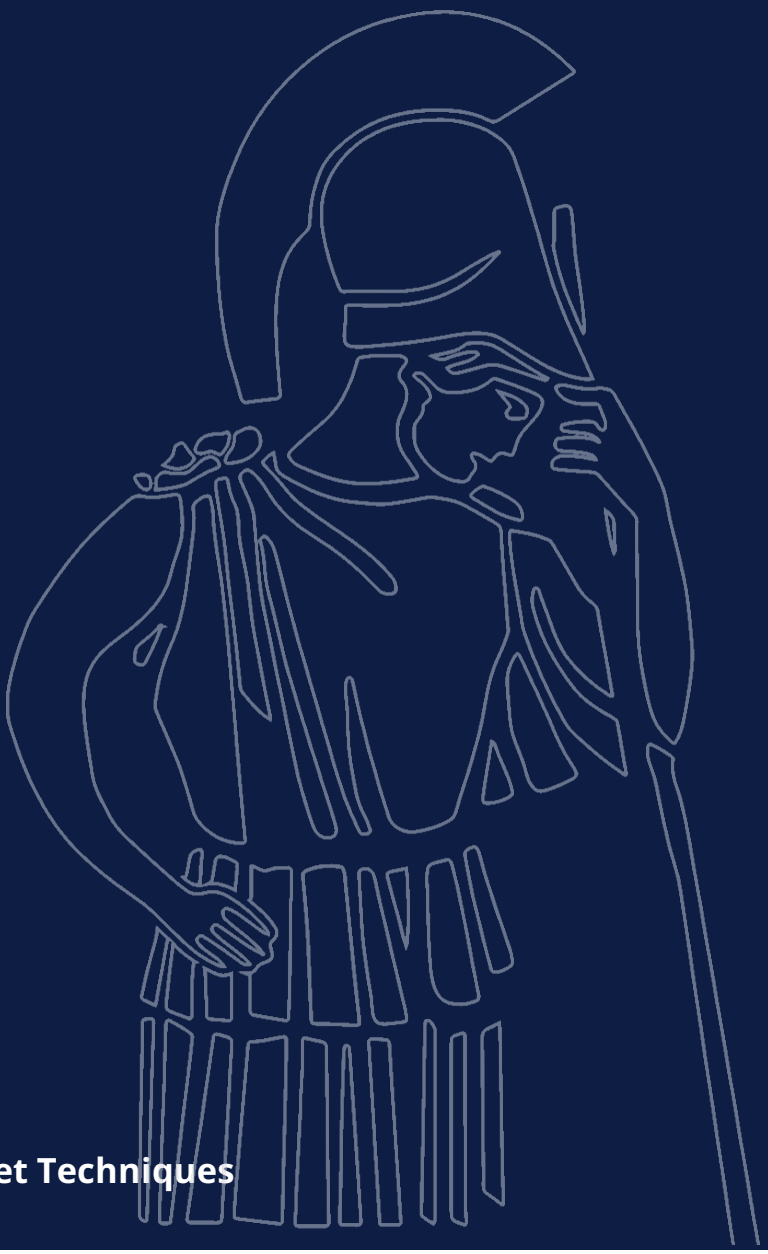
LES JEUNES IHEDN

[RECHERCHE]

# CLOUD ET FOG COMPUTING

## LEVIERS STRATÉGIQUES POUR LA SOUVERAINETÉ ET LA DOCTRINE MILITAIRE



**Par Romain D. et Samuel H.**
**Groupe d'Études Scientifiques et Techniques**

*Ce texte n'engage que la responsabilité des auteurs. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.*

# SOMMAIRE

# À PROPOS DE L'ARTICLE

Cet article est publié par le groupe d'étude scientifique et technique des Jeunes de l'IHEDN. Crée début 2025 il vise avant tout à rendre accessible les enjeux techniques et scientifiques, tout en les reliant aux enjeux doctrinaux et géopolitique, afin d'avoir une meilleure compréhension des concepts.

Nous proposons au sein de cette article une analyse technique des enjeux du *cloud* et du *fog computing*. Devenu aujourd'hui un enjeu de souveraineté le *cloud* est tout aussi utile pour les Armées que pour la société civile afin d'effectué leur tâche quotidienne. Alors que des lois comme le « *cloud act* » mettent en danger les données de nombreux utilisateur et que les unités de combat sont de plus en plus infovaloriser. Nous étudierons dans un premier temps ce qu'est le *cloud* et son utilisation civile et les enjeux de souveraineté associé puis dans un second temps nous étudierons le *fog computing* nouvelle forme de gestion et traitement des données. Enfin nous verrons comment ces technologies sont utiles dans la mise en œuvre de doctrines militaires contemporaines.

Nous tenons à remercier le professeur des universités Guillaume Pierre, d'abord pour avoir éveillé notre curiosité sur ce sujet, puis pour sa relecture attentive.

# À PROPOS DES AUTEURS

**Romain D.** est étudiant en informatique à l'Université de Rennes, il est engagé en tant que Chargé de Mission des Jeunes-IHEDN au sein du Groupe d'Etudes Scientifiques et Techniques, où il occupe le poste de chef de projet Cyber / IA.

