VAUBAN
SESSIONS

# #6 FRANCHIR LES OBSTACLES À L'ADOPTION DU *CLOUD* PAR LES ARMÉES

MARS 2023

Forward

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

# VAUBAN PAPERS

**Cette collection sur l'impact de la transformation numérique sur les Armées et la conduite des opérations synthétise les travaux menés dans la première série de « Vauban Papers », fruit d'un partenariat entre Forward Global et VMware.**

Ces notes sont à la fois le résultat et la poursuite des discussions menées dans le cadre des Vauban Sessions 2021 et 2022, conférence annuelle organisée par Forward Global et le Corps de Réaction Rapide - France (CRR-Fr) à la citadelle Vauban de Lille. L'édition 2022 a rassemblé plus de 150 représentants d'états-majors de 19 nations alliées, de l'OTAN, de l'Union européenne, et de l'industrie de défense.

Les idées et opinions exprimées dans ce document n'engagent que leurs auteurs et ne reflètent pas nécessairement les positions de Forward Global ou de VMware. Forward Global demeure responsable des propos engagés dans cette publication, développés en indépendance.

## À PROPOS DE FORWARD GLOBAL

**Forward Global** est une société mondiale d'intelligence, d'affaires internationales et de cybersécurité. **La branche Cybersecurité et Stratégie de Forward Global** accompagne ses clients publics et privés dans leur prise de décision, leur gestion du risque, leur transformation numérique, leur prospection et leur rayonnement en France, en Europe et dans le monde. Ses consultants combinent une vision prospective avec une approche métier et une connaissance opérationnelle des secteurs dans lesquels ils opèrent.

PLUS D'INFORMATIONS SUR :
**forwardglobal.com**

Forward

## À PROPOS DE VMWARE

**VMware**, **leader des services multi-*Cloud* pour tout type d'application**, soutient l'innovation numérique en permettant aux entreprises de contrôler leurs environnements. En tant qu'accélérateur d'innovation, l'éditeur propose des solutions fournissant aux organisations la flexibilité et le choix nécessaires pour bâtir leur avenir. Basé à Palo Alto, en Californie, VMware est déterminé à créer un avenir meilleur en suivant son agenda pour 2030.

PLUS D'INFORMATIONS SUR :
**vmware.com/company**

vmware

COLLECTION

# VAUBAN PAPERS

## PRÉFACE

La transformation numérique des Armées représente un enjeu essentiel pour leur adaptation à l'évolution permanente de l'environnement géostratégique, des risques et des menaces, et des cadres d'emploi des forces. Les « Vauban Papers » publiés à ce jour ont permis d'établir les principes fondateurs de cette transformation numérique opérationnelle et les enjeux qui la sous-tendent. De ces réflexions, il apparaît clairement que cette évolution va marquer une étape importante dans la modernisation des Armées qui auront su la conduire avec vision et pragmatisme en tirant le meilleur parti du potentiel exceptionnel de l'espace numérique et des technologies qui le sous-tendent. Celles aussi qui sauront maîtriser ses limites et risques propres pour définir des concepts d'emploi robustes et résilients.

Au cœur de cette transformation, se situe la donnée, véritable ADN de ce nouvel espace. L'intérêt, les avantages, les limites de l'exploitation des vastes flux de données qui irriguent les chaines opérationnelles depuis le niveau stratégique jusqu'au combattant ont été examinés dans les « Vauban Papers » précédents. De ces réflexions, il est clairement ressorti que le potentiel des technologies du *« Cloud computing »*[1] se prêtaient parfaitement aux besoins d'accès à ces précieuses bases de données exprimés par les commandeurs aussi bien que les exécutants, dans leurs différents domaines opérationnels en créant ainsi des « *Clouds* de combat ». Pour constituer ces véritables mémoires dynamiques de nombreuses options s'offrent aux décideurs qui doivent pouvoir en apprécier la pertinence, la résilience, la dépendance vis-à-vis de tiers fournisseurs, la sécurité, les conditions d'accès y compris dans un environnement fortement dégradé, le potentiel d'évolution ou encore la confidentialité. Ce dernier point retient particulièrement l'attention, car il impose de revisiter les classifications rigides qui régissaient jusqu'ici les informations opérationnelles afin de les adapter à une gestion dynamique des critères de confidentialité. C'est une des clés du concept de *« Federated Mission Networking »* prôné par l'OTAN pour développer des nouveaux systèmes d'informations agiles, interopérables, fiables et sécurisés.

