentaire alors que les effectifs sont limités[82].

Des cultures numériques différentes

Ces différentes attentes s'expliquent également par l'hétérogénéité des profils au sein du ministère des Armées. Les agents du ministère présentent une grande diversité d'âges, de niveaux hiérarchiques et de connaissances des outils informatiques. Tous les personnels n'ont donc pas la même culture numérique, ce qui peut expliquer d'éventuelles difficultés d'intégration du *cloud* au sein de l'organisation. Les personnels les plus jeunes, par exemple, ressentent une certaine frustration face au manque de réactivité des outils numériques qu'ils comparent à ceux qu'ils connaissent dans le domaine civil. Parallèlement, les agents maîtrisant mal les nouveaux outils informatiques ont tendance à se méfier de la technologie et à s'en détourner[83]. Afin de s'assurer que tous les agents disposent d'un minimum de compétences numériques, plusieurs projets de formation ont été mis en place, à l'image du « Passeport numérique » et de « l'Académie du numérique » portés par la DGNUM, le SGA et la DRH-MD.

Recruter dans les fonctions SIC

Enfin, l'un des plus grands défis auquel est confronté le ministère des Armées est la difficulté de recrutement dans les fonctions SIC. Alors que les besoins en ressources humaines croissent tous les ans, le ministère peine à recruter et à fidéliser les agents. Cette difficulté vient essentiellement du manque d'attractivité de la fonction publique par rapport aux entreprises du secteur numérique qui emploient des profils analogues mais proposent de meilleures rémunérations et des outils plus innovants. La DIRISI est l'organisme qui pâtit le plus de ce manque de compétitivité, avec une érosion constante de ses effectifs depuis une dizaine d'années, avec près de 20 % de pertes sur la période 2008-2018[84]. Or si l'infogérance permet de soulager les personnels de certaines tâches, le développement du *cloud* défense requiert néanmoins la mobilisation de ressources humaines supplémentaires et suppose l'acquisition de nouvelles compétences. Si le ministère des Armées travaille actuellement sur ces questions, avec notamment une revalorisation de sa grille salariale, d'importants efforts seront

82. Enquête réalisée entre octobre 2018 et juin 2019. Voir C. Bômont, « Le poids des représentations dans la construction du *cloud* défense », *op. cit.*
83. Entretien avec un agent RH de la DIRISI, janvier 2020.
84. DIRISI, *Plan de modernisation. Volet stratégique*, Paris, août 2018.

encore nécessaires pour parvenir à un effectif et un niveau de compétences optimaux.

Le développement du *cloud* tactique

Si le ministère des Armées partage la question de la sensibilité des données et de la diversité de ses agents avec d'autres services étatiques, la fonction combattante lui est propre. Le *cloud* pouvant contribuer à la capacité informationnelle des forces, il est voué à intégrer l'infostructure de combat. Utilisé en opérations, il est appelé « *cloud* tactique », « *cloud* de combat » ou « *cloud* de théâtre », et présente certaines spécificités, tant dans son déploiement que dans ses usages.

Qu'est-ce qu'un cloud *tactique ?*

Pour définir ce qu'est le *cloud* tactique, il convient dans un premier temps d'établir ce qu'il n'est pas, techniquement comme conceptuellement. Contrairement aux solutions « traditionnelles » qui promeuvent l'infogérance, la virtualisation et la rationalisation, le *cloud* tactique a pour principale fonction de faciliter l'accès à l'information et la communication sur les théâtres. Une distinction doit donc être opérée entre le *cloud* développé au niveau du réseau d'entreprise du ministère des Armées, qui se rapproche des offres commerciales classiques, et le *cloud* tactique, déployé dans des conditions et sur des dispositifs autrement plus contraignants.

Par ailleurs, le terme de « *cloud* tactique » est fréquemment employé non pas pour désigner l'outil technologique en lui-même mais, souvent inconsciemment, pour évoquer l'infostructure de combat dans son ensemble, soit les réseaux, les plateformes, les données, les équipements… Alors synecdoque, il est parfois présenté comme un « concept[85] » ou une « construction intellectuelle[86] ». Dans ce type de discours, il désigne souvent le « système de systèmes » pensé par Owens.

En réalité, le *cloud* tactique est le support technologique permettant la réalisation de ce macro-système. Il est une adaptation de l'architecture des Systèmes d'information opérationnels et de communication (SIOC) aux évolutions technologiques sur les champs de bataille. Il permet la mutualisation des données, en dépit de l'hétérogénéité de leurs sources et de leurs récepteurs, grâce à la mise en relation des différentes plateformes impliquées dans une opération, des centres de commandement jusqu'aux terminaux

85. D. Deptula, « Evolving Technologies and Warfare in the 21st Century: Introducing the "Combat Cloud" », *Mitchell Institute Policy Papers*, vol. 4, 2016, p. 1-10.
86. J. Hess *et al.*, « The Combat Cloud: Enabling Multidomain Command and Control across the Range of Military Operations », *Wright Flyer Papers*, n° 65, 2019, p. 1-28.

embarqués. Il est également un prérequis pour exploiter les nouvelles technologies permettant la corrélation, la fusion et le traitement automatisé de données, comme le *big data* et l'intelligence artificielle. Ces derniers sont des outils d'aide à la décision qui deviennent indispensables pour faire face aux nouveaux « déluges d'informations[87] », aussi bien aux niveaux tactique et opératif, qu'au niveau stratégique. Leur exploitation est l'une des motivations principales de la mise en place du *cloud* tactique.

Le cloud *tactique, comment ?*

L'intégration du *cloud* sur les théâtres pose toutefois des défis sécuritaires, techniques et cognitifs. Rappelons d'abord que les infrastructures d'un *cloud* tactique sont, au moins en partie, déployées dans un environnement hostile – ou *a minima* contraint. L'infostructure ne bénéficie généralement pas des conditions techniques optimales pour son fonctionnement et elle peut être une cible pour les adversaires. La sécurité des données y est donc particulièrement menacée, aussi bien en termes de confidentialité et d'intégrité que de disponibilité. En effet, le *cloud* permet davantage de résilience mais sa vulnérabilité réside dans le fait qu'il rassemble, théoriquement, toutes les données relatives à l'opération en cours. Si un adversaire accède au *cloud*, il accède ainsi à une très grande quantité d'informations éminemment sensibles. Des protocoles de destruction des appareils, en particulier des terminaux, sont donc envisagés, et une grande vigilance de la part des utilisateurs est impérative.