**Samuel H.** est doctorant en cybersécurité à CentraleSupélec. Il est membre du Groupe d'Etudes Scientifiques et Techniques au sein de l'équipe Cyber / IA des Jeunes-IHEDN.

# La tête dans les nuages

## Qu'est-ce que le cloud ?

Le *cloud* est une technologie informatique qui a pu se développer considérablement ces dix dernières années, grâce à des connexions au réseau internet de plus en plus rapides et de moins en moins coûteuses. Il y a encore quelques années, la majorité des applications informatiques devaient nécessairement être installées sur des ordinateurs que l'utilisateur possédait, et les entreprises devaient dépenser des milliers d'euros dans leurs propres des infrastructures physiques. L'essor d'internet a permis de délocaliser tous ces services dans le *cloud*, et in fine de réduire les coûts. Concrètement, des entreprises comme Amazon, Microsoft ou *OVHcloud* mettent à disposition, via internet, des serveurs (des ordinateurs conçus pour exécuter des tâches spécifiques) afin que des clients puissent y exécuter leurs applications.

Aujourd'hui, toute application et infrastructure informatique classique est capable d'être hébergée sur une infrastructure de *cloud*, distante de l'appareil de l'utilisateur. Cela permet aux particuliers et aux entreprises, d'une part, de réduire les coûts liés à la mise en place et au maintien en condition opérationnelle, d'une infrastructure informatique et, d'autre part, de bénéficier d'une simplicité d'utilisation. En effet, pourquoi une entreprise qui souhaite créer un site web ou se doter d'une grande infrastructure informatique (avec des bases de données, une gestion centralisée des utilisateurs, etc.) achèterait-elle des serveurs, embaucherait-elle des informaticiens et consentirait-elle à de grands investissements, alors que le *cloud* permet, pour une fraction de ce prix, d'être hébergé chez un prestataire ? Ce dernier mettra à disposition l'infrastructure nécessaire, c'est-à-dire les serveurs, mais aussi potentiellement des applications déjà prêtes à l'emploi dans le *cloud*.

Le dernier avantage pour les entreprises est la modularité. Celles-ci n'ont plus besoin de réaliser des investissements dispensable ou temporaires. Par exemple, un site de vente en ligne n'a plus à acheter un serveur supplémentaire pour faire face au pic d'activité sur son site à Noël ; il lui suffit d'augmenter ses ressources dans le *cloud*, puis de les réduire après les fêtes. En effet, dans la logique du *cloud*, le client ne paie que ce qu'il utilise. Enfin, pour le particulier, la simplicité d'avoir accès à ses données partout et à tout moment est un avantage non négligeable, lui évitant de nombreuses manipulations.

L'offre *cloud* aujourd'hui ce divise en trois grands types : *Software as a Service* (SaaS), *Platform as a Service* (PaaS) et *Infrastructure as a Service* (IaaS). Ces termes regroupent différents niveaux d'abstraction informatique. Un SaaS désigne l'exécution d'une application dans le *cloud*, comme l'utilisation de Google Docs ou de Word en ligne via Office 365. L'IaaS, en revanche, représente une abstraction bien plus large, où l'ensemble du service informatique d'une entreprise peut être externalisé dans le *cloud* (bases de données, sites web, gestion des utilisateurs, etc.), mais cela nécessite alors du personnel formé afin de mettre en œuvre ces solutions.

Cependant, le *cloud*, bien que distant, est bel et bien une réalité matérielle. En effet, ces applications sont exécutées grâce à des centres de données (data centers) composés de nombreux serveurs. Ces centres, indispensables, sont toutefois coûteux, que ce soit lors de leur construction ou de leur exploitation. Le fait qu'un data center soit localisé dans un pays spécifique ou exploité par une entreprise d'une certaine nationalité peut avoir son importance, comme nous le verrons plus loin. De même, la consommation électrique des data centers

représente un enjeu écologique majeur[1], surtout dans les pays où l'électricité n'est pas décarbonée.

## Intérêt stratégique du *cloud*

Cette délocalisation des applications est désormais un enjeu de souveraineté. En effet, les leaders du marché du *cloud* sont aujourd'hui essentiellement des entreprises étrangères et extra-européennes. Au-delà des enjeux économiques liés à la perte de ce marché, le contrôle du *cloud* par des entreprises soumises à des lois et obligations bien différentes des nôtres pose un problème de souveraineté. Internet n'ayant pas de frontières physiques, celles-ci sont bien souvent juridiques. De plus, la perte d'accès au *cloud* en raison de tensions diplomatiques pourrait entraîner des conséquences néfastes pour nos intérêts économiques. Malgré la présence d'opérateurs français et européens, ceux-ci restent bien en dessous des grandes entreprises américaines et chinoises sur le marché[2]. L'utilisation de solutions extra-européennes que ce soit par l'État ou par les entreprises françaises, pose alors un problème grave en termes de souveraineté et une vulnérabilité que nos compétiteurs pourraient exploiter.