Les technologies de virtualisation se prêtent particulièrement bien à cet objectif. Elles constituent la base du concept fondateur du développement du nouveau Système de Combat Commun (CCS) britannique. Celui-ci établit différents niveaux de sécurité qui correspondent au niveau de confidentialité requis par les opérations qu'elles soient purement nationales (*Secret*), ouvertes au travail au sein de l'OTAN ou de coalitions de circonstance (*Mission Secret*) ou enfin les échanges « Officiels » qui peuvent se satisfaire d'une classification allégée. Il est ainsi possible selon le besoin et les circonstances de faire transiter des informations de manière dynamique d'un niveau à l'autre en définissant des droits d'accès. Cette analyse méthodologique est un préalable à l'établissement d'un *« Combat Cloud »* efficace, résilient et sécurisé. Elle permet également de choisir en fonction des missions et de l'environnement la structure la plus adaptée et de définir les termes de collaboration avec des tiers de confiance pour tirer le meilleur des nouvelles technologies de l'information.

En conclusion, le développement des différentes solutions qui peuvent permettre de tirer le meilleur parti des flux de données qui caractérisent les opérations modernes ne peut résulter de choix purement techniques. Il nécessite avant tout une réflexion profonde sur l'organisation du commandement, les délégations consenties au niveau d'exécution, le fonctionnement en mode dégradé et comme démontré *supra* une nouvelle définition plus dynamique des critères de confidentialité attachés à ces données, qui, sans altérer les besoins de souveraineté autorisent des échanges au sein de l'OTAN ou de toute autre coalition de circonstance. Ainsi, le succès de cette entreprise et par là même de la transformation numérique opérationnelle repose sur la collaboration de tous les acteurs publics et privés qui seule permettra dans une logique de partenariat « gagnant/gagnant » d'expérimenter le potentiel des nouvelles technologies de l'information au service des opérations.

**Général (2S)**
**Jean-Paul PALOMÉROS**
*Ancien Commandant suprême allié Transformation (SACT) de l'OTAN et Conseiller Sénior chez Forward Global*

1. Cf. Vauban Paper n°5.

# FRANCHIR LES OBSTACLES À L'ADOPTION DU *CLOUD* PAR LES ARMÉES


CONTRIBUTEURS

**Axel DYÈVRE**
Associé
FORWARD GLOBAL

**Martin DE MAUPEOU**
Directeur
FORWARD GLOBAL

**Marin MESSY**
Analyste
FORWARD GLOBAL


**Dans la dernière décennie, de nombreuses armées ont travaillé sur la doctrine et les moyens capacitaires du combat collaboratif, dans les différents milieux (Terre - Air - Mer). Basé sur l'usage de systèmes, de terminaux et d'appareils connectés échangeant en permanence des données du terrain vers le C2 et inversement, le combat collaboratif repose sur des transferts de données massifs et, en conséquence, sur la capacité des unités engagées à avoir un accès fiable et suffisamment rapide au réseau.**

## Mesurer et intégrer le défi de la connectivité

Face aux défis de stockage et de traitement des volumes de données générés par la numérisation des armées, les technologies du *Cloud* peuvent apporter une solution efficace. Elles permettent également de démultiplier la puissance des terminaux (« *Cloud computing* » - calculs à distance) et l'usage en ligne d'applications (*Software as a Service*). Quels que soient les usages qui en sont faits, le recours au *Cloud* implique certaines contraintes d'emploi. La principale - logique pour des usages distants - est d'avoir **une connexion suffisante en débit, en réactivité (latence) et sécurisée**, entre les serveurs où les données ou applications sont stockées et les utilisateurs et moyens déployés sur le terrain (véhicules, drones, ordinateurs, effecteurs, vecteurs...). Ce besoin de connectivité, qui ne pose pas de problèmes particuliers dans la majorité des applications civiles et commerciales, est une contrainte majeure pour les usages des forces armées en opérations. Celles-ci ne peuvent pas toujours reposer sur un réseau filaire de qualité, et reposent sur des moyens radios ou satellites pour le transport des données comme pour les liaisons vocales. En outre, l'environnement et les conditions dans lesquels évoluent et sont déployées les unités sur les théâtres d'opérations ont une très forte influence sur la disponibilité d'une connexion avec un débit et une latence suffisants. Le maintien d'une connexion constante ne peut être assuré en toute circonstance en raison des contraintes physiques imposées par l'environnement, de la mobilité des unités ou encore des actions de l'ennemi :

