VAUBAN PAPERS

[*CLOUD* ET OPÉRATIONS MILITAIRES :
DÉFIS ET OPPORTUNITÉS]

SÉRIE 2

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 Froward 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

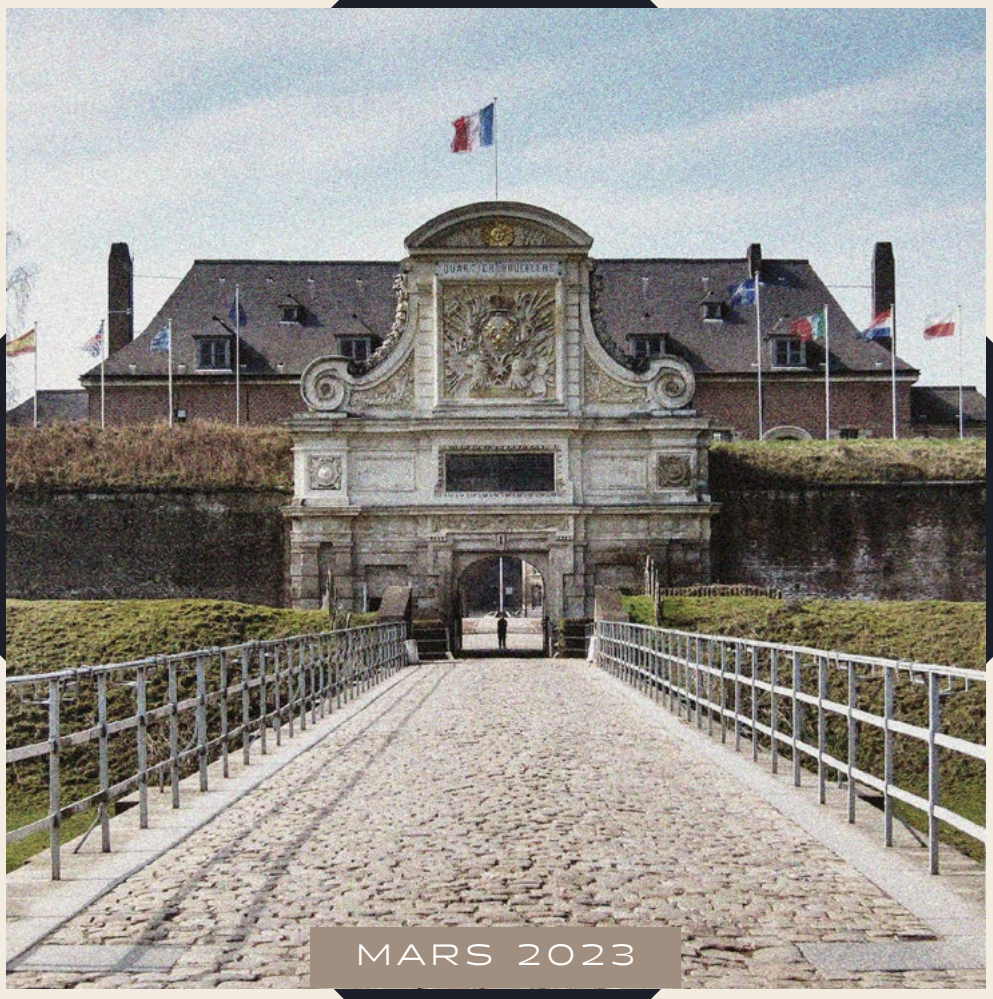
COLLECTION

VAUBAN PAPERS

SOMMAIRE

VAUBAN
SESSIONS

#5 MODÈLES DE SERVICES *CLOUD* POUR LA DÉFENSE



MARS 2023

Forward

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

PRÉFACE

Les « Vauban Papers » s'inscrivent dans une approche résolument opérationnelle de la transformation numérique. Dans ce sens, ils s'appuient sur « les rencontres Vauban » initiées par le Corps de Réaction Rapide - France de Lille et qui réunissent chaque année des commandeurs opérationnels, des autorités de l'UE aussi bien que de l'OTAN, des acteurs industriels du numérique ainsi que des décideurs étatiques. Les premiers opus des « Vauban Papers » se sont focalisés sur l'impact de la transformation numérique sur les opérations, au niveau des chefs aussi bien que celui de l'exécution, sur ses avantages et sur ses défis. Ils ont aussi permis de mettre en évidence la nécessité d'un travail collaboratif incrémental entre opérationnels, services experts et sociétés motrices du numérique à même de mettre au service des forces armées le meilleur des nouvelles technologies. Sans surprise, il est clairement apparu au fil des échanges et réflexions que l'exploitation des innombrables données opérationnelles quelle qu'en soit l'origine constitue pour les forces armées à la fois la clé et l'objectif stratégique de leur transformation numérique. Dès lors, se pose la question de la localisation de ces gigantesques bases de données. Pour répondre à cette « problématique » cruciale, une approche purement technique ne saurait se suffire à elle-même, cependant les nouvelles technologies du numérique, en particulier *« le Cloud computing »*, ouvrent des horizons prometteurs. Il convient en premier lieu de poser les principes essentiels auxquels doit répondre la localisation, l'exploitation et la diffusion des données opérationnelles. Sans être exhaustif, on peut citer la souveraineté qui n'exclue pas le partage sélectif au sein d'une organisation collective (UE, OTAN…) ou d'une coalition, l'accessibilité et la disponibilité quasi instantanée, la fiabilité et son corollaire, la résilience. À l'évidence, les systèmes d'information actuels par nature très centralisés et très spécialisés ne répondent pas à la question. Cependant, certaines évolutions des réseaux de liaison de données tactiques (Liaison 16 par exemple) ont ouvert la voie à une connectivité élargie qui constitue une première étape vers le graal opérationnel que constituerait le *« combat Cloud »*. Comme présenté dans le corps de ce Vauban Paper, aucune solution magique ne s'impose aujourd'hui que ce soit le *Cloud* privé, le *Cloud* public voire le *Cloud* hybride, ou les différents niveaux de service à la demande qui permettraient le traitement, le partage et le stockage des données : mise à disposition d'applications partagée, *Software as a service* (SaaS), d'infrastructures informatiques hébergées sur le *Cloud, Infrastructure as a service* (IaaS) ou carrément de plateformes complètes prêtes à l'emploi, *Platform as a Service* (PaaS). Une évolution en cours dans la gestion des données jouera un rôle important dans ces choix, l'avènement de l' *« Edge computing »* va permettre de traiter une partie des données opérationnelles au plus près des combattants. On le voit, le *Cloud*, qui a désormais atteint un haut niveau de maturité dans les activités civiles, s'invite désormais au cœur des systèmes opérationnels comme un élément essentiel de la bataille cognitive, de l'accélération des boucles décisionnelles, de l'optimisation de l'ensemble des capacités mises en œuvre dans les différents milieux et les différents domaines de lutte.

Cette nouvelle série des Vauban Papers vise à aider les décideurs opérationnels à définir, en collaboration avec les acteurs de l'espace numérique, les solutions les plus à même de satisfaire les besoins exigeants qu'impose le nouveau contexte géostratégique. Pour les forces armées, la transformation numérique n'est désormais plus une option, c'est un impératif pour garantir leur liberté d'action et leur efficacité opérationnelle.