Sur les théâtres, la connectivité est assurée par des liaisons satellitaires, radios, hertziennes, ou, plus rarement, filaires lorsqu'il est possible d'utiliser les infrastructures locales. La bande passante y est souvent faible et aléatoire, ce qui peut contraindre la disponibilité des données et le recours à des outils permettant leur exploitation, en particulier lorsque ceux-ci ne sont déployés qu'au niveau des centres de commandement, voire en métropole seulement[88]. Le *cloud* tactique est parfois présenté comme une solution à ce problème, puisqu'il permet de rapprocher des utilisateurs les capacités de stockage et de traitement des données. Le caractère aléatoire de la connectivité peut néanmoins entraver son fonctionnement et c'est un aspect à prendre en compte dans sa conception. Le dispositif doit rester opérationnel même en cas de latence ou de déconnexion.

87. O. Becht et T. Gassilloud, *Rapport d'information sur les enjeux de la numérisation des armées*, *op. cit.*
88. DIA-6_SIC-OPS, « Les systèmes d'information et de communication (SIC) en opérations », Paris, CICDE, 2014 [amendée en 2016].

Il faut ajouter à ces contraintes le besoin de mobilité des équipements. Leur poids et leur taille doivent être restreints afin de permettre leur portabilité. En dépit des progrès dans le domaine de la réduction des composants électroniques, la diminution de la taille des équipements influe nécessairement sur leurs capacités de stockage et de traitement qui s'en trouvent amenuisées. La mobilité des équipements embarqués et des terminaux suppose également qu'ils devront parfois fonctionner sur batterie[89].

Enfin, la mise en œuvre du *cloud* tactique est entravée par le manque d'interopérabilité des plateformes. Les dispositifs SIC se sont longtemps développés de façon parallèle dans les trois armées, conduisant à la disparité actuelle des systèmes. Pour que le *cloud* tactique fonctionne, ces systèmes doivent pouvoir échanger. L'amélioration de l'interopérabilité des capacités SIC est donc un travail en cours au sein des forces françaises, qui se conduit essentiellement à travers l'évolution des divers équipements et armements, progressivement modifiés ou remplacés, à l'image du véhicule blindé multi-rôles Griffon du programme SCORPION de l'armée de Terre. Le développement du *cloud* tactique suppose également l'adaptation des forces elles-mêmes aux nouveaux systèmes. Elles doivent être formées aux nouveaux outils et procédés afin d'être capables de les appliquer en combat, ce qui peut être perçu comme une tâche supplémentaire lourde dans un contexte d'affrontement[90].

Pour répondre à ces impératifs, le *cloud* tactique se conçoit à divers niveaux. On le trouve d'abord au niveau des commandements, en zone arrière, à l'écart des zones de combat direct. Des infrastructures physiques peuvent alors être déployées, notamment dans des containers qui transportent des installations prêtes à l'emploi, comprenant aussi bien les fonctions informatiques que de refroidissement. Ces containers peuvent être assemblés pour augmenter les capacités, et ont une mobilité réduite. Il existe également des *clouds* décentralisés au niveau des différentes plateformes sur le théâtre (plateformes navales, aériennes, SI tactiques et régimentaires…). Ils prennent alors la forme de petits caissons mobiles intégrant des serveurs rudimentaires sur lesquels sont exécutées des machines virtuelles. Cela correspond par exemple au dispositif « Snowball » d'Amazon Web Services[91], qui a une capacité de 50 à 80 teraoctets de données, pèse moins de 23 kilogrammes, mesure environ 50 centimètres de hauteur et de profondeur et 30 centimètres de largeur, et est conçu pour résister à

89. A. Magar, « Assessing the Use of Tactical Clouds to Enhance Warfighter Effectiveness », *Defence Research and Development Canada*, avril 2014.
90. Entretien avec un sous-officier de l'armée de Terre, février 2019.
91. Amazon Web Services constitue la filière *cloud* de l'entreprise Amazon.

des conditions extrêmes (chute, météo, humidité, explosion…) Microsoft propose un dispositif similaire dont les caractéristiques sont identiques : la « Data Azure Box ». Enfin, sont comprises dans le *cloud* tactique des sortes de micro-*clouds* dont les capacités sont très limitées et que l'on trouve au niveau des unités, sur les terminaux.

Ces deux dernières solutions s'apparentent davantage à du *edge computing*, dont le principe est de ramener de petites capacités de stockage et de calcul localement, voire directement dans les terminaux, afin de permettre un premier traitement et une discrimination des données. Cela permet d'obtenir davantage de réactivité avec des informations extraites sur place, et de désengorger la bande passante. Le *edge computing* est d'ailleurs complémentaire du *cloud*, et il est à prévoir que les prochaines évolutions des architectures numériques, militaires comme civiles, tendent de plus en plus vers une combinaison des deux technologies.