Bien que des réglementations soient en vigueur pour protéger les données personnelles des citoyens de l'Union européenne, les entreprises ne bénéficient pas des mêmes protections. De plus même si le RGPD est censé protéger les données des citoyens, des réglementations comme le *Cloud* Act, appliqués par les États-Unis, exposent tout de même les données personnelles des citoyens aux services de renseignement américains. Il en va de même pour les entreprises,

[1] SDES. « La consommation d'électricité des centres de données entre 2018 et 2023 ». *SDES* [en ligne], 16/10/2025. Disponible sur : https://www.statistiques.developpement-durable.gouv.fr/la-consommation-delectricite-des-centres-de-donnees-entre-2018-et-2023.

[2] « Les chiffres clés du marché du cloud en septembre 2025 ». *Tic Magazine* [en ligne], 09/09/2025. Disponible sur : https://ticmagazine.bf/les-chiffres-cles-du-marche-du-cloud-en-septembre-2025.

voire les services de l'État dépendant de prestataires étrangers pour leur infrastructure informatique[3].

Cet accès aux données des citoyens français soulève également des questions dans le cas d'une analyse globale de celles-ci par des entreprises ou des États étrangers. Si l'on considère les réseaux sociaux comme une partie du *cloud* (les données et les applications étant majoritairement hébergés dans le *cloud*), des entreprises comme Meta, ByteDance et d'autres détiennent alors une mine d'informations personnelles sur les citoyens français. Cette détention de données pourrait, dans notre cas, poser question quant au risque de manipulation de l'opinion publique, dans un contexte de guerre hybride permanente.

Enfin, la dernière application récente du *cloud* est l'utilisation de l'intelligence artificielle (IA). Les algorithmes derrière cette « révolution » technologique sont en effet incapables de s'exécuter sur les ordinateurs des utilisateurs finaux dans la majorité des cas ; leur accès est donc conditionné à l'utilisation de centres de données ultra-performants. Il apparaît nécessaire, au vu de l'importance croissante de l'IA pour les citoyens français, de permettre une alternative, que ce soit pour la mise au point de grands modèles de langage (LLM) ou pour leur localisation sur le territoire national. Cela permettrait également une réduction non négligeable des émissions de $CO_2$ liées à l'utilisation de l'IA, la consommation électrique sur le territoire français étant très décarbonée.

## Le *Cloud* souverain et le *cloud* de combat

Ainsi il apparait nécessaire, la mise en place de solutions. Celle-ci sont par ailleurs déjà en cours de développement grâce à la stratégie du *cloud*[4] développé pour répondre à la crise de la souveraineté des données. Ainsi, les labels « *Cloud* de

[3] Sénat. « Audition de MM. Anton Carniaux, directeur des affaires publiques et juridiques, et Pierre Lagarde, directeur technique du secteur public, de Microsoft France ». *Commission d'enquête sur la commande publique* [en ligne], 10 juin 2025. Disponible sur : https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html.

[4] « Sécurité, performance et souveraineté : les enjeux de la stratégie cloud du Gouvernement ». *Ministère de l'économie et des finances* [en ligne], 06/04/2023. Disponible sur : https://www.economie.gouv.fr/securite-performance-souverainete-strategie-cloud.

Confiance » et « *SecNumCloud* »[5], portés par l'ANSSI, permettent d'attester et de connaître l'état de la souveraineté et de la sécurité des données chez les prestataires de services *cloud*. De même, le projet GAIA-X vise à offrir aux entreprises européennes des solutions de *cloud* européen, réduisant ainsi leur dépendance aux acteurs extra-européens.

Par ailleurs, la transformation numérique de l'État essaie de reposer sur des solutions de *cloud* interne : l'État devient alors son propre prestataire de services *cloud*, ce qui permet d'exécuter des applications informatiques critiques nécessitant une souveraineté renforcée. Pour les applications non critiques, l'État s'appuie sur des solutions conformes au label *SecNumCloud* pour le traitement de données sensibles ou d'applications sensibles. Enfin, pour les autres besoins des administrations, des solutions *cloud* génériques sont utilisées.

Le *Cloud* est désormais un enjeu majeur, y compris dans le au sein du ministère des Armées[6] et d'autres systèmes d'armes futurs. Ces projets prévoient d'intégrer le « *Cloud* de combat », une évolution logique du « combat info-valorisé ». Ce dernier doit permettre la fusion des capteurs ISR, une prise de décision plus rapide, voire l'intégration d'IA dans les choix de commandement. Cette centralisation des données et des moyens logistiques par l'informatique devrait améliorer significativement les capacités opérationnelles de l'armée française. Cependant, comme nous le verrons plus loin, l'expression « *Cloud* de combat » pourrait relever soit d'un non-sens, soit d'un abus de langage.





[5] Agence National de la Sécurité des Système d'Information. « Posture générale et actions de l'ANSSI sur le cloud ». *ANSSI* [en ligne]. s.d. Disponible sur : https://cyber.gouv.fr/enjeux-technologiques/cloud/.

[6] BOMONT, Clotilde. « Le cloud défense : défi opérationnel, impératif stratégique et enjeu de souveraineté ». *IFRI* [en ligne], focus stratégique n° 107, novembre 2021. Disponible sur : https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/bomont_cloud_defense_2021.pdf.