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

MODÈLES DE SERVICES *CLOUD* POUR LA DÉFENSE

CONTRIBUTEURS

Axel DYÈVRE
Associé
FORWARD GLOBAL

Marie KETTERLIN
Analyste
FORWARD GLOBAL

Depuis le milieu des années 2000, les appareils et terminaux connectés *(Internet of Things, IoT)* se sont multipliés. La transformation numérique, couplée à l'augmentation des débits des réseaux, s'est traduite par l'inclusion progressive de ces objets connectés dans la conduite opérationnelle des forces armées. Ces équipements représentent de fait un avantage opérationnel conséquent : l'échange d'informations à tous les niveaux et en « quasi-temps réel » permet de raccourcir, *in fine*, la boucle décisionnelle, et de déployer un modèle de combat collaboratif. Les appareils connectés générant des données (par action humaine ou automatiquement), les volumes de données échangées sur les réseaux via ces terminaux connectés ont explosé.

Dans ce contexte, les forces armées sont aujourd'hui confrontées à un **enjeu de connectivité** à deux dimensions. Les **volumes de données** produites et utilisées sur le terrain sont décuplés, rendant l'enjeu de leur échange - et donc, l'accès aux réseaux - crucial. Par exemple, les besoins de « discrétion visuelle » et de réduction de l'empreinte électromagnétique des échanges radiophoniques participent au développement des échanges de données en réseau. De plus, les missions prennent place dans des **conditions généralement dégradées,** marquées par une difficulté d'accès aux réseaux, du fait de l'action de l'adversaire, mais également des contraintes de terrain. Afin d'éviter les dysfonctionnements liés à la latence des réseaux, les unités doivent être en mesure de travailler « connectées » et « déconnectées », selon des solutions de connexion plus ou moins localisées.

Cet objectif repose sur trois conditions : le besoin de puissance, la capacité de stockage et la répartition des ressources.

Le cadre défini par ces différents éléments n'est ainsi plus favorable à un seul fonctionnement « en local » : il n'est désormais plus possible pour les forces armées de reposer uniquement sur l'utilisation des ressources stockées dans les terminaux déployés sur le terrain. Le fonctionnement ***« en Cloud »*** apparaît comme une solution intéressante, définie par **l'hébergement à distance** des données et des applications.

Se déclinant en **différentes architectures,** le *Cloud* propose des **services** variables :

- Dans une architecture de *Cloud* public, les ressources sont hébergées sur le serveur d'un fournisseur, partagé avec d'autres utilisateurs. Ces ressources sont disponibles à la demande via Internet, pour leurs propriétaires et leurs invités.
- Le *Cloud* privé repose sur le stockage de données sur une architecture de serveurs réservée à l'usage exclusif d'une seule organisation, hébergée par l'organisation elle-même - sur son réseau ou via internet par VPN ou tunnel - ou hébergée par un tiers. Le *Cloud* privé présente des avantages en termes de contrôle, de protection et de confidentialité des données et applications hébergées. Cette architecture, plus coûteuse que le *Cloud* public, est principalement mise en œuvre par des organisations de très grande taille.
- Le *Cloud* hybride vise à combiner des infrastructures de *Cloud* privées et publiques : une partie de l'architecture *Cloud* est physiquement hébergée dans les locaux de l'organisation, l'autre partie se trouvant chez un ou plusieurs prestataires extérieurs. Les données et applications sont ensuite réparties en fonction de leur sensibilité ou de l'importance de leur disponibilité. Le *Cloud* hybride combine les avantages en termes de coûts et d'évolutivité des *Clouds* publics d'une part et la sécurité d'un *Cloud* privé d'autre part.

Une architecture *Cloud* peut également être déployée autour de **plusieurs services de *« Cloud computing »***, c'est-à-dire, l'accès à la demande, via Internet, à des ressources informatiques comme par exemple la puissance de calcul et la capacité de stockage — provenant de différents fournisseurs : il s'agit alors d'une structure ***« Multi-Cloud »***. Chaque architecture repose sur la combinaison unique de *Clouds* (publics et/ou privés). Les contenus, données, logiciels et applications sont alors répartis entre les différents serveurs.

MODÈLES DE SERVICES *CLOUD* POUR LA DÉFENSE

Pour raccourcir les temps de réponse et/ou économiser de la bande passante, l' ***« Edge computing »*** propose une architecture d'informatique distribuée rapprochant le calcul et le stockage des sources de données - via les appareils connectés ou l'usage de serveurs locaux.

Ces architectures de réseau permettent *in fine* de **distribuer** ces masses de données, de **s'appuyer sur des applications ou de la puissance de calcul** « externes » à partir d'un appareil local connecté en réseau.

Le déploiement des forces armées vers des **théâtres éloignés et dans des intervalles de temps toujours plus réduits** rend nécessaire le raccourcissement de la boucle informationnelle dans des environnements et contextes d'opération dégradés. Pour ce faire, le partage, le traitement et le stockage de l'information doivent devenir un service quasi « sur-mesure », « à la demande », adapté aux procédures et aux conditions du terrain. Le *Cloud*, pouvant être déployé selon **trois niveaux d'intervention,** offre des possibilités de communication et de partage de l'information :

- **Application :** le « logiciel en tant que service » *(Software as a service,* ***SaaS****)* est un modèle de distribution de logiciels dans lequel un fournisseur de *Cloud* héberge des applications et les met à la disposition des utilisateurs via Internet - généralement via un navigateur - suivant un modèle d'abonnement payant. Dans ce modèle de « logiciel à la demande » le fournisseur donne aux clients un accès en réseau à une copie unique d'une application. Les données du client peuvent être stockées localement, dans le *Cloud*, ou à la fois localement et dans le *Cloud.*

- **Infrastructure :** l' « infrastructure en tant que service » *(Infrastructure as a service,* ***IaaS****)* garantit un accès à la demande à une infrastructure informatique hébergée sur le *Cloud* - serveurs, capacité de stockage et ressources réseau - que les clients peuvent approvisionner, configurer et utiliser, tandis que le fournisseur de services *Cloud* héberge, gère et entretient le matériel et les ressources informatiques dans ses propres centres de données. Les utilisateurs de *l'IaaS* utilisent le matériel via une connexion Internet et paient pour cette utilisation sur la base d'un abonnement.

- **Plateforme :** la « plateforme en tant que service » *(Platform as a service,* ***PaaS****)* garantit un accès à la demande à une plateforme complète, prête à l'emploi, hébergée sur le *Cloud*, pour développer, exécuter, maintenir et gérer des applications. Le fournisseur de services *Cloud* héberge, gère et entretient tout le matériel et les logiciels inclus dans la plateforme - serveurs, système d'exploitation, stockage, mise en réseau, bases de données - ainsi que les services associés pour la sécurité.

Pour les forces armées, ces technologies et leurs usages comportent **plusieurs enjeux**, à commencer par l'enjeu du **fonctionnement « en *Cloud* »**, qui est avant tout d'assurer une **bonne répartition** des ressources informatiques entre les différents niveaux afin de garantir la disponibilité, la résilience et l'autonomie possible de chaque niveau. Cette question comprend celle, subsidiaire, du **stockage matériel** des machines. L'infrastructure physique de l'architecture *Cloud* peut être hébergée au sein de l'organisation qui l'utilise (privée, publique) et déployée par ses propres réseaux. Cette solution est particulièrement coûteuse : le *Cloud* reposant sur un besoin de connectivité, de disponibilité et de redondance en termes de sécurité, ce qui est à la fois coûteux et compliqué à mettre en œuvre. Le *Cloud* hybride permet de gérer les données et leur répartition, entre « interne » et « externe ». Une architecture *« Multi-Cloud »* permet, elle, d'assurer une répartition des données à un niveau élevé de sécurité, rendant la reconstruction quasi-impossible en cas d'attaque. Cependant, tout avantage créant une dépendance, ces architectures (hybride, *« Multi-Cloud »*) augmentent la dépendance aux réseaux.