Le cloud *tactique, bientôt une réalité ?*

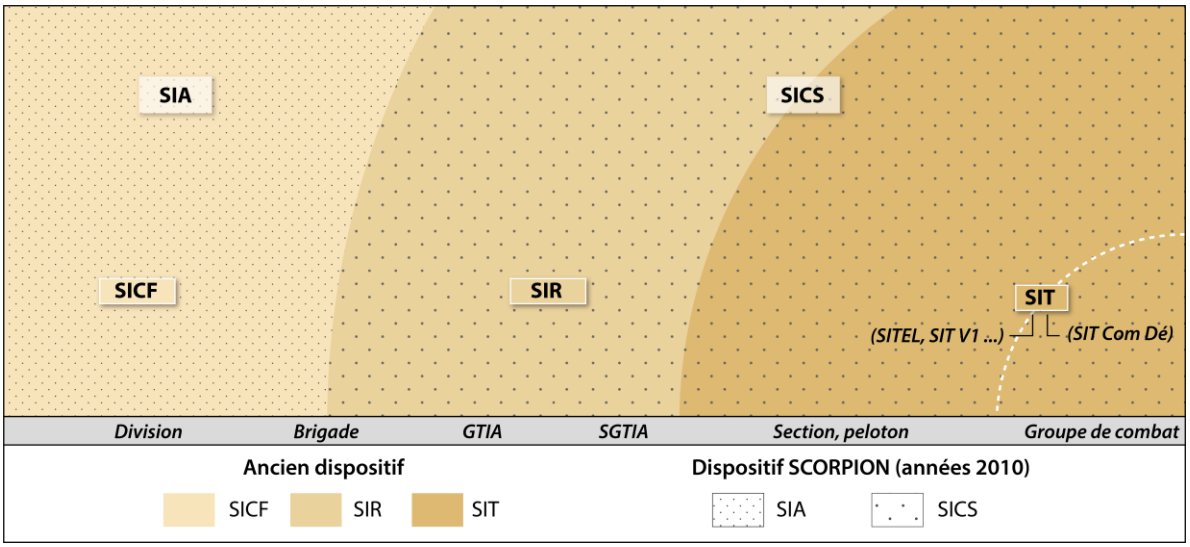
Des projets de *cloud* tactique sont déjà en cours au niveau des trois armées. Le projet de système de combat aérien du futur (SCAF), qui doit permettre le développement d'un système global de combat aérien (SGCA) à l'horizon 2040[92], est sans doute celui qui repose le plus explicitement sur le *cloud*[93]. Le SCAF réunit un ensemble d'équipements qui comprend notamment un chasseur nouvelle génération, remplaçant du *Rafale*, et des drones accompagnateurs (*remote carriers*). Ces équipements seront interconnectés grâce à un *cloud* tactique, afin de « multiplier les effets [des performances individuelles des plateformes][94] ». En avril 2021 ont eu lieu sur les *Rafales* les premiers essais du standard F4, qui doit permettre sa transition vers le combat collaboratif et donc, à terme, vers le SCAF. Le projet est mené conjointement par la France, l'Allemagne et l'Espagne. Si quelques divergences entre les acteurs français et allemands sur le partage d'expertise et de savoir-faire industriel avaient ralenti le projet, un accord a été signé en mai 2021 pour lancer la réalisation d'un démonstrateur qui doit voir le jour en 2026.

Au sein de l'armée de Terre, c'est le programme SCORPION qui initie l'intégration des technologies *cloud* en opérations. Acronyme de « synergie du contact renforcée par la polyvalence et l'infovalorisation », SCORPION doit augmenter la communication et

92. O. Fix, « Le combat collaboratif : la clé de voûte du système de combat aérien des vingt prochaines années », *Revue de Défense nationale*, juin 2019, p. 188-194.
93. P. Gros, « Le *cloud* tactique, un élément essentiel du système de combat aérien futur », Fondation pour la recherche stratégique, note n° 8/19, juin 2019.
94. O. Becht et T. Gassilloud, *Rapport d'information sur les enjeux de la numérisation des armées*, *op. cit.*

le partage d'informations entre les forces et ouvrir la voie au combat collaboratif. Il prévoit la modernisation de certains matériels, comme le char Leclerc, la mise en service de nouveaux véhicules blindés Griffon, Jaguar et Serval, et surtout, le rassemblement des SI de combat au sein d'un SI unique, le Système d'information du combat Scorpion (SICS). Les systèmes d'information régimentaires (SIR) et les systèmes d'information terminaux (SIT) sont donc voués à disparaître (schéma n° 3).

Schéma n° 3 : Évolution des SIOC de l'armée de Terre



Source : Clotilde Bômont, réalisation : Clotilde Bômont ; Guilhem Marotte, 2021.

La Marine nationale n'est pas en reste sur ces questions et travaille activement sur divers projets de plateformisation. Le projet « Axon@V » prévoit par exemple la mise en réseau des forces aéromaritimes afin d'optimiser l'exploitation des données. Dans un souci d'interopérabilité, il devra s'appuyer sur « des architectures numériques compatibles avec les technologies *cloud*[95] ».

Pour augmenter encore les effets du combat collaboratif, le *cloud* tactique a également vocation à être multi-domaines[96]. Lancé en 2012, le programme de Système d'information des armées (SIA) s'inscrit dans cet objectif, puisqu'il vise la convergence des SIOC des trois armées. Dans le même esprit, le *cloud* tactique peut aussi être interalliés. L'OTAN a ainsi annoncé fin janvier 2021 qu'elle confiait la réalisation de son premier *cloud* de combat à l'entreprise Thales et qu'elle avait retenu sa solution « Nexium Defence Cloud ». L'un des plus grands défis pour la mise en place d'un *cloud* tactique

95. H. Perrin, N. Cuoco et C. Canivenc, « Innover pour vaincre. Gagner la bataille des données », *Cols bleus*, n° 3095, avril 2021, p. 16-25.
96. Les cinq domaines de confrontation militaire sont la terre, la mer, l'air, l'espace et le cyber.

otanien est sans doute l'interopérabilité des systèmes de C4ISR[97] des Alliés. La révision du système de classification français IGI 1300 et les programmes comme SIA devraient néanmoins atténuer ces contraintes.

SCORPION lors du salon Eurosatory de 2018

Source : Clotilde Bômont.

97. *Command, control, communications, computer, intelligence, surveillance and renaissance.*

Un *cloud* non souverain pour un ministère régalien ?

Le ministère des Armées ne dispose pas des ressources pour développer et assurer seul le fonctionnement du *cloud* défense. Il doit donc faire appel à des partenaires industriels. Le recours à des fournisseurs privés n'est cependant pas sans risque, en particulier lorsque ces acteurs sont soumis à des juridictions étrangères. Les échecs des précédentes initiatives pour développer des solutions *cloud* dites « souveraines » ont toutefois montré les limites nationales, et les réflexions stratégiques semblent aujourd'hui devoir s'ouvrir au niveau régional.

L'infogérance, quels risques ?

Les réticences culturelles

Ainsi qu'expliqué précédemment, l'intégration du *cloud* au sein du ministère des Armées soulève des inquiétudes d'ordre sécuritaire. Elle nécessite incontestablement des précautions techniques et organisationnelles. Cependant, le *cloud* peut aussi améliorer la sécurité d'un système, et les craintes avérées doivent être distinguées des appréhensions d'ordre culturel, qui sont généralement liées à la numérisation et la « technologisation » dans leur ensemble. Elles renvoient dans un premier temps à la potentielle dépendance à la technologie et au risque que cela représente pour la continuité de l'activité en cas de défaillance du dispositif. Il est vrai que le progrès des technologies numériques et leur intégration au sein des armées peuvent amener certains décideurs à survaloriser le rôle de la technologie dans un combat, parfois aux dépens des autres moyens de la guerre. L'appropriation de la technologie est une autre source d'inquiétude, l'intégration du *cloud* dans les SIC du ministère des Armées nécessitant l'acquisition de nouvelles compétences, tant en termes de recrutement que sur le plan individuel pour tous les agents du ministère.