- **Les contraintes géophysiques :** telles que le relief, mais aussi tout simplement la rotondité de la Terre, peuvent gêner la propagation des ondes et donc des informations qu'elles véhiculent, que ce soit la voix ou les données. En 2013, lors de l'opération française Serval au Mali, les unités engagées ont été par moments étirées sur plus de 700 km et la liaison radio s'est avérée parfois difficile.
  Le milieu naturel constitue une autre forme de contrainte, les ondes ne se propageant pas de la même manière dans l'air que dans l'eau. Un submersible devra se rapprocher de la surface pour émettre et recevoir et donc mettre à risque son principal atout, sa furtivité.
  Autre facteur, la météo - par nature imprévisible à long terme - qui joue sur la propagation des ondes.

- **Le chiffrement des données contribue à augmenter le volume à transporter :** une donnée chiffrée pèse son poids plus celui du chiffrement. Si le réseau est chiffré, son débit est réduit par rapport à sa capacité théorique pour les mêmes raisons : son chiffrement est la première donnée qu'il transporte en permanence.
  La sécurité indispensable des transmissions est donc un facteur qui pèse sur la connectivité.
  Si le réseau est disponible, elle limite la vitesse à laquelle les données sont transmises (« rétrécissement du tuyau ») et augmente le volume (données chiffrées donc plus lourdes) à transmettre.

- **Les technologies numériques sont par nature énergivores :** processeurs, stockage et réseau induisent autant de composants électroniques qui utilisent de l'électricité. Présents partout dans les moyens mis en œuvre, du serveur surpuissant à l'objet connecté sur le soldat, ils augmentent en permanence le besoin d'énergie. Un appareil connecté sans énergie s'arrêtant, le besoin de connectivité demande aussi un besoin de production, de stockage voire de recharge en énergie sur toute la chaîne, que ce soit côté serveurs ou côté utilisateurs sur le terrain.

- Enfin, la chaîne de connectivité nécessaire au bon fonctionnement d'un système en *Cloud* étant un ensemble complexe de moyens, elle est exposée aux **pannes et aux dysfonctionnements techniques,** comme aux erreurs humaines. Une surveillance permanente, un système d'alerte et des moyens d'analyse du fonctionnement sont donc nécessaires.

## Prioriser les données et les besoins d'informations

Si ces enjeux liant connectivité, disponibilité, usage et sécurité sont connus des militaires, ils sont amplifiés et complexifiés par la nature intrinsèquement connectée du *« Cloud computing »*. Ce constat rend nécessaire d'intégrer dès la conception d'un *Cloud* militaire la réflexion sur les conditions d'un déploiement et d'une utilisation de ces technologies « en mode dégradé », soit un fonctionnement en situation de réduction de la bande passante disponible voire de perte totale de connexion, qu'elle soit la conséquence d'une contrainte technique ou d'une action ennemie. Pour le *« Cloud computing »*, la réflexion sur un usage en mode dégradé passe à la fois par des réponses techniques telles que le recours à la méthode du *« Edge computing »* et par la définition de doctrines d'emploi qui, combinés, permettront d'optimiser l'utilisation des données, la résilience des systèmes connectés et *in fine* la maîtrise de l'information.

En environnement contraint, la principale conséquence d'une réduction de la bande passante disponible sera de limiter le flux de données transmissible dans un temps donné. Autrement dit, plus on cherche à transmettre de données, plus cela prendra du temps. En conséquence, il est essentiel de prioriser les données en fonction de leur usage en se demandant : quelles données sont indispensables pour les missions ? Quelles informations sont requises pour l'échelon supérieur ? Quels logiciels doivent nécessairement être déployés à tel niveau ou à tel autre niveau ? Dans le cas d'un véhicule de combat blindé qui transmet constamment des informations à son PC tactique, certaines sont plus critiques que d'autres pour la mission. On peut imaginer qu'en cas de débit limité, on aura - par exemple - tendance à transmettre les données tactiques de localisation des forces amies et ennemies et à attendre avant de transmettre celles concernant l'état technique d'un véhicule ou d'autres informations avec un caractère d'urgence moindre. Dans des cas plus critiques, il est envisageable que certaines fonctions du véhicule nécessitant une connexion puissent même devenir inopérantes, impliquant d'anticiper autant que possible afin d'assurer la meilleure résilience potentielle en mode très dégradé. Disposer, pour chaque système connecté, de typologies de données selon leur niveau de criticité permettra de disposer d'un ordre de priorité pour leur transmission. Ce qui permettra une simplification et un allègement des flux de données tout en évitant un déploiement lourd d'infrastructures, de moyens SIC, de connexions, etc.