# Du nuage au brouillard de guerre

## Faiblesse du *cloud* de combat

La France manifeste une volonté affirmée d'assurer sa souveraineté dans le *cloud*, afin de limiter les risques liés à l'extraterritorialité du droit de certains États. Toutefois, cette démarche n'écarte pas les interrogations concernant la sécurité propre au *cloud*. En effet les vulnérabilités induites par la centralisation créent alors un point de défaillance unique. Toutefois même si les fournisseurs de *Cloud* propose des solutions de décentralisation (*Availability Zone*), ces solutions restent vulnérables aux risques globaux et sont pour l'instant très couteuses voire impossible pour un Etat qui souhaite avoir un cloud propriétaire avec des moyens limités. L'exemple le plus frappant étant sans doute l'incendie survenu dans l'un des plus grands data centers gouvernementaux de Corée du Sud[7]. Les risques pesant sur l'infrastructure en elle-même, sont nombreux : frappe de précision pour décapiter le commandement assisté par le *Cloud*, sabotage par des agents étranger, attaque informatique.

De plus, la connexion entre le *Cloud* et le théâtre des opérations présente certaines limites. Les informations doivent être transmises jusqu'aux datacenters avant d'être analysées, ce qui peut entraîner une latence importante, une forte consommation de bande passante et des difficultés en cas de connexion réseau limitée. Si la liaison est physique, elle peut être détruite par du sabotage ou des frappes. Lorsqu'elle repose sur des ondes, elle peut subir des brouillages dans le spectre électromagnétique. Or ce spectre est désormais fortement contesté dans le cadre des combats de moyenne à haute intensité et son usage évolue rapidement.





[7] SERRA, Yann. « Datacenters en feu : le gouvernement coréen a lui aussi négligé les sauvegardes ». *LeMagIT* [en ligne], 08/10/2025. Disponible sur : https://www.lemagit.fr/actualites/366632441/Datacenters-en-feu-le-gouvernement-coreen-a-lui-aussi-neglige-les-sauvegardes.

La mise en place de solutions de *cloud* allégées sur le dit théâtre pourrait bien être une solution. Néanmoins à l'heure où les centre de commandement (C2 Command and Control) en Ukraine sont aisément détectés et détruits par des moyens de frappe dans la profondeur[8]. On peut légitimement se poser des questions quant à la survie d'un tel dispositif devant alors recevoir mais surtout émettre des signaux électromagnétiques[9].

## L'Edge et Fog computing [10,11]

Le *Edge computing* apporte une réponse à ces limites. Plutôt que de transférer l'ensemble des données vers le *cloud*, une partie du traitement est effectuée au plus près de la source de production des données, c'est-à-dire à la périphérie du réseau. Le réseau désigne ici l'ensemble des infrastructures qui assurent la communication entre les équipements : routeurs, antennes 5G, passerelles réseau. Cela permet d'analyser et de filtrer les données plus près de leur source avant de ne transmettre au *cloud* que ce qui est nécessaire. En effet la multiplication des capteurs ISR comme les satellites, IoT militaire, les radar, sonar, les renseignement issus de l'OSINT, renseignement électromagnétique, drone, et bien d'autre, induit alors une large et trop grande quantité de données à traiter et à envoyer. Ironiquement un champ de batailles trop transparent devient opaque en raison d'une massification des sources d'information[12].

Cette approche présente plusieurs avantages majeurs. Elle réduit la latence, un critère essentiel pour des applications critiques telles que les véhicules connectés,





[8] GROS, Philippe ; DELORY, Stéphane & TOURRET, Vincent. « Stratégies russes et guerre en Ukraine : état des lieux ». *Fondation pour la Recherche Stratégique* [en ligne], note n°03/22, 01/03/2022. Disponible sur : https://www.frstrategie.org/sites/default/files/documents/publications/notes/2022/202203.pdf.

[9] « La survivabilité des postes de commandement ». *Point de mire* [en ligne], décembre 2024. Disponible sur : https://www.terre.defense.gouv.fr/sites/default/files/ccf/Point%20de%20mire%20survivabilit%C3%A9.pdf.

[10] AHMED, Arif & al. « *Fog* Computing Applications : Taxonomy and Requirements ». *Arxiv* [en ligne], 26/06/2019. Disponible sur : https://arxiv.org/pdf/1907.11621.

[11] MOURADIAN, Carla & al. « A Comprehensive Survey on *Fog* Computing: State-of-the-Art and Research Challenges ». *IEEE* [en ligne], *vol. 20, n°1,* 2018 Disponible sur : https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8100873.

[12] Académie de la défense. « Le Champ de bataille 2040 ». *Paris Defence and Strategy Forum 2025* [en ligne]. Disponible sur : https://www.youtube.com/watch?v=0jh8D8HwrRA&list=PLkZ9xqja2UKHY4AeV7VZA1udjtplbJaCw&index=9.

les interventions médicales à distance ou encore certaines applications militaires. Dans ce dernier cas, le traitement local des données permet une réactivité accrue sur le terrain, importante pour la coordination des drones, des véhicules autonomes ou des dispositifs de surveillance. Elle diminue aussi la consommation de bande passante en évitant d'envoyer inutilement des volumes massifs d'informations.