MODÈLES DE SERVICES *CLOUD* POUR LA DÉFENSE

L'enjeu opérationnel central de l'usage du *Cloud* pour la défense est de **raccourcir la boucle décisionnelle**. L'échange de données et le recours à des services de traitement des données en réseau permettent, en principe, d'améliorer le combat en réseau en reliant les entités qui composent l'architecture de combat collaboratif. Les technologies *Cloud* permettent de partager la situation le plus rapidement et le plus précisément possible, assurent une meilleure compréhension de l'environnement *(situation assessment)* et ainsi une meilleure coordination des feux pour, *in fine*, participer à une accélération de la manœuvre.

MODÈLES DE SERVICES *CLOUD* POUR LA DÉFENSE

CONTRIBUTEUR

Général de division (2S), Sully BARBE
ancien chef de la division systèmes d'information et de communication et cyberdéfense du quartier général
CORPS DE RÉACTION RAPIDE - FRANCE

Définie comme la capacité à collecter, traiter, diffuser un flux d'information continu, exploiter celui d'un adversaire ou l'en priver, la suprématie informationnelle facilite la supériorité opérationnelle. Les informations proviennent de la corrélation des données produites par différentes sources ou capteurs, textes, chiffres ou un mélange des deux, mais aussi de tableaux, de graphiques. Converties en connaissance et décision, elles procurent un avantage à une force apte, par ailleurs, à combiner ses effets traditionnels et ceux des champs immatériels.

La maitrise du « *Cloud computing* », de l'intelligence artificielle et du « *big data* », offre cette capacité de transformation. Communauté de ressources partageables selon les besoins des utilisateurs et consommables à la demande, le *Cloud* permet de disposer de moyens plus importants, et d'une puissance de calcul quasi illimitée. Il constitue un objectif primordial pour les armées modernes. Elles sauront ainsi, stocker, gérer et exploiter le volume exponentiel de données produites par leurs plateformes de combat, les objets qui y sont connectés, et l'environnement dans lequel elles accomplissent leurs missions. Elles bénéficieront des outils performants nécessaires au traitement de ces informations par des algorithmes, dans des délais compatibles avec le rythme des opérations du niveau stratégique ou tactique.

Les projets de *Cloud* en cours de réalisation dans les Armées françaises se déclinent par niveaux :

- **Central** (noyau, en métropole), constitué d'un *Cloud* privé et d'un *Cloud* public, pour héberger des applications et des données « métier » des armées, directions et services français.
- **Local** ou « *edge* », qui font relais en métropole ou en entrée de théâtre, outre-mer ou sur les bâtiments de la Marine nationale française. Ils seront développés avec des technologies *Cloud* classiques durcies, adaptées à l'environnement tactique (température, poussière, chocs) et bénéficiant de débits suffisants mais limités.
- **De combat** ou « *far edge* », qui nécessitent des technologies spécifiques (« *fog computing* »[1]) et des capacités distribuées dans les systèmes d'armes qui sont mis en œuvre dans un contexte de connectivité intermittente.

S'inscrivant dans ce concept, l'armée de Terre française développe un *Cloud* de combat terrestre. Véritable système nerveux et mémoire collective, il sera capable de partager et de fusionner l'information au profit des postes de commandement et des unités tactiques, qui pourront partager une image commune des opérations et être en mesure de voir toutes les données opérationnelles qui sont nécessaires pour leur mission. Le souhait est de démultiplier les effets tactiques par l'amélioration du combat collaboratif et d'améliorer l'agilité du commandement par l'aide apportée pour la planification et à la décision. En outre, il est à noter qu'il s'agira encore d'utiliser cette technologie pour assurer l'appui au commandement et aux opérations par des fonctions en « *reachback* », celles requérant, en particulier des expertises techniques de haut niveau. Enfin, la technologie du *Cloud* permettra aussi d'améliorer le maintien en condition des équipements (MCO prédictif), et plus en amont la définition des capacités futures de l'armée de Terre par la capacité à analyser des volumes importants de données.

Assurer la sécurité du *Cloud* est indispensable pour la sécurité numérique de la force. Dans les phases de conception et de réalisation, une approche systémique et une intégration continue de la sécurité dans les projets et programmes sont nécessaires. Une consolidation des structures de gouvernance, une généralisation de l'analyse de risques et les efforts entrepris auprès des instances pour que la conformité réglementaire prenne mieux en considération la réalité des engagements terrestres doivent être poursuivis.

1. Approche combinée selon 3 axes, l'aspect statique qui met en évidence la structure du système, sa composition, ses éléments et leurs relations structurelles, l'aspect dynamique qui met en évidence l'évolution du système au cours du temps, et l'aspect fonctionnel met en évidence les traitements réalisés, les calculs du système.

MODÈLES DE SERVICES *CLOUD* POUR LA DÉFENSE

D'un point de vue technique, la sécurité du *Cloud* repose sur la sécurité des données et des applications hébergées et du réseau. Les études réalisées sur ce sujet montrent que l'atteinte à la confidentialité des données est souvent liée à des erreurs humaines de configuration ou des attaques ciblées. Ces dernières sont possibles quand des droits excessifs sont attribués à un administrateur, qui peut accéder à des informations confidentielles ou données critiques ; soit avec des identifiants volés avec lesquels les attaquants peuvent accéder à des zones critiques des services *Cloud* ou effectuer des vols d'informations.

Sur l'intégrité des données, des identités et des accès mal gérés peuvent permettre à un utilisateur non autorisé d'accéder aux données internes. Un cyber-attaquant pourrait aussi parvenir à usurper l'identité d'utilisateurs légitimes, pour lire, modifier ces données ou pour intercepter des transactions et renvoyer des informations falsifiées ou/et rediriger les utilisateurs vers des sites illicites.

Sur la disponibilité des données, une attaque DDOS[2] sur les services peut empêcher les utilisateurs d'accéder à leurs données. Une infection par un logiciel malveillant peut paralyser ou détruire l'infrastructure du *Cloud*, en forçant un service à surconsommer des ressources comme la puissance de traitement ou la mémoire, est possible. Ces attaques peuvent aussi provoquer un ralentissement des systèmes utilisateurs légitimes par la saturation de la bande passante, ou les rendre inaccessibles. Enfin, une suppression accidentelle de service par le fournisseur, due à une catastrophe naturelle ou un incendie, peut entraîner une perte définitive de données.

Sur les applications, l'architecture technique du *Cloud* repose sur la virtualisation, les micro-services et les interfaces de programmation des applications (API)[3]. Méthode privilégiée de création d'applications modernes, en particulier pour les appareils mobiles et l'Internet des objets, ces API peuvent être le vecteur de code malveillant si leur intégrité n'est pas contrôlée.

Enfin, une atteinte à la disponibilité des réseaux est un risque important et probable. Il peut être provoqué par une attaque visant à saturer la bande passante, brouiller les communications, ou par une panne matérielle ou une mauvaise gestion de la qualité de services. Il est à noter que la « 5G » conçue en particulier pour les objets connectés, définie par logiciel et utilisant le langage commun et les protocoles Internet, présente un risque supplémentaire d'attaque que les réseaux de génération précédente. Il est évident que cette liste n'est pas exhaustive, et ces risques d'attaque doivent être adaptés à l'environnement dans lequel le *Cloud* est utilisé.