La perspective quasi-certaine d'une déconnexion du réseau - que son origine soit accidentelle ou intentionnelle - demande donc d'être préparé aux conséquences d'une coupure totale des flux de données, montants ou descendants, pour une durée indéterminée. Afin d'assurer la continuité opérationnelle des unités et des plateformes de combat, il est primordial d'arbitrer en avance des capacités et outils devant rester à tout prix opérationnels en local, c'est-à-dire indépendamment de leur accès réseau.

## Concevoir et déployer des solutions et des doctrines d'emploi adaptées

Se poser la question des conséquences d'une réduction ou d'une coupure de la bande passante implique également d'envisager le scénario du rétablissement des communications. D'autant plus qu'il peut être aussi souhaitable pour une unité d'avoir la capacité de couper puis de rétablir ses émissions de données selon la situation, par exemple pour réduire le risque d'être détecté et repéré par l'ennemi. Or, le ralentissement ou l'arrêt des flux de données ne signifie pas nécessairement un ralentissement de la captation d'information, ce qui entraine un risque probable de conflits entre différentes versions de la même donnée lors du rétablissement des liaisons. Par exemple, la progression d'un convoi blindé ennemi est suivie par plusieurs capteurs qui transmettent les informations sur sa composition et l'évolution de sa position à un C2. Si un des capteurs perd la connexion pendant quelques minutes et soudain se met à transmettre des données devenues « anciennes », se pose le problème de la « réconciliation » de ces données et donc de la manière dont le système va arbitrer pour ne garder que les données les plus à jour. Ce d'autant plus qu'il est raisonnable d'imaginer que plusieurs unités puissent se déconnecter et se reconnecter simultanément. Afin de prévenir ce risque, il est donc nécessaire de concevoir des solutions techniques et des protocoles permettant d'effectuer cette réconciliation des données.

Ce problème étant aussi rencontré - pour des raisons différentes - par de nombreux secteurs civils depuis des années, notamment dans le domaine des applications mobiles, des solutions ont toutefois été développées pour permettre la synchronisation des informations lorsqu'un terminal retrouve de la connectivité. Comme souvent dans le domaine numérique, les développements issus du secteur civil peuvent donc alimenter les développements faits pour les armées et leurs besoins spécifiques.

Pour optimiser les transmissions et la connectivité dans un environnement de guerre contraint, il peut être également nécessaire d'avoir des « entrepôts tactiques de données » avec des capacités de traitement très déconcentrées ; ces entrepôts pouvant être parfois le capteur lui-même qui concentre à la fois les fonctions de collecte, de stockage, de traitement et de transmission. À cet égard, une piste pertinente est celle du recours au *« Edge computing »*, une méthode qui consiste à traiter les données à la périphérie du réseau soit au plus près de la source des données. En appliquant le principe d'un traitement des données au plus proche des capteurs, on répartit la puissance de calcul nécessaire et on ne se concentre que sur la transmission des données post-traitement, donc en principe réduite par rapport au volume brut initial. En plus de limiter le volume de données transmises lors de la remontée de la chaîne hiérarchique, cette méthode de répartition de la charge de calcul entre les différentes unités augmente la résilience du dispositif : on réduit ainsi l'impact de la perte, ou de l'incapacité temporaire, d'une partie du réseau ou des moyens. Là encore, l'enjeu est d'arbitrer entre la puissance de calcul et les capacités de stockage à embarquer *(Edge)* dans les unités ou les plateformes et le nombre (et la nature) d'opérations à traiter par capacités déportées *(Cloud)* aux niveaux supérieurs. Il revient donc de décider quelles capacités doivent absolument rester disponibles aux unités sur le terrain en mode dégradé. Ce qui sera par exemple le cas des outils de cartographie et de localisation.

Ces différents scénarios soulignent la nécessité de définir et mettre en place des standards opérationnels pour adapter les technologies du *« Cloud computing »* à un usage dans un contexte militaire et interalliés. Cela signifie que dès la conception des systèmes de combat et des tactiques, il est nécessaire de prendre en considération ces cas de figure et de faire en sorte que l'utilisation des réseaux ne soient pas indispensables à la manœuvre et au combat : les unités doivent pouvoir conserver leur capacité opérationnelle en cas de perte des connexions. Si les plus-values opérationnelles du *Cloud* pour les armées ne sont plus à démontrer, le combat collaboratif exige en effet de penser un mode de déploiement et d'utilisation de cette technologie, prenant en compte les risques techniques et les contraintes opérationnelles et plaçant celle de la connectivité (ou plus exactement de sa perte) au cœur de la réflexion. Ce travail permettra de prioriser, rationaliser et organiser les capacités de traitement des données et de transmission des informations entre tous les intervenants des théâtres d'opération.