Enfin, elle accroît la résilience des systèmes. En cas d'interruption de la connexion au *cloud*, les traitements locaux essentiels, par exemple l'analyse de capteurs ou la détection d'anomalies, peuvent continuer à fonctionner de manière autonome.

Le *Fog* computing étend cette logique du edge computing. Plutôt que de s'appuyer uniquement sur les équipements réseau tels que les antennes, routeurs ou passerelles, il mobilise l'ensemble des ressources de calcul disponibles dans l'environnement. Cela peut inclure des mini-serveurs locaux, des ordinateurs portables, des machines industrielles ou encore des micro-ordinateurs. En pratique, la mise en place de moyen de *fog* computing crée une sorte de « nuage distribué » proche des utilisateurs. Cette flexibilité peut améliorer encore les performances et réduire la dépendance au *cloud*.

Cependant, cette approche soulève plusieurs défis techniques. Il est nécessaire de distribuer la charge de calcul entre des équipements hétérogènes et souvent moins puissants qu'un serveur dédié. Se pose aussi la question de la fiabilité : que se passe-t-il en cas de défaillance ou d'indisponibilité d'un nœud de traitement ? Cela nécessite des mécanismes de redondance, de gestion intelligente des ressources et une sécurité renforcée, car la surface d'attaque potentielle est plus large.

Par exemple avant l'envoi de photo ou vidéo prise par un drone de reconnaissance nous pourrions imaginer que les photos ou flux vidéo passent en premier lieu au sein d'un noeud *fog* ayant un algorithme d'intelligence artificielle permettant

d'identifier seulement les images utiles comme les regroupements de troupe, blindés et autres… Enfin la mise en oeuvre du *fog* computing permettrait « une relative » furtivité ou du moins discrétion électromagnétique.

## Intérêt doctrinal du *Fog* Computing

Le « *Fog* computing » permet, comme dit précédemment, de pallier de nombreuses difficultés techniques sur le champ de bataille. Au-delà d'une solution technique, le *fog computing* permettrait le développement de certains concepts doctrinaux.

## Le *Fog* un atout dans la guerre réseaux centrée

Le principe de la Network Centric Warfare (NCW)[13], ou la « guerre en réseau centrée »[14] version française de la doctrine[15], est d'acquérir l'avantage tactique et stratégique via la supériorité informationnelle sur un adversaire. Cette supériorité informationnelle est rendue possible grâce à la multiplication des moyens C4ISR (*Computerized Command, Control, Communications Intelligence, Surveillance, Reconnaissance*), qui induisent alors une transparence du champ de bataille[16]. Néanmoins, avoir accès aux informations ne suffit pas à garantir la supériorité tactique ou stratégique : c'est au belligérant qui saura le mieux exploiter ces informations, par l'intermédiaire d'actions coordonnées, que reviendra cette supériorité.

Afin de mettre en œuvre la NCW, le ou les belligérants doivent permettre la remontée d'informations vers le C2, qu'elles proviennent de capteurs ISR ou d'unités combattantes. De plus, le partage des informations entre les composantes de la force, afin de créer une « Common Operational Picture », est

[13] https://fr.wikipedia.org/wiki/Network_centric_warfare
[14] Michael Shurkin, Raphael S. Cohen, Arthur Chan, « French Army Approaches to Networked Warfare » *RAND CORPORATION Research Report*, 06/07/2022 Disponible sur : https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2946/RAND_RR2946.pdf
[15] On notera l'intérêt de l'ouvrage de Guy HUBIN *Perspective Tactique*, publié en 2000, bases de l'approche française de la NCW et des thèses défendues ci-dessous.
[16] Académie de la défense de l'Ecole Militaire « Le Champ de bataille 2040 » *op.cit.*

déterminant pour multiplier les effets et accélérer la capacité des unités à manœuvrer.

La NCW a notamment été employée lors de la guerre d'Irak, où elle a permis la victoire de l'armée américaine face aux forces irakiennes, alors considérées comme l'une des principales armées du monde. Cette victoire a été due en partie au partage de l'information, à la réduction de la boucle OODA, à un ciblage précis et à la coordination des forces. Cela a alors affaibli, puis cassé le dispositif adverse, aussi bien sur le plan tactique que stratégique.

La mise en œuvre de la NCW n'est permise que par des moyens techniques, comme les moyens ISR et de communication. C'est ainsi que le *fog computing* pourrait contribuer (si ce n'est déjà le cas) à l'application de cette doctrine en devenant l'une des briques technologiques des systèmes de systèmes. L'implémentation du *fog* permettrait d'améliorer le partage de l'information entre toutes les composantes des armées. En effet, toutes les armées développent le *cloud* de combat, comme la France avec les systèmes d'armes SCAF et MGCS, également des projets comme TITAN succession du projets SCORPION dans l'armée de Terre. Il existe également des projets similaires aussi dans la Marine National dans l'Armée de l'Air et de l'Espace[17]. Toutefois malgré la présence du terme *Cloud* de combat au sein de la majorité de ces projets ne devrait-on pas plutôt parler de « *Fog* de combat » ? (Cela étant sans doute déjà le cas par exemple au sein du Système d'Information du Combat Scorpion via le « boitier vétronique »[18] et la radio logicielle CONTACT[19])





[17] BOURGASSER, Margaux & AUBERT, Fabrice. « Le combat collaboratif, combat du futur ? ». *Esprit défense* [en ligne], n°5, automne 2022. Disponible sur : https://www.defense.gouv.fr/sites/default/files/ministere-armees/esprit-defense-numero-5-automne-2022-dossier-combat-collaboratif-combat-du-futur.pdf.