Pour répondre à ces besoins de sécurité, les actions préconisées pour le *Cloud* consistent à adopter une approche *« data centric »*[4]. Elle vise à fiabiliser les données pour améliorer leur traitement dans les services du *Cloud*, à automatiser les services de sécurité afin de réduire les besoins en personnel, de diminuer le temps de réponse aux menaces. Ces actions visent en outre à faciliter la corrélation et l'agrégation de tous les flux de données afin de soutenir la défense en profondeur et à générer des informations facilement compréhensibles et exploitables pour les administrateurs et les opérateurs de sécurité. En complément, la mise en œuvre d'une architecture *« zero trust »* est souvent préconisée. C'est un concept qui exige un accès sécurisé et authentifié à toutes les ressources, selon le principe du moindre privilège. Il comprend aussi une surveillance continue (en temps réel) du système d'information de l'entreprise (y compris de tous les appareils connectés), et un audit régulier des données stockées.

Pour les armées, une grande partie de la sécurité du *Cloud* des armées devra être prise en compte dans les phases amont des programmes ou projets. Les études et analyses visant

2. DDOS : Une attaque par déni de service (abr. DoS attack pour *Denial* of *Service attack* en anglais) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (abr. *DDoS attack* pour *Distributed Denial of Service attack*).
3. API : L'API est une solution informatique qui permet à des applications de communiquer entre elles et de s'échanger mutuellement des services ou des données.
4. Approche *« data centric »* : vision unifiée et intégrée des données modélisées et gérées de manière centralisée pour toute l'entreprise.

à définir les actifs (données processus, équipements, personnels…) à protéger, détecter les vulnérabilités intrinsèques et les menaces générales, déterminer l'environnement des prestataires, fournisseurs et partenaires, et définir les chemins d'attaques potentiels, permettront de remédier aux risques les plus critiques. Par ailleurs, même s'il présente une surface d'attaques importante compte tenu du nombre important des parties prenantes du système d'information, l'occurrence d'une attaque courante est limitée compte tenu de sa faible exposition directe à Internet.

Le risque peut résider dans une attaque complexe intervenant sur les fonctions d'appui ou de soutien connectées à leurs fournisseurs et prestataires pour lesquels une analyse de la maturité cyber n'est pas toujours possible. Il peut aussi découler d'une attaque visant les infrastructures, ou les réseaux, et rendant indisponibles les ressources du *Cloud*. D'autres attaques peuvent être menées par des groupes APT, soutenus par des États et ayant les capacités à trouver des vulnérabilités *« zero-day »*, infiltrer et compromettre les systèmes les plus protégés. Leur dangerosité réside aussi dans leur capacité à s'adapter aux mesures de sécurité, et à se déplacer discrètement sur les réseaux du centre de données pour atteindre leurs objectifs.

Dans le cadre d'un engagement potentiel au sein d'une coalition multinationale, la maturité cyber des partenaires doit être évaluée. Pour des besoins d'interopérabilité, leurs accès au(x) *Cloud(s)* qui centralisent des données doivent être étudiés en tenant compte des exigences de sécurité et des impératifs, à plus long terme, de souveraineté.

La sécurité du *Cloud* demande une expertise de haut niveau des opérateurs externes et internes de *Cloud*. Ils doivent être capables de maitriser des domaines d'expertise comme la gestion des identités et des accès, la sécurité des objets connectés, la sécurité des données, ou la mise en place de plan de résilience. Sinon, le risque de perte de maîtrise du système d'information est important, et il sera alors difficile d'acquérir une supériorité informationnelle sur le champ de bataille.

Pour une sécurité numérique efficace en opération, le *Cloud* peut impliquer une simplification des architectures techniques, et faciliter ainsi leur protection, mais celle-ci ne modifie pas fondamentalement la démarche à adopter. Les mécanismes techniques de sécurité implémentés dans les plateformes doivent être complétés par la mise en œuvre des structures adaptées de sécurité opérationnelle. Elles doivent pouvoir suivre l'évolution des menaces et prendre les mesures pour corriger les vulnérabilités résiduelles, protéger la force, anticiper et détecter les attaques, réagir si nécessaire. De même, une sensibilisation au risque cyber des utilisateurs de ces systèmes de combat modernes, doit être accrue. Les actes élémentaires de sécurité du soldat utilisateur des systèmes d'armes doivent rester faciles à mettre en œuvre. Enfin, la résilience aux attaques cyber doit être développée par l'entraînement à la gestion de crise cyber, et à la poursuite des opérations dans un mode de services dégradé, en attendant leur restauration par les unités compétentes.

5. *APT : Advanced Persistent Threat.*
6. *Zero-day vulnerabilty :* Dans le domaine de la sécurité informatique, une faille/vulnérabilité *zero-day* est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. L'existence d'une telle faille sur un produit informatique implique qu'aucune protection n'existe, qu'elle soit palliative ou définitive.

LE CHAMP DE BATAILLE INTÉGRÉ

PLANIFIER POUR DES MILLIARDS DE CHOSES

CONTRIBUTEUR

Joe BAGULEY
Vice-president & Chief Technology Officer EMEA
VMWARE

« Toujours prêt » est la devise de tous les scouts. Elle reste applicable dans tous les domaines de la vie, longtemps après l'enfance. C'est particulièrement vrai dans l'armée, où les situations et les circonstances peuvent varier rapidement et de façon spectaculaire, et où les forces armées sont dans une course sans fin pour garder une longueur d'avance sur leurs adversaires. Cela me rappelle les « P » que l'on m'a enseignés lorsque j'étais jeune officier : « La préparation et la planification préalables prémunissent d'une piètre performance ».

Les forces armées doivent adopter ce qui est à la pointe du progrès aujourd'hui afin d'anticiper les années à venir lorsque les innovations, processus et technologies émergeant aujourd'hui seront devenus courants. L'Internet des objets *(IoT)* en est la meilleure preuve.

L'accélération technologique

Ce domaine technologique est un très bon exemple de l'accélération technologique et de la manière dont les armées peuvent agir ou se laisser distancer. La raison pour laquelle *l'IoT* est un concept si pertinent est que la technologie sous-jacente n'est pas nouvelle. En 2016, le laboratoire de l'armée de Terre américaine (ARL) a créé le projet *« Internet of Battlefield Things »* (pour Internet des objets du champ de bataille). Il s'agissait d'une réponse au schéma opérationnel de l'armée américaine sur la période 2020 à 2040, intitulé « Gagner dans un monde complexe », qui mettait l'accent sur le défi de garder la cadence face aux avancées technologiques des adversaires potentiels. Il existe des exemples similaires dans des pays du monde entier.

Nous voyons maintenant la théorie se concrétiser. Le ministère israélien de la Défense a récemment annoncé qu'il commencerait les essais d'un véhicule de combat robotique sans pilote, baptisé M-RCV (*Medium Robotic Combat Vehicle*), en 2023.

De toute évidence, le concept de connectivité est déjà bien établi. Mais la raison pour laquelle il doit rester au centre des préoccupations des forces armées est l'accélération du changement technologique et l'ampleur qu'il peut potentiellement atteindre - la taille du marché mondial de *l'IoT* militaire devrait atteindre 16 080 millions de dollars d'ici 2026, contre 10 620 millions de dollars en 2019 selon *Industry research*.