Parce que l'adoption du *« Cloud computing »* ne peut résulter que de choix purement techniques, il est également nécessaire de penser les implications du *« Cloud computing »* en termes de souveraineté dans le cadre d'engagements en coalition. En effet, dans le domaine militaire, la souveraineté est primordiale, mais l'interopérabilité est également essentielle. Dans le cadre de l'OTAN en particulier, assurer l'interopérabilité entre Alliés constitue donc un enjeu important pour les nations alliées, notamment au regard de la multiplication voire de la systématisation des opérations menées en coalition. Une fois la volonté de partager des données acquises au niveau politique, la définition et la conception d'une infrastructure en *Cloud* doit dès lors assurer le difficile équilibre entre confidentialité et flexibilité pour créer les conditions d'un partage instantané en définissant les critères de confidentialité attachés aux données, les niveaux d'autorisation appropriés et les passerelles techniques.

# FRANCHIR LES OBSTACLES À L'ADOPTION DU *CLOUD* PAR LES ARMÉES

CONTRIBUTEUR

**Général de brigade (2S) Olivier KEMPF**
**Directeur du cabinet stratégique La Vigie**
**Chercheur associé à la Fédération de la recherche stratégique**
**Auteur de Guerre d'Ukraine (Economica, 2022)**

Le *Cloud* (l'infonuagique) est à la mode, présenté par beaucoup comme inéluctable : la question ne serait pas de savoir s'il faut y passer, mais quand. Ce qui est valable pour des organisations civiles présente pourtant quelques difficultés pour le monde militaire : qu'il s'agisse des activités courantes en métropole, où des astreintes de sécurité de réseau existent mais ne sont pas insurmontables ; ou bien des opérations où les défis sont autrement grands.

## Rappelons tout d'abord les raisons du développement de l'infonuagique dans le monde privé

L'infonuagique (*Cloud computing* en anglais, souvent réduit à *Cloud*) désigne la livraison de ressources et de services à la demande par Internet. Autrement dit, là où les applications et les données étaient stockées sur le terminal ou sur le serveur de l'utilisateur (sur le disque dur), elles sont désormais stockées à distance, sur le nuage des fermes de serveurs. L'extension du *Cloud* dépend donc de l'amélioration de l'accès à Internet, en quantité aussi bien qu'en qualité. L'accroissement des débits, mais aussi leur diffusion géographique ont facilité ce passage au nuage. Le nuage bénéficie également de l'augmentation considérable de puissance des serveurs (la fréquence de fonctionnement des serveurs a été multipliée par un facteur 10, entre 1998 et 2008, les processeurs comportent entre quatre et dix cœurs) ; et de la baisse des coûts de stockage (pour le prix d'un disque dur de 1,2 Go en 2000, on a, en 2013, un disque de 1 000 Go).

Ce développement du nuage (donc de l'accès facile à Internet) a favorisé deux des grandes caractéristiques : la mobilité et la permanence. Le développement de l'infonuagique permet aux entreprises de toute taille d'acheter des ressources informatiques sous la forme de service.

Autrement dit, plutôt que d'acheter sur site des réseaux, des serveurs, des logiciels adaptés, des capacités de stockage et l'électricité correspondante, l'entreprise les loue. Ce qu'elle possédait en local, elle le loue désormais à un acteur distant.

Cela présente plusieurs avantages : d'une part, cette location variable permet des économies d'échelle puisque les grosses infrastructures sont partagées par tous les loueurs. Au lieu d'avoir par exemple plusieurs installations de refroidissement, il n'y en a qu'une seule qui travaille au profit de la ferme de serveurs ou de données. D'autre part, cela permet une meilleure gestion des compétences : plutôt que d'avoir un responsable informatique qui doit s'y connaître sur tous les segments (réseaux, serveurs, stockage) et qui doit suivre la mise à jour de la technologie, cette fonction est décentrée vers le spécialiste du nuage. Enfin et surtout, la location de services sur le nuage permet une gestion bien plus fine des ressources, puisqu'on ne consomme que ce dont on a réellement besoin, en fonction des nécessités de la production de l'entreprise. Celle-ci n'est donc plus contrainte soit par des capacités excédentaires inutilisées, soit par des capacités trop justes pour accompagner le développement. Accessoirement, le gestionnaire informatique transfère la responsabilité de la continuité de service au sous-traitant.