Certaines craintes sont plus directement dirigées vers le *cloud* lui-même. Initialement, le *cloud* était un symbole – un nuage – dans les schémas d'ingénierie informatique. Il représentait les parties du

réseau particulièrement fluctuantes et imprévisibles, aux composants difficilement identifiables, et dont la gestion n'était pas du ressort des ingénieurs en charge du SI. Cela concernait d'abord les réseaux téléphoniques puis, plus tard, internet. C'est précisément cette abstraction et cet aspect « boîte noire » du *cloud* qui effraient. Ajoutés à l'externalisation, ils font redouter une perte de maîtrise du système.

Un risque géopolitique

L'infogérance présente effectivement des risques mais qui, plus que technologiques, sont surtout géopolitiques. Ils concernent l'accessibilité des données hébergées sur un *cloud*. L'infogérance suppose que les données de l'utilisateur transitent par les infrastructures logiques et physiques d'un prestataire. Leur sécurité dépend alors également de ce prestataire. Or certains gouvernements sont dotés d'une législation leur permettant de forcer la confidentialité des données. Un prestataire peut ainsi être contraint de rendre les données de son client accessibles au gouvernement de l'État dont il dépend. Ces lois ont généralement une portée extraterritoriale, ce qui signifie qu'elles s'appliquent à toutes les données dépendant d'un fournisseur de services, y compris celles hébergées hors des frontières de l'État en question, et celles relatives à des organisations ou des citoyens étrangers. Dans ces circonstances, recourir à un prestataire soumis à une juridiction autre que la juridiction française présente un risque important pour la sécurité des données que ne peut prendre le ministère des Armées et pose, en sus, des enjeux de souveraineté.

Ce risque n'est toutefois pas évident à contourner. Le marché mondial du *cloud* est largement dominé par des fournisseurs de services américains (Amazon, Microsoft, Google, IBM, Cisco, Salesforce…), qui proposent des offres techniquement très performantes et économiquement compétitives. Si la France et l'Europe cherchent à développer leur écosystème industriel et comptent quelques entreprises de pointe dans ce secteur (OVHcloud, SAP, 3DS Outscale, Atos…), ces dernières peinent à rivaliser avec les géants américains. À titre de comparaison, Amazon détient en 2020 plus de 30 % du marché *cloud* mondial[98], tandis qu'OVHcloud, leader européen, en possède moins de 1 %[99].

En outre, le *cloud* est une technologie complexe qui peut impliquer plusieurs acteurs aux compétences complémentaires. Un fournisseur de services applicatifs peut par exemple avoir besoin de sous-traiter son hébergement à un autre industriel spécialisé. Cette

98. « Cloud Market Ends 2020 on a High While Microsoft Continues to Gain Ground on Amazon », *Synergy Research Group*, 2 février 2021, disponible sur : www.srgresearch.com.
99. R. Loukil, « Que pèse OVH dans le *cloud* en France, en Europe et dans le monde ? », *L'Usine Nouvelle*, 13 mai 2020, disponible sur : www.usinenouvelle.com.

chaîne de sous-traitance constitue autant d'occasions supplémentaires d'exposer les données à des juridictions étrangères, même si le prestataire initial répond au droit français. C'est par exemple le principal reproche qui avait été formulé à l'encontre de la Plateforme des données de santé (Health Data Hub) destinée à recevoir les données de santé des Français et hébergée par Microsoft[100]. Du fait de leur position oligopolistique, les acteurs américains interviennent souvent dans les chaînes de services *cloud*, en dépit du fait que les États-Unis soient connus pour leur juridiction intrusive. Ils disposent de lois telles que le *CLOUD Act* (*Clarifying Lawful Overseas Use of Data Act*), qui obligent les entreprises du numérique basées aux États-Unis à fournir au gouvernement toute donnée jugée utile, que celle-ci soit hébergée sur le sol américain ou en territoire étranger. Même si le *CLOUD Act* prévoit que la saisie des données soit autorisée par un juge et fasse l'objet d'un mandat[101], sa portée extraterritoriale entre en conflit avec certains aspects du Règlement général sur la protection des données (RGPD). Pour l'instant moins implantées en Europe, les entreprises chinoises du *cloud* (Alibaba, Huawei…) gagnent progressivement des parts de marché et apparaissent, au niveau mondial, comme les seuls potentiels challengers des acteurs américains. Elles doivent, elles aussi, faire l'objet d'une vigilance accrue et ne semblent pas pouvoir répondre aux exigences de sécurité du ministère des Armées.

Une question industrielle

En dépit de ces risques, il paraît aujourd'hui impossible d'écarter le *cloud*. Y renoncer reviendrait à se priver d'un avantage indéniable, tant sur le plan organisationnel qu'opérationnel. Inversement, ne pas intégrer le *cloud* dans les armées pourrait occasionner un retard important à l'heure où de plus en plus d'États se dotent des moyens de conduire des opérations réseau-centrées et où nos adversaires profitent de la réactivité des technologies *cloud*[102]. Au regard de ces éléments, il apparaît que la question industrielle occupe une place centrale dans la stratégie *cloud* du ministère des Armées. Le vice-amiral d'escadre Arnaud Coustillière, ancien DGNUM, affirme à ce titre « [qu']on choisit de moins en moins un fournisseur de

100. Le ministre de la santé Olivier Véran a annoncé en novembre 2020 que le gouvernement s'accordait deux ans pour changer la plateforme d'hébergeur.
101. La loi a été adoptée en 2018, à la suite de l'affaire qui opposait depuis 2013 l'entreprise Microsoft et le gouvernement américain. Ce dernier souhaitait accéder à des mails hébergés dans les *datacenters* de l'entreprise situés en Irlande, ce à quoi s'est opposé Microsoft en contestant l'étendue de la juridiction américaine. Le *CLOUD Act* permet de clarifier le cadre légal américain de la saisie des données.
102. O. Becht et T. Gassilloud, *Rapport d'information sur les enjeux de la numérisation des armées*, *op. cit.*

technologies, mais de plus en plus un partenaire stratégique[103] ». Le ou les fournisseurs de services au(x)quel(s) faire appel doivent donc répondre à un certain nombre de critères. L'évaluation des industriels devra ainsi tenir compte de leurs performances techniques, de leur sécurité informatique, de leur fiabilité économique et partenariale (soit leur viabilité, leur maturité et l'adéquation des offres aux besoins du ministère des Armées), de leur capacité d'innovation, et enfin, des garanties qu'ils offrent en matière de souveraineté et de gouvernance.