Un champ de bataille mondialement connecté

Si vous pensez que *l'IoT* et la connectivité ont totalement imprégné le milieu militaire, c'est que vous n'avez encore rien vu. Le nombre d'appareils connectés augmente rapidement et continue de croître. Les systèmes cyber-physiques - des systèmes embarqués plus grands et contrôlés par des algorithmes, comme les véhicules autonomes et les jumeaux numériques - prolifèrent et nous entrons dans une ère de connectivité totale.

Il ne s'agira pas simplement d'outils ou d'équipements particuliers, mais de tous les éléments du combat. Les fusils seront connectés aux individus qui les brandissent, qui seront connectés aux dépôts d'armes et aux outils de mesure de données vitales, etc. Il s'agira de passer de la gestion de centaines ou de milliers de terminaux à des milliards dans un champ de bataille interconnecté à l'échelle mondiale.

S'il subsiste encore un doute sur le fait que cet avenir se rapproche rapidement, il suffit de regarder ce qui se passe en Ukraine. Cette guerre se déroule sur le terrain des communications et des réseaux, comme en témoigne l'efficacité de Starlink, un système de communication par satellite déployé par la société SpaceX d'Elon Musk. Ce système a permis de maintenir la transmission de l'information, permettant de garder les hôpitaux connectés et servant de liaison avec les drones repérant les cibles russes pour l'artillerie ukrainienne. La force de reconnaissance aérienne de l'Ukraine a utilisé Starlink pour se connecter directement aux drones qui ont mis hors d'état de nuire de nombreux chars, centres de commandement mobiles et autres véhicules militaires russes.

Encourager les innovations de demain

Internet d'aujourd'hui est conçu pour permettre la communication de serveur à serveur entre centres de données ou *Clouds*, qui sont généralement situés dans des zones reculées, où l'immobilier et l'électricité sont facilement disponibles et peu coûteux. Le problème de cette architecture est qu'elle ne prend pas efficacement en charge la périphérie du réseau, là où se trouvent les utilisateurs et les objets. Pour les forces armées, les applications doivent pouvoir placer intelligemment les instances des applications et les données aux bons endroits afin d'optimiser les performances, l'expérience et les coûts.

Malheureusement, les réseaux d'aujourd'hui sont encore trop limités pour permettre le développement des innovations de demain. Les frontières entre les réseaux, les fournisseurs de *Cloud*, les fabricants, les télécoms et le stockage sont relativement claires aujourd'hui, mais tout cela va changer à mesure que la connectivité deviendra omniprésente - les chevauchements deviendront plus importants et vous ne pourrez plus faire la différence entre un opérateur de réseau, de *Cloud* ou un fournisseur informatique. Les chefs militaires doivent commencer à anticiper cela dès maintenant afin que, lorsque de plus en plus d'éléments seront connectés, ils ne retrouvent pas limités par les capacités ou les architectures de systèmes. C'est pourquoi il est essentiel d'appréhender la 6G dès maintenant.

Un avenir avec la 6G

Certains experts pensent que les réseaux 6G pourraient un jour nous permettre d'atteindre la vitesse d'un térabit par seconde (To/s) sur un appareil connecté. C'est mille fois plus rapide que 1 Go/s, le débit le plus rapide disponible sur la plupart des réseaux Internet domestiques aujourd'hui. Dans un contexte militaire, ce sera le fondement d'applications telles que les véhicules autonomes, la communication holographique et le soldat connecté.

Ces visions se concrétiseront lorsque la connexion deviendra aussi courante, abondante et transparente que l'air que nous respirons. C'est pourquoi VMware est un partenaire fondateur de *l'Open Grid Alliance* (OGA). Cette initiative rassemble les acteurs à la pointe du secteur. Elle a pour but de mettre en avant un programme et un ensemble de principes directeurs pour la formation d'un réseau ouvert *(Open Grid)* étendu à travers le monde, capable prendre en charge des services *multi-Clouds* à la demande via des ressources fongibles employées quand, et où elles sont nécessaires. Il combine de nombreuses technologies et de nombreux fournisseurs travaillant ensemble dans un cadre neutre où tous les participants peuvent bénéficier des contributions de chacun, tandis que les parties prenantes individuelles peuvent innover de manière unique et différenciée. Il s'agit d'une vision plus démocratique et décentralisée des architectures de réseau futures.

Les « I » de l'équipe

Indépendamment de ces développements, il n'existe pas de formule magique pour les armées. Le monde évolue si rapidement que même le plus ardent technologue ne peut que spéculer sur ce que seront les futures normes d'interopérabilité. C'est à la fois une opportunité et un défi : s'assurer que tout fonctionnera avec tout.

Pour un secteur qui repose sur le travail d'équipe, l'avenir des forces armées est confronté à de nombreux « I » : interopérabilité, interconnectivité et informations disponibles instantanément. Mais pour gagner demain, il faut se préparer dès maintenant. Si les forces armées ne commencent pas à planifier la construction d'architectures de réseau capables de gérer des milliards d'objets connectés, elles échoueront à l'avenir.

VAUBAN
SESSIONS

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

MARS 2023

Forward

VAUBAN-SESSIONS.ORG

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.

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.

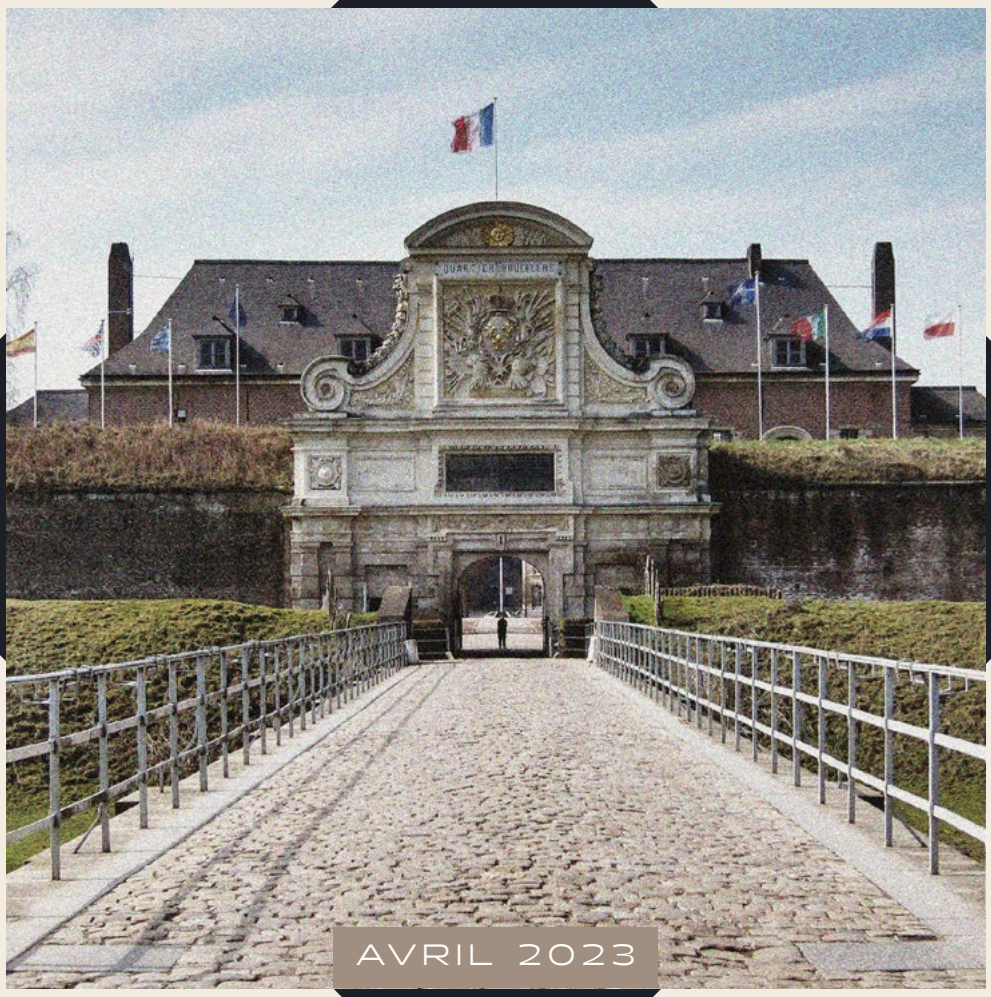
Optimiser l'architecture des systèmes d'information

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.