[18] Pour en savoir plus : GAIN, Nathan. « Entre câbles et cartes mères, plongée dans le cerveau du programme SCORPION » *FOB [en ligne]*, 08/06/2023, disponible sur : https://www.forcesoperations.com/entre-cables-et-cartes-meres-plongee-dans-le-cerveau-du-programme-scorpion/ .

[19] « Le Programme Scorpion : La Révolution du Combat Terrestre Français ». *Projet13* [en ligne], s.d. Disponible sur : https://www.projet13.com/blog-p13/584_le-programme-scorpion-la-revolution-du-combat-terrestre-francais.html.

En effet, le *Cloud* présuppose une connexion totale et constante à des infrastructures informatiques distantes. Cela soulève alors de nombreux problèmes techniques et stratégiques. D'un pur point de vue technique, même si ce *Cloud* de combat peut être déployé sur un théâtre d'opération, la communication avec le *Cloud* aura tout de même une certaine latence et un risque d'être vulnérable à divers brouillages, voire d'être piraté afin de donner des ordres contradictoires à toutes les composantes de la force. D'un point de vue stratégique, la présence dans nos forces d'un point de défaillance unique, en cas de frappe sur l'infrastructure, pourrait alors conduire à une désorganisation de nos propres dispositifs et, par conséquent, à la victoire de la partie adverse.

Le « *Fog* » est alors une solution technologique permettant la mise en œuvre de la Network Centric Warfare[20]. Le fait de déployer, via des systèmes de calcul et de stockage embarqués auprès de tous les échelons de nos forces, un « *Cloud* distribué » (définition même du *Fog* Computing), permettrait alors un ajout significatif de résilience et une réduction de la latence. Néanmoins, l'implémentation du *Fog* ne doit pas signifier la fin du *Cloud* : en effet, ces deux solutions doivent être complémentaires, car le *Fog* sera incapable de traiter un volume de données excessif ni d'effectuer des calculs trop coûteux. Enfin, l'interconnexion des *Fog*s entre les différentes unités combattantes permettrait alors de faire passer ce concept, encore assez théorique, en une réalité informatique, puis peut-être même physique, via, par exemple, l'interconnexion de systèmes d'armes, ce qui est déjà le cas, dans une moindre mesure, dans la Défense Surface Air présente et futur[21,22].





[20] GROS, Philipe. « Le « cloud tactique » un élément essentiel du système de combat aérien futur ». *Fondation pour la Recherche Stratégique* [en ligne], note n°8/19, 19/06/2019. Disponible sur : https://www.frstrategie.org/sites/default/files/documents/publications/notes/2019/201908.pdf.

[21] RIOU, Victor. « Northrop Grumman renforce la défense aérienne de la Pologne ». *Air et Cosmos* [en ligne], 22/05/2023. Disponible sur : https://air-cosmos.com/article/northrop-grumman-renforce-la-defense-aerienne-de-la-pologne-65017.

[22] « La défense surface-air à l'horizon 2035 ». *Centre interarmées de concepts, de doctrines et d'expérimentations*, ETIA-3.3.1.1_DSA(2022), 11/07/2022.

### *Du brouillard dans tous les milieux*

Au-delà de la *Network Centric Warfare*, le « *Fog* » permettrait l'application de la doctrine « *Multi-Domain Operation* » (MDO), qui au sein de l'armée française est la doctrine Multi-Milieux Multi-Champ (M2MC)[23]. Pour rappel, la doctrine M2MC repose sur la coordination des effets issus de plusieurs milieux (air, terre, mer, cyber, espace) et de plusieurs champs (électronique, informationnel), via des structures de C2 dédié[24,25] et l'interconnexion des unités de combat, dans le but d'obtenir, lors d'un engagement, la supériorité sur l'adversaire.

Tout comme pour la NCW, le *Fog* présente plusieurs avantages dans la mise en œuvre de la M2MC. Tout d'abord, le *Fog* permettrait aux différents milieux de communiquer entre eux en ne partageant que les informations utiles pour chaque effecteur de chaque milieu. La connexion, par exemple, entre le *Fog* du chef d'une unité d'infanterie et un avion de combat, afin de mener une mission de Close Air Support (CAS), pourrait être intéressante pour réduire le temps de mise en œuvre de l'arme aérienne. Du point de vue de l'infanterie cela permettrait une meilleure coordination des effets, afin de réduire un point dur adverse, et du point de vue de l'aviateur d'effectuer des frappes d'opportunité, par exemple en transmettant la position d'une cible de haute valeur détectée par un drone FPV. Cette application du *Fog* permettrait, par ailleurs, d'éviter des tirs fratricides, l'aviateur ayant alors, grâce à sa connexion au *Fog*, une pleine conscience de la disposition des unités sur le terrain.