Le JEDI américain, négatif du *cloud* défense français

L'influence historique des États-Unis sur l'intégration des NTIC au sein des SI militaires français et la position oligopolistique des fournisseurs de services américains amènent à s'interroger sur le développement d'un *cloud* défense étatsunien. Le programme « JEDI » (Joint Entreprise Defense Infrastructure) du département de la Défense américain est le pendant du *cloud* défense français. Analyser sa mise en place permet, comparativement, de souligner la nature politique des enjeux qui se posent en France et, plus largement, en Europe. Il est intéressant de constater que les questions industrielles jouent également un rôle majeur dans la réalisation du projet outre-Atlantique. Cependant, les préoccupations ne sont pas les mêmes : bien loin des enjeux de souveraineté, elles relèvent essentiellement de la concurrence industrielle.

Le choix d'une architecture commune

En décembre 2018, le DoD a publié en interne sa stratégie *cloud*, rendue publique deux mois plus tard, en février 2019[104]. Cette stratégie s'inscrit dans un plan plus large de modernisation de l'ensemble du dispositif numérique du département[105] qui prévoit notamment, aux côtés du *cloud*, l'accélération du développement et de l'implantation des solutions d'intelligence artificielle (IA), et l'actualisation des capacités et systèmes C3 (*Command, control and communication*). La stratégie *cloud* du DoD identifie des besoins proches de ceux du ministère des Armées et reconnaît, comme dans le cas français, les intérêts de l'informatique en nuage pour le département, à commencer par la rationalisation des ressources, le renforcement de la sécurité des systèmes et la facilité d'intégration des nouvelles technologies (IA, IoT, *big data*) qu'il permet. Une

103. *La Transformation numérique du ministère des Armées. Concepts clés*, Défense Connect, Paris, mars 2020.
104. *DoD Cloud Strategy*, Department of Defense, Washington D.C., décembre 2018.
105. *DoD Digital Modernization Strategy*, DoD Information Resource Management Strategic Plan FY19-23, Department of Defense, Washington D.C., juillet 2019.

différence notoire réside cependant dans le fait que plusieurs services du DoD utilisaient des solutions *cloud* antérieurement à la stratégie de 2018. Les efforts étaient toutefois très disparates en fonction des services, ce qui a conduit à des écarts dans le niveau de développement des solutions, à la création de silos et à des incompatibilités entre systèmes.

S'il est aujourd'hui abandonné, le programme « JEDI », pilier central de la stratégie *cloud*, devait justement permettre de développer une solution commune à l'ensemble du département. Le *cloud* JEDI avait vocation à accueillir les trois niveaux de classification du DoD, au sein d'environnements distincts et solidement cloisonnés. Il se concentrait sur les niveaux IaaS et PaaS, le niveau SaaS étant développé séparément. Il était également pensé comme un support pour les technologies émergentes, au premier rang desquelles l'IA. Enfin, la stratégie précise que le *cloud* JEDI devait s'étendre du Pentagone et de ses agences, sur un modèle de *cloud* centralisé, jusqu'au front, en appui des combattants, selon une logique de *edge computing*. À l'exception des données hébergées sur les infrastructures de théâtre (les « *tactical data centers* »), il était prévu qu'aucune donnée du DoD ne soit hébergée en dehors des États-Unis[106]. Le département de la Défense américain ambitionne néanmoins de développer une infrastructure hors des frontières étatsuniennes afin d'assurer la mise à disposition de capacités *cloud* en opérations. La stratégie devant guider la mise en place de cette infrastructure complémentaire est parue fin mai 2021[107]. Elle insiste particulièrement sur la transition vers les opérations multi-domaines et rappelle le rôle du *cloud* dans cette évolution.

L'agence en charge du développement du *cloud* JEDI était le Cloud Computing Program Office (CCPO), qui était originellement sous la direction conjointe du DoD Chief Information Officer (DoD CIO) et de la Defense Information Systems Agency (DISA), avant d'être basculé sous la direction exclusive de cette dernière en janvier 2021. Le socle architectural constitué par JEDI devait être complété par d'autres solutions, parmi lesquelles la Defense Enterprise Office Solution (DEOS), qui est une offre de *cloud* SaaS fournissant des outils de bureautique étendus, et *milCloud 2.0,* qui est une offre de *cloud* tactique complémentaire fournie par l'entreprise General Dynamics Information Technology et gérée par la DISA.

106. Entretien avec un responsable du CCPO (Cloud Computing Program Office) du DoD, novembre 2019.
107. *DoD Outside the Continental United States (OCONUS) Cloud Strategy*, Department of Defense, Washington D.C., avril 2021.

L'échec du programme JEDI

La mise en place du *cloud* JEDI n'a cependant pas été sans provoquer quelques turbulences. La stratégie de 2018 annonçait que le DoD ne pouvait développer seul le projet et devait s'associer à un partenaire industriel :

> « La complexité de cette démarche et le manque d'expérience du département en matière de *cloud* commercial d'entreprise à grande échelle [rendent ce partenariat] crucial pour la réalisation du *cloud* [devant servir l'ensemble du département][108]. »

Un appel d'offres pour un contrat de dix ans s'élevant à dix milliards de dollars a ainsi été lancé peu après la parution de la stratégie, auquel ont notamment répondu les entreprises Oracle, IBM, Google, Amazon et Microsoft. Oracle et IBM étaient particulièrement impliqués dans les projets du DoD qui ont précédé JEDI, mais le manque d'investissement dans leurs capacités *cloud* comparativement à leurs concurrents les a rapidement disqualifiés[109]. Si Google était un concurrent sérieux, notamment du fait de ses compétences en IA, l'entreprise a décidé de se retirer de la course à la suite des protestations véhémentes de ses employés qui ne soutenaient pas la vision du DoD. Le Chief Management Officer John H. Gibson, numéro trois du département, avait en effet affirmé que le projet visait à « augmenter la létalité du département[110] ». Pour les mêmes raisons, Google avait déjà mis un terme quelques mois plus tôt au projet « Maven » dont l'objectif était d'améliorer, grâce à l'IA, la surveillance militaire basée sur des images obtenues par drones. Restaient en lice Amazon Web Service et Microsoft.