VAUBAN
SESSIONS

#7 APPORTS DU *CLOUD* AU FONCTIONNEMENT DES C2 : CONCILIER TECHNOLOGIE COLLABORATIVE ET PERFORMANCE DU COMMANDEMENT



AVRIL 2023

Forward

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

PRÉFACE

L'art du commandement dans ses grands principes n'a pas fondamentalement évolué depuis que Sun Tzu l'a clairement exprimé dans son « Art de la guerre ». Ainsi, l'anticipation, la préparation et l'entraînement, la connaissance et le renseignement, la distribution des responsabilités et la délégation d'autorité ou encore la résilience, pour ne citer que quelques-uns de ses commandements, demeurent particulièrement pertinents dans la gestion des crises, la conduite des opérations modernes et singulièrement dans le cadre de la guerre en Ukraine. Aujourd'hui, dans chacun de ces domaines, l'homme tient plus que jamais une place essentielle, même si l'évolution rapide des moyens techniques à sa disposition, en particulier dans le domaine numérique, peut donner l'illusion d'une possible automatisation des processus de décision, voire d'exécution.

Bien au contraire, la transformation numérique des forces armées, pour porter tous ses bénéfices, doit intimement associer tous les acteurs de la chaîne opérationnelle, comme l'a souligné la série de « Vauban Papers » parus à ce jour. Les fonctions de Commandement et Contrôle (C2) qui constituent le véritable système nerveux de cette chaîne sont au cœur de cette transformation numérique opérationnelle. Elles peuvent désormais bénéficier de flux de données massifs et continus qu'il convient de gérer, de filtrer, de classer, d'exploiter, d'échanger et de stocker. Le *Cloud computing*, grâce à son potentiel d'accès et de traitement à distance, représente une solution déjà éprouvée dans le monde civil et dans les entreprises, certaines armées l'ont déjà adopté en l'adaptant à leurs besoins. En la matière, le partage d'expérience et des meilleures pratiques constitue à la fois un axe de progrès et d'interopérabilité. En effet, l'adoption du *Cloud computing* au sein des chaînes opérationnelles offre un remarquable potentiel d'accélération de la boucle décision/action en permettant l'accès aux données pertinentes à chacun des niveaux, de la décision à l'exécution et en offrant à tous une vision commune de la situation opérationnelle. Le *Cloud computing* se présente dès lors comme un élément constitutif du combat collaboratif multi-domaines. La mise en œuvre du « *Cloud* » dans les structures de commandement et contrôle doit tout d'abord donner lieu à une analyse exhaustive des processus d'échange et de stockage de données opérationnelles pré-existants. Cela doit conduire en particulier à une nouvelle approche des niveaux de confidentialité de ces données, tels qu'évoqués dans le « Vauban Paper 6 : Contraintes et enjeux du *Cloud* » pour assurer la meilleure fluidité des échanges tout au long de la chaîne des opérations, qu'elles soient purement nationales, interalliées (OTAN, UE) ou au sein d'une coalition *ad hoc*. L'adoption du *Cloud* doit en fait ouvrir la voie à une nouvelle dynamique dans le commandement et la conduite des opérations. Il ne s'agit pas de mettre en cause le besoin d'un niveau de commandement centralisé à même de mettre en œuvre des stratégies militaires cohérentes et efficaces. Tout au contraire, l'objectif est bien de permettre aux décideurs opérationnels de déléguer l'autorité d'engagement au niveau le plus approprié de la chaîne en s'assurant que celui-ci dispose des informations les plus pertinentes pour assurer cette responsabilité. Ainsi, tout en accélérant la boucle décisionnelle *Observe-Orient-Decide-Act* (OODA *loop*) le *Cloud* de combat vise aussi à fiabiliser et à organiser en temps réel toutes les données qui contribuent à son efficacité.

La maîtrise des données opérationnelles est plus que jamais un enjeu stratégique, opératif et tactique. Le *Cloud* présente en la matière un potentiel exceptionnel, il ne saurait cependant se substituer à l'expérience et à la compétence des différents acteurs de la chaîne opérationnelle, bien au contraire, il doit permettre de valoriser l'art du commandement et celui de l'exécution dans une vision très dynamique des opérations modernes, c'est tout l'intérêt de ce septième « Vauban Paper ».

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

APPORTS DU *CLOUD* AU FONCTIONNEMENT DES C2 : CONCILIER TECHNOLOGIE COLLABORATIVE ET PERFORMANCE DU COMMANDEMENT

CONTRIBUTEURS

Axel DYÈVRE
Associé
FORWARD GLOBAL

Martin DE MAUPEOU
Directeur
FORWARD GLOBAL

Marin MESSY
Analyste
FORWARD GLOBAL

L'OTAN définit le commandement et la conduite des opérations (C2) comme « *l'ensemble des fonctions des commandeurs, de leurs équipes et autres corps de commandement pour le maintien des forces, la préparation des opérations et la direction des troupes en vue de leurs missions* ». Désignant le processus décisionnel, la capacité à diriger et des systèmes d'information et de communication, le C2 permet de planifier, programmer et conduire les opérations du plus haut niveau stratégique au dernier niveau tactique, en tenant compte des évolutions sur le théâtre.

Les évolutions des moyens de communication ont une grande influence sur le C2. La numérisation en cours des armées implique une massification du volume des données opérationnelles et techniques générées. Dans ce contexte, la performance du C2 repose sur la capacité permanente d'acquérir, de communiquer, de traiter puis de synthétiser à l'échelon pertinent l'information. Capacité qui repose elle-même sur les moyens nécessaires pour produire, recevoir, stocker et transmettre plus rapidement que l'adversaire, informations et ordres.

Les plus-values opérationnelles d'un C2 numérisé - que l'on pourrait résumer au raccourcissement de la boucle décisionnelle ou OODA (*Observe-Orient-Decide-Act*) - sont largement reconnues et identifiées depuis des capacités de renseignement accrues jusqu'à l'aide à la décision, permettant ainsi au chef de gagner en liberté d'action et de manœuvre.

Un outil horizontal au service de la verticalité du commandement

En offrant des moyens accrus de stockage, d'accès et de traitement à distance des données, le *Cloud computing* sert la performance du C2. Concrètement, le *Cloud computing* se traduit pour le commandement et la conduite des opérations par :

- Une infrastructure qui permet à toutes les unités et aux états-majors d'accéder à distance aux informations, limitant ainsi le volume des systèmes d'information et de communication (SIC) des postes de commandement et permettant, par exemple, aux unités de gagner en mobilité.
- Le partage d'une vision commune de la situation opérationnelle (ou *Common Operational Picture*) à tous les échelons, basé sur un partage amélioré de l'information. Cette vision commune n'est plus seulement centralisée au plus haut niveau du C2, l'information peut être partagée à tous les échelons, ce qui peut notamment augmenter l'autonomie et l'initiative aux plus bas échelons tactiques.
- Des capacités de réplication et de synchronisation des données avec une architecture comprenant des « mini-*Clouds* » sur le théâtre d'opérations en interaction avec un *Cloud* plus central au niveau stratégique ; ce qui permet une plus grande résilience de la chaîne de commandement en cas de perte de contact avec l'un des échelons.