Autrement dit, l'infonuagique permet le libre-service à la demande, l'élasticité et le paiement à l'utilisation, donc pour les seules ressources effectivement consommées. Plusieurs inconvénients sont à signaler. Le stockage local permet un accès rapide et simplifié grâce à la proximité du stockage. Surtout, il n'y a pas lieu de craindre une interruption de service due à une indisponibilité du réseau. Enfin, beaucoup considèrent que le stockage local est plus sûr que le stockage distant. Autrement dit, la disponibilité et la sécurité des données sont les deux objections majeures à l'infonuagique.

# FRANCHIR LES OBSTACLES À L'ADOPTION DU *CLOUD* PAR LES ARMÉES

## L'avènement de l'infonuagique doit donc être considéré comme un véritable changement de paradigme

Auparavant, l'ordinateur individuel (celui d'un usager privé ou celui d'un collaborateur d'entreprise) était au centre du réseau. Désormais, cet ordinateur est devenu un périphérique du réseau, du nuage, qui devient donc le cœur du système. Le réseau devient système, et pas seulement interconnexion.

Cela amène à une sorte de paradoxe : le réseau est central, même s'il est décentralisé. Le périphérique est local, il permet une autonomie d'action, mais à condition qu'il ait accès au réseau. Au fond, tout ordinateur devient un objet connecté : il ne procure tous ses bénéfices qu'à la condition d'être relié à Internet (ou au réseau) ou dans le cadre de certaines configurations très précises (par exemple de réseaux fermés). Dans le monde de l'infonuagique, on parle de *Cloud* public, hybride ou fermé, selon l'accès des utilisateurs audit nuage.

Si les armées françaises ont organisé un certain nombre de leurs systèmes d'information internes selon des techniques de nuage, ceux-ci sont à l'évidence très « privés » (« *Cloud* défense » mis en œuvre par la DIRISI – Direction interarmées des réseaux d'infrastructure et des systèmes d'information). Mais il s'agit là de la gestion des activités organiques, ayant lieu sur le territoire national pour le service courant. Le vrai défi de l'informatique en nuage concerne les opérations.

En effet, le combattant et les systèmes d'armes sont de plus en plus interconnectés, selon une dynamique qui ne va pas cesser (programme de Système d'information des armées -SIA-, ou encore programme Scorpion de l'armée de Terre et SICS associé). Ces Systèmes d'information opérationnels et de communication (SIOC) vont faire face aux mêmes contraintes que les grandes organisations civiles : augmentation des volumes d'information, mise en réseau des hommes, équipements et infrastructures, mobilité et réactivité des armées. C'est d'ailleurs tout le sens du combat collaboratif. La question du stockage et de l'échange de masses énormes de données suscite des défis techniques auxquels l'informatique en nuage peut répondre en partie.

Il s'agit de déployer des unités militaires dont chaque pion serait relié à l'ensemble de façon automatisée pour transmettre et recevoir des données tactiques. Un char rendrait compte automatiquement de ses consommations, tandis que le chef de char recevrait automatiquement l'ordre graphique de son chef direct qui s'afficherait directement dans son écran de cartographie. Cette philosophie serait évidemment égale entre pairs ou entre un niveau et un niveau immédiatement supérieur, mais il faut aussi prévoir que ces informations puissent potentiellement remonter (avec des processus d'agrégation et de simplification) toute la chaîne hiérarchique. Ainsi, la position du char doit indiquer celle du peloton, donc de l'escadron, donc du régiment, de la brigade, de la division… Les renseignements sur l'ennemi suivent les mêmes circuits avec les difficultés de pertinence : ce qui intéresse un chef de char (tel blindé ennemi se trouve à distance de tir dans telle direction) n'intéresse pas le colonel commandant le régiment qui se demande si ledit blindé est isolé, s'il marque l'avant-garde de l'ennemi ou son effort ? Il ne s'agit pas simplement de transmettre des volumes énormes de données, il faut aussi les traiter simultanément pour donner à chacun l'information (la donnée qualifiée) qui l'intéresse.

Techniquement, la technologie nuagique permet ceci puisqu'elle vise justement à profiter des effets d'échelle de calcul pour effectuer des travaux de *Big data* et d'intelligence artificielle.