Dès les prémices du projet, des réticences avaient été exprimées au sein du Congrès quant au recours à un fournisseur unique pour un contrat si conséquent. Le risque de *vendor lock-in*[111] avait été particulièrement pointé du doigt, et certains membres du Congrès s'inquiétaient de l'atteinte à la libre-concurrence que pouvait occasionner ce monopole pour les futurs contrats. Cet argument a notamment été repris par Oracle qui dénonçait, en sus, des biais dans le contrat JEDI qui auraient favorisé Amazon. C'est néanmoins à Microsoft que le contrat a été attribué en octobre 2019.

108. *DoD Cloud Strategy*, *op. cit.*
109. Entretien avec un journaliste américain, novembre 2019.
110. P. Gralla, « Should Microsoft Help the Pentagon 'Increase Lethality'? », *Computerworld*, 5 novembre 2018, disponible sur : www.computerworld.com.
111. Parfois traduit par « enfermement propriétaire », le *vendor lock-in* désigne une situation dans laquelle un utilisateur ne peut se détacher d'un fournisseur sans que cela n'entraîne des coûts importants, voire une transformation profonde de son dispositif. Cette dépendance est principalement due à un manque de compatibilité et d'interopérabilité des offres avec celles d'autres fournisseurs.

Cette attribution a immédiatement été contestée en justice par Amazon qui a accusé l'ancien président des États-Unis Donald Trump d'avoir influencé la décision. L'hostilité était effectivement grande entre Donald Trump et Jeff Bezos, le fondateur d'Amazon qui se trouve aussi être le propriétaire du journal *Washington Post* dont la ligne anti-Trump était ouvertement affichée. La plainte déposée par Amazon a été jugée recevable et la juge fédérale Patricia Campbell-Smith a décidé, en février 2020, de suspendre le projet en attendant la résolution du procès. Cela a finalement conduit à la réouverture du contrat. Après réévaluation des propositions, le DoD s'est de nouveau prononcé fin 2020 en faveur de Microsoft, ce qui a derechef été contesté par Amazon sur la base de modifications apportées aux critères d'évaluation entre les deux appels d'offres. Le procès ne trouvant toujours pas d'issue près de deux ans après le lancement du programme JEDI, le département de la Défense a pris la décision en juillet 2021 d'annuler le contrat. Si les travaux pour mettre en place des solutions *cloud* au sein du DoD ont été grandement ralentis par ces désaccords entre les deux grands acteurs industriels, ils ne sont pas restés au point mort pour autant. Ces démêlés juridiques ont donné l'occasion au département de réévaluer ses besoins et un nouvel appel d'offres devrait être lancé prochainement. Appelé Joint Warfighter Cloud Capibility, le nouveau projet s'inspirera largement de la stratégie de 2018 mais remplacera JEDI et impliquera cette fois plusieurs fournisseurs[112].

Vers un consortium industriel européen ?

L'exemple du *cloud* américain JEDI souligne l'importance de la dimension industrielle dans les stratégies *cloud*. Il met en exergue la particularité européenne de la « souveraineté numérique ». Cette question est aujourd'hui au cœur des stratégies numériques nationales et européennes, et conditionne le développement du *cloud* défense.

Une offre nationale limitée

Le lien entre souveraineté et *cloud computing* a été fait dès le début des années 2010, lorsque le projet Andromède de *cloud* souverain a été lancé par le gouvernement Fillon. Fondé sur un partenariat public-privé, Andromède prévoyait la construction *ex nihilo* d'une offre de *cloud* pour les administrations françaises. Une mauvaise gouvernance, un manque de compréhension de la technologie et des enjeux, et la méconnaissance de l'écosystème industriel français du

112. K. Conger et D. E. Sanger, « Pentagon Cancels a Disputed $10 Billion Technology Contract », *The New York Times*, 6 juillet 2021, disponible sur : www.nytimes.com.

cloud ont toutefois conduit à l'échec du projet gouvernemental, déjà scindé en deux initiatives concurrentes – Cloudwatt, porté par Orange et Thales, et Numergy, mené par SFR et Bull – quelques mois à peine après son lancement[113]. Le projet aura finalement coûté plus de 75 millions d'euros à l'État français qui s'en retire officiellement en 2015. S'il a entamé les velléités politiques et a freiné, pendant un temps, les initiatives nationales, cet échec a tout de même permis une prise de conscience quant à l'importance stratégique du *cloud* et a révélé l'ampleur des travaux à conduire pour élaborer des offres « souveraines ».

En dépit des efforts fournis ces dernières années, les offres nationales restent limitées et ne permettent pas d'assurer de façon optimale l'ensemble des services *cloud*. Aucun acteur français n'est aujourd'hui en mesure de répondre seul à tous les besoins du ministère des Armées en matière de *cloud* (IaaS, PaaS, SaaS, connectique, sécurité informatique, terminaux…). En outre, même si le ministère des Armées privilégie des partenaires nationaux, il est difficile de garantir que l'ensemble d'un dispositif est un produit entièrement français. Le VAE Arnaud Coustillière précise à ce sujet :

> « Croire que les composants ou les logiciels pourraient être tous nationaux est une illusion. Cet effort serait inutile car, même développés en propre, les produits numériques ne pourront jamais être considérés comme parfaitement fiables. De plus, leur maintien à jour et en conditions de sécurité est bien souvent un défi coûteux, rendant les logiciels propriétaires non nationaux très attractifs.[114] »

Il semble donc que le *cloud* défense doive reposer sur un consortium industriel qui intégrera fatalement, à un niveau ou à un autre, des acteurs étrangers.