Le *Cloud computing* contribuera donc à un renforcement et à une accélération de la prise de décision par l'amélioration de l'accès à l'information (flux montant du niveau tactique vers le stratégique) et de la transmission et la coordination des ordres (flux descendant du niveau stratégique vers le théâtre). Sur le théâtre, les ordres arrivent plus vite aux unités subordonnées, voire directement aux systèmes d'armes sans intermédiaires humains (conduite de tir automatique, guidage des missiles…).

Un risque accru de fragilisation de la chaîne de commandement

Le fonctionnement « en *Cloud* » génère par nature de très nombreux échanges d'informations entre différents niveaux de décision et installe une certaine horizontalité entre les acteurs du C2 que traduit l'expression « combat collaboratif ». Ces évolutions amplifient certains défis et contraintes ayant un impact sur la verticalité de la chaîne de commandement, où chaque échelon doit disposer du juste et nécessaire niveau d'information, gage de sa liberté de décision et d'action. À titre d'exemple, dans le cas d'un escadron de chars, un accès généralisé au réseau de l'escadron « *permet à chacun des chefs de char de comprendre sa place dans le dispositif, il ne signifie pas que le réseau n'est plus dirigé et que les liens de subordination entre éléments ne sont pas clairement établis* »[1].

Pour les commandants, au niveau opératif, voire stratégique, l'accès à une quantité massive d'informations en temps réel peut faire naître une tentation de pratiquer du **micro-management**, terme emprunté au monde de l'entreprise et désignant la pratique dans laquelle le manager contrôle de trop près les activités de ses subordonnés. L'opportunité de suivre en direct et avec grande précision l'évolution d'une section, ou même d'un groupe de combat, peut entraîner une forme « d'effet tunnel » dans lequel le décideur peut s'enfermer malgré lui. Ce biais de perception risque de se faire au détriment de la prise de distance nécessaire au commandement de grandes unités de combat. La chaîne hiérarchique est alors brisée par l'échelon supérieur qui contourne ou écrase les échelons intermédiaires. En miroir au concept de « caporal stratégique » désignant comment une action individuelle à portée tactique peut engendrer un véritable retournement stratégique, on pourrait alors parler de « général tactique ». Les premiers retours d'expérience de la guerre en Ukraine montrent les conséquences opérationnelles que peut avoir la réduction de la prise d'initiative au niveau tactique, liée à un contrôle trop strict par les échelons supérieurs. La chaîne de commandement de l'armée russe, très verticale et ne comprenant que peu de sous-officiers, accorde peu d'autonomie aux unités tactiques ; ces dernières ont tendance à se retrouver réduites seulement à opérer en réaction.

A contrario, la doctrine ukrainienne encourage les prises d'initiative tactiques, engendrant de l'imprévisibilité et des attitudes bien plus réactives.

Facilitée par le *Cloud computing*, l'abondance possible d'informations parfois accessibles en temps réel et à distance peut également interférer dans le processus de prise de décision en exposant le décideur à :

→ Une **« avalanche informationnelle »** pouvant conduire à une **surcharge informationnelle**[2] où les remontées de données sont trop denses pour pouvoir être traitées efficacement. Cette surcharge peut s'expliquer par des failles techniques d'une part, la capacité de calcul n'est pas suffisante pour exploiter la masse de données remontée et stockée ; par des limites humaines d'autre part, les opérateurs sont exposés à une surcharge cognitive et ne parvienne pas à extraire l'information utile de la masse de données disponibles. En avril 2012, ce risque a conduit le *Regional Command East* en Afghanistan à interdire les retours vidéo de drones *Predator* vers le *Joint Operations Command*, car ces flux distrayaient les opérateurs de leurs missions[3]. Cette « infobésité » peut entraîner des effets de distraction et détourner l'attention des informations essentielles à la conduite des opérations.

→ **Un blocage de la chaîne de commandement par attente permanente d'informations supplémentaires.**
Alors que le comportement pertinent face à l'abondance des données pourrait être de limiter volontairement le flux des données entrantes, on cherche souvent à disposer de toujours plus d'informations afin d'éclairer au mieux le choix. Or, une décision ne peut être jugée appropriée que dans un contexte précis et selon la temporalité dans laquelle elle se situe. À vouloir constamment réduire l'incertitude, on finit par paralyser la prise de décision. Pour le chef militaire, le risque est de réduire sa capacité d'initiative et de se placer dans une posture réactive vis-à-vis du contexte. Conserver une capacité à décider en incertitude est d'autant plus nécessaire que l'information sera toujours incomplète et imparfaite : l'action de l'ennemi ou les conditions imposées par le théâtre entraîneront une perte de connexion avec certaines unités et donc un arrêt dans la transmission des informations.

1. CES Martin Pinel, « *La subsidiarité au combat : de quoi s'agit-il ?* », Fondation Maréchal Leclerc, 18/12/2020, URL : https://www.fondation-marechal-leclerc.fr/wp-content/uploads/2017/08/CES-PINEL_Subsidiarite-au-combat.pdf
2. Caroline Sauvajol-Rialland, « *La surcharge d'emails, nouveau vecteur de la souffrance au travail* », Huffington Post, 31/08/2012, URL : https://www.huffingtonpost.fr/actualites/article/la-surcharge-d-emails-nouveau-vecteur-de-la-souffrance-au-travail_8843.html
3. Serge Caplain, « *Les 10 pièges de la numérisation des forces terrestres* », Linkedin, 15/01/2018 URL : https://www.linkedin.com/pulse/les-10-pièges-de-la-numérisation-des-forces-serge-caplain/?originalSubdomain=fr

APPORTS DU *CLOUD* AU FONCTIONNEMENT DES C2 : CONCILIER TECHNOLOGIE COLLABORATIVE ET PERFORMANCE DU COMMANDEMENT

Dans un contexte de dépendance accrue aux réseaux, ces risques pesant sur la chaîne de commandement rappellent l'importance pour le C2 de :

- Maintenir rigoureusement le principe de subsidiarité du commandement ;
- Conserver la réactivité du processus décisionnel, notamment en environnement dégradé où l'accès aux données pourra être limité, voire coupé ;
- Gérer l'afflux croissant de données aux différents niveaux de la chaîne de commandement tout en évitant de paralyser la prise de décision ;
- Fluidifier le traitement de données hétérogènes provenant de sources multiples ;
- Rendre l'information plus accessible à tous les échelons grâce à des outils et des interfaces ergonomiques.

Ces exigences passent d'abord par la gestion des remontées d'information et des descentes d'ordres via chaque maillon de la chaîne adapté à l'instantanéité des flux de données pour l'ensemble des acteurs branchés sur le réseau. Cela signifie aussi qu'il y a un traitement progressif des informations dans le sens montant, mais aussi un ajustement des ordres donnés dans le sens descendant à chaque échelon hiérarchique. Le *Cloud computing* peut contribuer à cette organisation, car il permet une répartition optimale des données entre « stockage local » (jusqu'au niveau du combattant) et « stockage réseau » (jusqu'au niveau stratégique). Son corollaire pour la répartition des capacités de calcul (*Edge computing*) permet également de traiter les données « en local », sur les plateformes et terminaux. Autre technologie étroitement liée au *Cloud computing*, l'intelligence artificielle permet d'automatiser le traitement des données et de dégager de la masse de données des informations utiles pour orienter - plutôt qu'automatiser ou remplacer - la prise de décision.