## Obstacles et défis

Malheureusement, ce modèle rencontre des obstacles techniques : tout d'abord celui de la transmission des données qui suppose une bande passante épaisse et constante ; ensuite celui des calculateurs qui nécessitent à la fois le stockage de la donnée, mais aussi les processeurs suffisamment nombreux pour computer les données. Ajoutons les contraintes de confidentialité, de synchronisation, de traçabilité et d'intégrité et nous faisons face à des défis immenses, sans même parler des sources d'énergie, dimension qui est loin d'être neutre en opération.

# FRANCHIR LES OBSTACLES À L'ADOPTION DU *CLOUD* PAR LES ARMÉES

Construire un nuage privé en Opex, par exemple au milieu du désert, entraîne donc des difficultés immenses surtout si l'on envisage de tout contrôler, ce qui est le réflexe français. Faut-il plusieurs étages de *Cloud* ? Déployer une ferme de données de proximité et une en métropole ? Prévoir des systèmes asynchrones, permettant de fonctionner malgré l'absence de liaison ? Autant de questions qui restent ouvertes.

Or, la guerre en Ukraine apporte d'autres interrogations. Les militaires ukrainiens montrent qu'on peut tout à fait faire la guerre sans utiliser de systèmes d'information propriétaires avec classification de défense et chiffrement dédié. L'utilisation de moyens civils y est répandue. Que l'on pense ainsi au système satellitaire Starlink ou au développement d'applications de drones permettant d'observer et de guider ses propres moyens de feu. L'armée ukrainienne utilise ainsi un mélange de nuages privés tout en concentrant ses moyens propres à des usages dédiés, mais simplifiés. Cette hybridation de moyens militaires et de moyens civils (avec les usages et les procédures associées) peut mettre en cause notre conception de l'infonuagique militaire.

En effet, nous avons prévu notre combat collaboratif pour des effectifs réduits. Le retour de la guerre industrielle en Europe avec ses impératifs de masse peut mettre aussi en question ce modèle expéditionnaire. Un *Cloud* de combat taillé pour les opérations usuelles de l'armée française (taille maximale de 5 000 combattants) risque d'être inadapté aux conflits futurs, si la masse devient la norme.

Voici donc bien des contraintes associées au *Cloud* de combat. Cela ne signifie pas qu'elles sont insurmontables, simplement que cela nécessite des considérations techniques compliquées que les responsables doivent prendre en compte dans leurs facteurs de décision.

# DONNÉES ET APPLICATIONS SUR LE TERRAIN

CONTRIBUTEUR

**Joe BAGULEY**
**Vice-president & Chief Technology Officer EMEA**
VMWARE

Les premières images qui viennent à l'esprit dans l'imaginaire collectif lorsque l'on évoque les forces armées sont celles de soldats, d'armes et de véhicules militaires. Si ces éléments font bien partie intégrante de toute campagne militaire, d'autres composantes tout aussi essentielles ne peuvent être représentées et saisies visuellement. Il s'agit des communications, de l'information et de l'agilité.

En effet, dans une ère de forte dispersion des forces, de guerre hybride et de banalisation croissante des opérations offensives et défensives dans le domaine cyber, la capacité à déployer des innovations et des applications en temps réel sur le terrain est devenue un facteur décisif pour la victoire.

## Séparer les meilleurs des autres

Développer ces capacités de déploiement reste un défi d'envergure, et ce même pour les forces armées les plus avancées. En effet, sur le terrain, les unités doivent s'adapter à des situations évolutives, marquées par l'apparition régulière de nouvelles innovations dans des environnements en constante mutation. Dans le même temps, elles peuvent affronter des adversaires généralement de plus petite envergure, souvent plus agiles, mais disposant pourtant des mêmes outils et technologies.

Il peut être pertinent de comparer les armées avec des grandes entreprises privées, ou avec des institutions publiques, qui ont souvent un important héritage de méthodes et d'outils issu de leur longue histoire. Ces entités ont recours à des solutions et des processus faisant l'objet de longs cycles d'acquisition ou de partenariats historiques, qui ne sont peut-être plus adaptés mais dont il est difficile de se défaire. Le cycle d'évolution de ces organisations est tel que l'innovation progresse plus vite qu'elles.

Cette inertie est souvent liée à des couches de complexité organisationnelle et des silos de communication hermétiques qui ralentissent la diffusion d'informations et d'innovations là où elles seraient pourtant nécessaires. Les institutions militaires n'y échappent pas et aujourd'hui la façon dont ces problématiques sont gérées marque la différence entre les meilleures organisations des autres.