De nombreuses initiatives européennes

Dans cette perspective, il convient de définir les potentiels partenaires étrangers garantissant au ministère des Armées la maîtrise la plus satisfaisante de son *cloud* défense. Pour l'heure, seuls quelques acteurs industriels européens peuvent y prétendre. Dans la *Revue stratégique de défense et de sécurité nationale* de 2017, la France avait effectivement admis la possibilité de coopérer avec des

113. C. Bômont et A. Cattaruzza, « Le *cloud computing* : de l'objet technique à l'enjeu géopolitique. Le cas de la France », *Hérodote*, n° 177-178, 2020, p. 149-163.
114. A. Coustillière, « La transformation numérique du ministère des Armées », *Hérodote*, n° 177-178, 2020, p. 165-177.

partenaires étrangers dans les domaines technologiques, tout en affirmant une préférence européenne[115].

Le développement de solutions *cloud* au niveau européen n'est pas une idée neuve, et plusieurs démarches ont été entreprises dans ce sens, aussi bien par les institutions européennes que par les fournisseurs de services *cloud* eux-mêmes. Toutes les parties prenantes s'accordent effectivement sur le besoin d'ouvrir le marché du *cloud* à l'échelle européenne afin de permettre aux entreprises d'atteindre une taille critique. La Commission européenne a ainsi publié deux stratégies portant sur l'informatique en nuage, en 2012[116] et 2016[117]. Dans le cadre du marché unique du numérique[118], elle a aussi missionné plusieurs groupes de travail chargés d'émettre des propositions sur divers sujets comme la réglementation, la portabilité et la réversibilité des données, et l'établissement de bonnes pratiques et de certifications[119]. Elle a également inauguré le 19 juillet 2021 l'Alliance industrielle européenne pour les données, le *edge* et le *cloud*, qui rassemblera des représentants politiques, des entreprises et des membres de la société civile[120].

Parallèlement, les acteurs industriels européens du *cloud* se sont organisés en groupes d'intérêt afin d'influencer les orientations politiques et de promouvoir communément leurs visions. Parmi ces groupes, EuroCloud Europe est la plus importante fédération d'acteurs du *cloud* au monde et réunit, au sein de 31 branches locales (EuroCloud Sweden, EuroCloud Croatia, CIF -ex-EuroCloud UK…), aussi bien des entreprises que des groupements industriels nationaux déjà constitués. On peut également évoquer l'association Cloud Infrastructure Services Providers in Europe (CISPE) qui réunit des sociétés fournissant des services IaaS et actives sur le marché européen (plus de 90 % d'entre elles sont européennes, et 75 % sont françaises ou italiennes).

115. *Revue stratégique de défense et de sécurité nationale*, Paris, DiCoD, 2017.
116. *Exploiter le potentiel de l'informatique en nuage*, Commission européenne, 2012.
117. *Initiative européenne pour l'informatique en nuage. Bâtir une économie compétitive des données et de la connaissance en Europe*, Commission européenne, 2016.
118. *Stratégie pour un marché unique numérique en Europe*, Commission européenne, 2015.
119. « Shaping Europe's Digital Future: Cloud Stakeholder Working Groups Start Their Work on Cloud Switching and Cloud Security Certification », Commission européenne, disponible sur : www.ec.europa.eu.com.
120. *Digital Sovereignty: Commission Kick-starts Alliances for Semiconductors and Industrial Cloud Technologies*, Bruxelles, Commission européenne, Communiqué de presse, 19 juillet 2021, disponible sur : www.ec.europa.eu.com.

GAIA-X : de l'affirmation d'un marché à celle de valeurs communes

Ces nombreuses initiatives au niveau européen confirment la volonté des États membres de s'affirmer sur le sujet et traduisent le partage de valeurs communes. Plusieurs pays européens, parmi lesquels la France, semblent ainsi vouloir développer des alternatives aux solutions américaines et chinoises en ouvrant une « troisième voie » construite sur la transparence et la protection des utilisateurs. La nouvelle stratégie *cloud* française de mai 2021 évoque ainsi la notion de « *cloud* de confiance » et propose un label qui viendrait compléter la certification « SecNumCloud » de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et qui garantirait que les solutions labellisées ne sont pas soumises à des juridictions extraterritoriales. Portée notamment par le ministre de l'Économie et des Finances Bruno Lemaire, cette nouvelle stratégie est résolument tournée vers les projets européens, et en particulier vers le projet GAIA-X.

GAIA-X est une association internationale à but non lucratif de droit belge dont l'objectif est la création d'une « infrastructure de données européenne » commune[121]. Le projet cherche à fédérer les différents acteurs du *cloud* en Europe afin de faciliter l'interopérabilité des offres et le partage de données industrielles pour valoriser leur exploitation. GAIA-X a été pensé comme un moyen de redonner aux utilisateurs européens (individus, administrations et entreprises) la maîtrise de leurs données, grâce à des standards techniques assurant la portabilité, la réversibilité et la sécurité des données, et à des exigences juridiques empêchant leur captation. Cependant, depuis novembre 2020, l'association a décidé d'accepter en son sein des acteurs étrangers, parmi lesquels de grands acteurs américains (Google, Microsoft, Oracle, Salesforce, Palantir…) et chinois (Alibaba, Huawei, Haier).

Le conseil d'administration de GAIA-X a annoncé fin mars 2021 qu'un label allait être mis en place pour la fin de l'année afin de distinguer les offres respectant l'ensemble des exigences posées par l'association et qu'« être membre [de Gaia-X] ne garantit pas que les services sont conformes [à ces exigences][122] ». Les membres du conseil d'administration de GAIA-X ont expliqué que ne pas impliquer les plus grands acteurs du secteur dans le projet limiterait son envergure et freinerait encore l'interopérabilité, pourtant au cœur de la démarche. S'il ne fait pas de doute que certaines de ces entreprises souhaitent se conformer aux exigences de GAIA-X,

121. Voir le site web du projet GAIA-X : www.gaia-x.com.
122. « GAIA-X Accelerates with 212 New Organizations Joining and Announces a Forthcoming Compliance Label », GAIA-X, Communiqué de presse, 29 mars 2021.

en particulier concernant le respect de la souveraineté des États sur leurs données, la possibilité effective de cette conformité interroge.