Cet exemple idéal du CAS est peut-être un peu caricatural, mais bien d'autres situations pourraient profiter d'une interconnexion de *Fog*, comme les appuis d'artillerie, les opérations amphibies. Enfin, le « *fog* » permettrait peut-être d'éviter

[23] « Multimilieux et multichamps (M2MC), la vision française interarmées ». *Centre interarmées de concepts, de doctrines et d'expérimentations*, CIA-0.1.1_M2MC (2021), 11/07/2022.
[24] LYAUTEY, Nicolas. « Le Commandement et le contrôle (C2) des opérations multi-milieux multi-champs de haute intensité : vers une nouvelle Révolution dans les affaires militaires (RMA) ». Les *Cahiers de la Revue Défense Nationale* [en ligne], septembre 2023. Disponible sur : https://www.defnat.com/pdf/cahiers/CAH100/05.%20Lyautey%20(CHEM%202023).pdf.
[25] « Commandement et contrôle interarmées en environnement multimilieux-multichamps ». ». *Centre interarmées de concepts, de doctrines et d'expérimentations*, CEIA-3.0_C2IA-M2MC_vision prospective (2022), 18 Juillet 2022.

la surcharge cognitive, notamment pour les combattants qui doivent multiplier les sources de communication et l'utilisation de matériels et d'armements.

### *Un brouillard pour la dilution des forces*

Comme indiqué précédemment, la mise à disposition d'infrastructures de *fog* computing au niveau tactique permettrait alors l'indépendance de celles-ci vis-à-vis d'une communication constante avec le *Cloud*. En effet, ce lien pouvant être brouillé, piraté, ou même l'infrastructure *Cloud* de théâtre pouvant être détruite, il paraît alors nécessaire que l'unité puisse être autonome dans son accès à la situation tactique. Ce concept s'inscrit alors dans la droite ligne de la décentralisation du commandement dans la guerre de haute intensité[26].

En effet, en raison d'une létalité accrue du feu, d'une réduction de plus en plus grande du temps de décision et de capacités importantes de frappe dans la profondeur, il semble aujourd'hui important d'effectuer une dilution des forces[27]. C'est ainsi qu'un pion tactique devrait être capable, dans une moindre mesure, via le commandement par intention (*auftragstaktik*)[28], de prendre de lui-même des décisions quant à l'emploi de sa force et de ses effets. Nous laisserons au lecteur l'appréciation du choix de la taille du pion tactique, pouvant aller du simple combattant (dans des situations de guerre irrégulière) aux SGTIA.

Afin de mener à bien cette décentralisation du commandement, il est alors important que le chef de l'unité tactique puisse avoir à sa disposition, via le « *Fog* », toutes les informations sur la situation de combat, afin de mieux coordonner ses effets disponibles et sa manœuvre. De plus, des interconnexions entre les *Fog*s tactiques de plusieurs unités permettraient alors au chef d'unité de bénéficier

[26] SHURKIN, Michael. « Kill the Homothetic Army: Gen. Guy Hubin's Vision of the Future Battlefield ». *War on the rocks* [En ligne], 04/02/2021. Disponible sur : https://warontherocks.com/2021/02/kill-the-homothetic-army-gen-guy-hubins-vision-of-the-future-battlefield/.

[27] Analogie à la thèse défendue par Guy BROSSOLET dans *Essai sur la Non-Bataille*.

[28] Passage du Général Guy HUBBIN dans la conférence : « La tactique au XXIe sciècle : anatomie de la bataille contemporaine ». *Fondation pour la Recherche Stratégique* [en ligne], 10/10/2022. Disponible sur : https://www.youtube.com/watch?v=K-xJbFm56wQ.

d'une meilleure vision du champ de bataille, voire de coordonner ses effets avec d'autres pions tactiques, sans besoin du C2 ou d'un C2 plus décentralisé[29,30].

Afin de mener cette « guerre en essaim »[31], ou bien la *mosaic warfare*, les chefs d'unité tactique pourraient alors faire appel au *Fog* d'autres unités tactiques, que ce soit pour des demandes d'information ou pour la demande de soutiens. Par ailleurs cette décentralisation et la mise en place de « combat non linéaire » permettrait dans un contexte de transparence du champ de bataille un renouveau de la surprise tactique[32], par la dissimulation de nos forces via leur dilution et leur action offensive via des manœuvre en essaim. Enfin nous noterons que cette décentralisation du commandement vaut pour tous les milieux et qu'elle peut aisément s'intégrer à la M2MC[33].

Nous porterons tout de même une attention particulière à ce que le commandement décentralisé n'implique pas une disparition complète du C2. Les modalités de disposition de ce C2 « décentralisé » étant encore discutées. Cette décentralisation reste relative aux modalités d'emploi de la force : il serait en effet illusoire, qu'en temps de paix de déléguer la responsabilité de la destruction d'un aéronef d'une puissance étrangère franchissant les limites de notre espace aérien, au vu des retombées stratégiques que pourrait avoir cette décision.





[29] GROS, Philippe. « La décentralisation du commandement et du contrôle (C2) des opérations aériennes », *Fondation pour la Recherche Stratégique* [en ligne], n°12/2020, septembre 2020. Disponible sur : https://www.frstrategie.org/sites/default/files/documents/publications/recherches-et-documents/2020/202012.pdf.