## Flux d'information des lignes arrières au front

Certains organismes militaires parviennent à déployer et à développer des applications, des systèmes et des processus qui facilitent la remontée des informations depuis l'intérieur vers les décideurs militaires. Ces entités se distinguent parce qu'elles réussissent là où la plupart échouent et parce qu'elles fonctionnent différemment.

Au sein de l'US Air Force, la division *Kessel Run*, qui met en œuvre une usine de logiciels évolutifs permettant de concevoir, fabriquer et exploiter des systèmes de *« Command & Control »*, en est un exemple. Un autre exemple est celui de *l'US Army Futures Command* - un programme de transformation continue et de modernisation de l'armée américaine fondé sur un partenariat public-privé et visant à doter les combattants de concepts et capacités innovants pour mener les guerres de demain.

Dans un autre registre, les forces armées doivent travailler en coalition - ce à quoi les organisations civiles ne sont pas confrontées. Ce cas de figure ajoute un niveau supplémentaire de complexité, car il implique que des forces alliées soient capables d'imbriquer leurs organisations respectives et de partager leurs ressources. Force est de constater que cette interopérabilité ne fonctionne pas forcément aujourd'hui.

## Le cercle de confiance

La principale raison de cet échec est que chaque force armée dispose de son propre *« SaaS » (System as a Service)*, ce qui crée une frontière entre deux nations. Historiquement, cela s'explique par des enjeux de souveraineté et de sécurité, mais dans un monde interconnecté, c'est un héritage qui implique que les membres d'une même coalition ne peuvent partager rapidement et efficacement leurs applications logicielles

respectives. C'est là que la confiance mutuelle joue un rôle vital. Elle garantit l'absence de compromission des informations.

La solution est d'instaurer un « cercle de confiance » qui intégrerait les *Clouds* de défense des QG généraux, les *Clouds* tactiques de combat à la périphérie et toutes les connexions avec les appareils et terminaux recueillant et traitant l'information entre ces *Clouds*. La condition essentielle est alors de s'assurer que chaque membre de la coalition partage les mêmes standards de sécurité, une compréhension commune de comment l'information est traitée ainsi qu'un degré de standardisation des données afin qu'elles puissent être exploitables et fiables.

Il s'agit d'un objectif manifestement plus facile à dire qu'à réaliser, mais les coalitions doivent travailler à l'instauration de ce cercle de confiance mutuelle sinon l'échec est inévitable.

## L'évolution du poste de commandement

La projection et la mobilité des différents composants d'une entité militaire sur le terrain constituent un défi supplémentaire. Traditionnellement, il faut environ une semaine pour déployer un poste de commandement tactique, avec son attirail de matériel informatique et de câbles, le tout dégageant de la chaleur. Dans le jargon militaire, c'est ce qu'on appelle une cible facile. Mais ici aussi, nous assistons à des innovations comme le projet Lelantos. Ce projet vise à développer des centres de données définis par logiciel *(software-defined data centers)* qui seraient ici des postes de commandement définis par logiciel. Ce dispositif, basé sur la virtualisation des ressources, peut être déployé et déplacé en quelques jours, ce qui réduit considérablement le niveau de vulnérabilité d'un poste de commandement.

## Optimiser l'architecture des systèmes d'information

Malgré cette innovation et bien d'autres, l'objectif de disposer d'un flux de données efficace disponible instantanément là où l'information est utile, n'est toujours pas atteint. Des données continues d'être perdues en chemin rendant l'ensemble du système inefficace. Les choses doivent changer. Les Alliés doivent se réunir pour optimiser les architectures de leurs systèmes d'information. C'est là qu'une stratégie *« multi-Cloud »* prendrait tout son sens. Elle apporterait de l'agilité, car c'est un moyen de faciliter l'interopérabilité, sans dépendre d'un seul fournisseur - ce qui ne sera jamais possible.

C'est là que les différents organismes militaires doivent réfléchir collectivement et dans un objectif commun. Elles doivent définir les normes et le format des informations, mais aussi avoir une perspective commune des données classifiées et non classifiées. Bien que des problèmes évidents subsistent, il est également clair que le défi auquel nous sommes confrontés au niveau de la communication et de l'information n'est pas qu'un problème technologique, mais aussi un problème d'organisation et de personnes. Et alors que les solutions abondent, aucune ne sera utile tant que les forces armées ne sauront pas tirer parti de la technologie et faire évoluer leurs doctrines.


Forward

vmware