On retrouve, au niveau national, une certaine symétrie avec l'ouverture du label « *cloud* de confiance » à des entreprises non françaises, et même non européennes. La stratégie de 2021 indique : « les services [édités par des entreprises extra-européennes] pourront également être labellisés sous certaines conditions portant notamment sur l'entité opérant ces services et sur la localisation des données[123] ». La territorialisation des données est effectivement un impératif, mais elle ne suffit pas du fait de la portée extraterritoriale de certaines juridictions étrangères. La question de l'opérateur renvoie, elle, au nouveau positionnement du gouvernement qui envisage que les technologies étrangères soient intégrées aux partenariats sous licence, et qu'elles soient donc opérées par des acteurs français. La mise en œuvre de ce nouveau type de partenariats reste cependant à préciser et devra faire l'objet de développements plus conséquents.

Le niveau européen semble donc pertinent pour favoriser la croissance de l'écosystème industriel national. Toutefois, l'implication d'acteurs américains ou chinois dans les projets européens et la récente ouverture française aux entreprises non européennes peuvent s'avérer problématiques pour le ministère des Armées. La déclinaison de la nouvelle stratégie nationale au sein du ministère des Armées soulève également quelques interrogations : s'il est admis que le *cloud* défense sera construit par un consortium d'acteurs, les modalités de partenariats et l'intégration d'acteurs extra-européens restent encore à déterminer.

123. *Stratégie nationale pour le* cloud, mai 2021, *op. cit.*

Conclusion

En moins d'une génération, les technologies de l'information et de la communication ont été massivement intégrées à l'environnement militaire. Si elles ont permis sa modernisation, elles ont également généré de nouveaux besoins, notamment informatiques. Le *cloud* permet en partie d'y répondre, et apparaît comme un prérequis pour conduire la transformation numérique du ministère des Armées et pour faciliter l'adoption de technologies émergentes telles que l'intelligence artificielle ou la 5G/6G.

Évoqué pour la première fois en 2010, le *cloud* défense semble aujourd'hui, plus que jamais, près de devenir réalité. De nombreux chantiers indispensables à sa réalisation ont été entrepris (recensement des besoins métiers, recrutements, préparation de l'opérateur, rationalisation des infrastructures…) et il a fait l'objet de plusieurs feuilles de route au sein du ministère. Toutefois, les tâtonnements politiques ralentissent l'exécution du projet, qui doit déjà compter avec les défis internes au ministère des Armées : développement du *cloud* tactique, refonte du système de classification, acculturation des agents…

La question industrielle s'avère être l'un des principaux enjeux dans la mise en place d'un *cloud* à usage des armées, ainsi qu'en témoignent les atermoiements autour du *cloud* américain JEDI. Dans le cas du *cloud* défense français, cette question renvoie également aux vifs débats qui ont actuellement cours au sujet de la souveraineté numérique. Face à l'oligopole américain et à la montée en puissance des challengers chinois, celle-ci paraît ne pouvoir se construire qu'en comprenant une dimension européenne.

Le déploiement du *cloud* défense français dépend toutefois de l'avancement de divers chantiers préalables à la transformation numérique du ministère. Les travaux d'urbanisation[124] et de transversalité des SI devront ainsi être accélérés et conduits jusqu'aux plus bas échelons de commandement. La réunion, à l'échelle du ministère, des efforts et des investissements (humains, financiers, technologiques) peut encore être poursuivie et faciliterait également l'intégration du *cloud* au sein du ministère.

124. En informatique, l'urbanisation d'un SI est une démarche qui consiste à cartographier et organiser les différents éléments constitutifs du SI et leurs relations.

En outre, le positionnement stratégique de la France en matière de *cloud*, mais aussi plus généralement sur les questions numériques, gagnerait à être plus affirmé. Il repose sur des concepts, à l'image de la « souveraineté numérique », qu'il conviendrait de mieux définir pour les rendre davantage opérationnels[125]. Ainsi, les modalités de construction du *cloud* défense et de recours à des fournisseurs non nationaux pourraient être mieux encadrées afin de répondre aux impératifs politiques et stratégiques.

Le *cloud* défense, enfin, ne pourra être pérenne qu'à condition que les décideurs politiques s'appliquent à comprendre autant les rouages techniques de la technologie que le contexte social dans lequel elle se développe. Cette approche socio-technique devrait ainsi permettre de ne pas reproduire les erreurs du *cloud* souverain.

125. Le Rapport parlementaire sur la souveraineté numérique du 1er octobre 2019 affirme à ce sujet que « la stratégie gouvernementale pour la défense de la souveraineté numérique est dispersée entre souveraineté et libertés publiques, sécurité et défense, et présence économique effective sur un marché nécessairement mondial, ce qui la rend peu lisible ». Voir F. Montaugé (président) et G. Longuet (rapporteur), *Rapport fait au nom de la commission d'enquête sur la souveraineté numérique*, Rapport n° 7, Paris, Sénat, octobre 2019.

Les dernières publications des *Focus stratégique*

- Raphaël Briant, « La synergie homme-machine et l'avenir des opérations aériennes », *Focus stratégique*, n° 106, Ifri, septembre 2021.
- Raphaël Briant, Jean-Baptiste Florant et Michel Pesqueur, « La masse dans les armées françaises : un défi pour la haute intensité », *Focus stratégique*, n° 105, Ifri, juin 2021.
- Laure de Rochegonde et Élie Tenenbaum, « Cyber-influence : les nouveaux enjeux de la lutte informationnelle », *Focus stratégique*, n° 104, Ifri, mars 2021.
- Corentin Brustlein (dir.), « Collective Collapse or Resilience ? European Defense Priorities in the Pandemic Era », *Focus stratégique*, n° 103, Ifri, février 2021.
- Marc Hecker, « Djihadistes un jour, djihadistes toujours ? Un programme de déradicalisation vu de l'intérieur », *Focus stratégique*, n° 102, février 2021.
- Morgan Paglia, « Réparer 2020 ou préparer 2030 ? L'entraînement des forces françaises à l'ère du combat multi-domaine », *Focus stratégique*, n° 101, janvier 2021.
- Jean-Baptiste Florant, « Cyberames : la lutte informatique offensive dans la manoeuvre future », *Focus stratégique*, n° 100, janvier 2021.
- Jean-Christophe Noël, « À la recherche du soldat augmenté : espoirs et illusions d'un concept prometteur », *Focus stratégique*, n° 99, septembre 2020.

27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org