[30] GORREMANS, Adrien & NOËL, Jean-Christophe. « L'avenir de la supériorité aérienne. Maîtriser le ciel en haute intensité ». *IFRI* [en ligne], Focus stratégique n° 122, janvier 2025. Disponible sur : https://www.ifri.org/sites/default/files/2025-01/ifri_gorremans_avenir_superiorite_aerienne_2025_0.pdf.

[31] PETER, Mathieu & TERRIER, Julien. *Les opérations guerrières en essaims*. 2019.

[32] HEMEZ, Rémy. « L'avenir de la surprise tactique à l'heur de la numérisation ». *IFRI* [en ligne], Focus stratégique n°69, juillet 2016. Disponible sur : https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/fs69hemez.pdf.

[33] GROS, Philippe & al. « Intégration multimilieux / multichamps : enjeux, opportunités et risques à horizon 2035 ». *Fondation pour la Recherche Stratégique* [en ligne], Rapport n° 35/FRS/M2MC, 28/03/2025. disponible sur : https://www.defense.gouv.fr/sites/default/files/dgris/l%27EPS%202021-08%20M2MC%20enjeux%2C%20opportunit%C3%A9s%20et%20risques%20%C3%A0%20l%27horizon%202035-2040.pdf.

## Conclusion

Pour conclure, comme nous l'avons vu, le *cloud* est à la fois un enjeu de souveraineté et de supériorité tactique et stratégique avec l'*edge computing* et le *fog computing*. La supériorité informationnelle a toujours été un facteur décisif dans les guerres, les batailles et la rivalité entre les États. Aujourd'hui, la technologie nous a permis de passer de l'estafette à une connexion quasi en temps réel sur les champs de bataille ; et demain, nous verrons peut-être des data centers orbitaux[34], voire lunaires[35], lancés par des fusées.

Néanmoins, alors que les forces militaires emploient de plus en plus de moyens technologiques, il est important de prendre conscience des vulnérabilités induites par ceux-ci. Des vulnérabilités comme les attaques cyber et électronique, le manque de résilience et le manque de masse peuvent devenir des failles critiques exploitées par nos adversaires. C'est pourquoi les systèmes d'armes et la réflexion doctrinale doivent prendre en compte ces vulnérabilités et y pallier par la réflexion sur le mode dégradé et la production en masse d'équipements « faiblement » technologiques (comme les drones FPV), capables d'être produits en masse, contrairement à la production unique de systèmes ultra-technologiques en faible nombre[36].

De plus, afin de mettre en œuvre les technologies mentionnées comme le *fog computing* interarmées, il sera nécessaire d'uniformiser les données hétérogènes et de les protéger, que ce soit au repos (c'est-à-dire sur un serveur) ou en transit





[34] Etude de faisabilité faites par Thales Aliena Space pour la Commission Européenne : https://ascend-horizon.eu/data-centres-in-space/ ; BERGER, Éric « Eric Schmidt apparently bought Relativity Space to put data centers in orbit » *Arstechnica [en ligne]*, 02/05/2025. Disponible sur : https://arstechnica.com/space/2025/05/eric-schmidt-apparently-bought-relativity-space-to-put-data-centers-in-orbit/.

[35] NAYAK, Michael. « The Commercial Lunar Economy Field Guide A Vision for Industry on the Moon in the Next Decade ». *Air University Press Maxwell Air Force Base* [en ligne], juillet 2025. Disponible sur https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_186_Nayak_Lunar_Economy_Field_Guide.pdf.

[36] WAGNER, Clixte. « L'héritage du *Galactica* » : une analyse des défis et vulnérabilités induits par la technologie au sein de l'armée de Terre ». *Note de Recherche Commandement du Combat Futur* [en ligne], 22/05/2024. Disponible sur : https://www.terre.defense.gouv.fr/sites/default/files/ccf/20240531_NP_CCF_PEP-BAI_NDR_Galactica.pdf.

(c'est-à-dire lors de la communication) via par exemple la mise en œuvre du concept de Data *Centric Security*[37].

Enfin, à l'heure où des États concurrents de la France souhaitent garder leurs technologies afin d'en faire un moyen de pression géopolitique, et que ceux-ci disposent d'un quasi-monopole sur toute la chaîne de production, des puces aux algorithmes d'IA[38], il est, au vu de ces observations, nécessaire pour la France, l'Union européenne et l'armée française de développer et de maintenir une chaîne de production complète et surtout souveraine dans les technologies de cloud, fog et edge computing. Celles-ci seront demain des atouts pour nos forces militaires, mais aussi d'un intérêt pour les populations française et européenne, via les applications civiles de ces technologies.





[37] Pour en savoir plus : Romain D. « La nouvelle ligne Maginot : Protocoles cryptographiques et défense nationale a l'ère numérique ». *Les Jeunes IHEDN* [en ligne], 02/06/2025. Disponible sur : https://www.jeunes-ihedn.org/2025/protocoles-cryptographiques-et-defense-nationale/.

[38] MOROZOV, Evguyny. « La souveraineté comme marchandise américaine ». *Le Monde Diplomatique*, décembre 2025.







publication@jeunes-ihedn.org