Combinés, ces outils permettent un allègement des flux de données et donc d'informations échangées entre les différents échelons de la chaîne de commandement. Une fois les données stockées et traitées au niveau pertinent, seules l'information utile sera transmise aux échelons pertinents. En plus d'alléger les volumes transitant sur les réseaux - et donc de répondre à la contrainte de la connectivité limitée - ils amélioreront la performance du processus décisionnel en conservant, d'une part, et transmettant, d'autre part, l'information utile au niveau utile.

APPORTS DU *CLOUD* AU FONCTIONNEMENT DES C2 : CONCILIER TECHNOLOGIE COLLABORATIVE ET PERFORMANCE DU COMMANDEMENT

CONTRIBUTEUR

Général de corps d'armée (2S) Hervé GOMART
Ancien Major général de l'armée de Terre

Évolution du commandement avec l'apparition des technologies « collaboratives »

Comme le souligne la spécialiste des enjeux géopolitiques du numérique Asma Mhalla[4], 2022 aura été marquée par l'entrée du cyberespace dans le débat public. Que ce soit via les cyberattaques, les campagnes de désinformation sur les réseaux sociaux, la destruction ou la prise de contrôle des infrastructures réseau, le cyberespace met à disposition des États de nouveaux outils de puissance, de subversion et de coercition.

L'année 2022 aura également été marquée par l'invasion russe en Ukraine et la guerre qui s'y déroule depuis. Contre toute attente, l'armée russe n'a pas su atteindre ses principaux objectifs stratégiques ou opératifs, car elle s'est heurtée à des Ukrainiens bien préparés, bien organisés et très résilients. L'une des différences notables entre les deux armées en guerre réside dans le C2 (*Command and Control*). Là où l'armée russe est restée organisée selon le modèle soviétique fondé sur une centralisation excessive du commandement, l'armée ukrainienne a su évoluer depuis 2014 et la perte de la Crimée et d'une partie du Donbass en faisant effort sur un C2 décentralisé s'appuyant sur des postes de commandement réduits, mobiles et enterrés.

Le C2 étant reconnu comme le facteur de supériorité principal, il est donc vital pour les armées de considérer avec détermination les technologies numériques dites collaboratives pour faire évoluer leur commandement au sens de son organisation et de sa mise en œuvre et demeurer ainsi en capacité de gagner la guerre.

D'une part, l'un des enjeux du *Cloud computing* réside dans la capacité à acquérir toujours plus d'information, de pouvoir et savoir l'analyser, la stocker, l'exploiter, la transmettre et la suivre. L'armée qui est en mesure d'agir ainsi conservera sa liberté d'action dans les champs numérique et de la donnée. Elle aura la capacité à prendre l'ascendant sur ses compétiteurs ou adversaires en ayant un temps d'avance et en anticipant grâce à des outils d'aide à la décision plus puissants et plus performants.

D'autre part, les technologies dans les domaines spatial, satellitaire, imagerie, robotique..., participent directement à la transparence du champ de bataille qui constitue une donnée particulièrement importante dans la conflictualité actuelle. Même si elle n'est pas absolue, elle doit être prise en compte dans les différentes phases opérationnelles de la campagne stratégique. La conséquence directe de cette transparence s'applique sur le C2 qui peut difficilement demeurer établi sur une organisation fondée sur des états-majors pléthoriques, sédentarisés et alourdis par des outils numériques toujours plus encombrants. Aujourd'hui, une chaîne de commandement doit s'appuyer sur une organisation offrant réactivité et pragmatisme. Il s'agit donc pour chacun des niveaux (stratégique, opératif et tactique) de savoir fonctionner sur des EM ou PC réduits en volume, agiles et mobiles. Une organisation modulaire en PC distribués constitue déjà une réponse pertinente. Par ailleurs, le principe de subsidiarité est un impératif. Il est justement plus applicable par l'accès au *Cloud*. Toute entité de commandement doit être en mesure de s'y connecter et d'y trouver la situation opérationnelle commune (COP[5]). Une telle organisation autorise l'autonomie des PC jusqu'aux plus bas échelons, autonomie qui ne doit pas être vue comme une permanence du commandement, mais comme une opportunité à savoir exploiter en fonction de la manœuvre et de la situation du moment.

4. Asma Mhalla enseigne à Sciences-Po Paris et à l'Ecole Polytechnique
5. COP : *Common Operational Picture*

Cependant, s'il constitue une évolution technologique majeure, le *Cloud computing*, avec ses différentes applications (stockage, messagerie, outils collaboratifs, ...), ne doit pas être considéré comme la panacée du domaine de l'échange d'information. En effet, s'il peut apporter de réelles plus-values en termes de rapidité dans la collecte d'information, le traitement des données ne pourra pas être totalement exploité sans l'apport de l'intelligence artificielle. Compte tenu de la massification toujours plus importante d'informations, qu'elles soient opérationnelles ou techniques, l'homme n'est déjà plus en mesure de tout voir, tout analyser et d'exploiter les bonnes données dans le bon tempo. La surcharge informationnelle ne fera que croître dans l'exploitation de l'informatique en nuage, développant ainsi de réels risques cognitifs.

Oui, et c'est une réalité, les difficultés, voire les risques associés à l'apparition de nouvelles technologies collaboratives existent, mais compte tenu des enjeux liés à la supériorité cognitive, à l'accélération du processus écisionnel par le biais d'outils d'aide à la décision en capacité d'effetuer des analyses automatisées ou prédictives, les armées n'ont guère le choix de poursuivre avec détermination leur appréhension d'un C2 en constante évolution et de consolider la résilience de la chaîne de commandement. Par conséquent, non seulement celle-ci devra être protégée face aux menaces cyber, et aux brouillages en tout genre, mais elle devra également travailler sans cesse à accroître sa discrétion, à réduire sa signature électromagnétique et son empreinte thermique tout en promouvant une organisation au niveau opératif s'appuyant sur un système de réplications de parties du *Cloud computing* stratégique.

La transformation numérique de nos armées est en marche depuis déjà de nombreuses années. Les technologies collaboratives vont s'imposer de plus en plus, tout comme la réalité virtuelle ou autres solutions immersives. Aussi est-il vital de continuer à suivre les avancées de la high-tech et de poursuivre les évolutions de nos chaînes de commandement. La complexité du champ de bataille ou le brouillard de la guerre ne disparaîtra pas pour autant, mais pourra être plus appréhendable. Le pays qui n'effectuera pas les efforts et les investissements indispensables a déjà perdu la guerre.

APPORTS DU *CLOUD* AU FONCTIONNEMENT DES C2 : CONCILIER TECHNOLOGIE COLLABORATIVE ET PERFORMANCE DU COMMANDEMENT

CONTRIBUTEUR

Michael CROWLEY
Director secteur public EMEA
VMWARE

Adopter l'agilité pour éviter la fragilité

La guerre moderne est l'incarnation de la diversité. Elle est menée en environnement multi-milieux : terrestre, maritime, aérien et cyber, souvent simultanément. Bien qu'elle puisse impliquer régulièrement plusieurs nations agissant au sein d'une coalition avec des troupes opérant avec des équipements diversifiés, utilisant plusieurs langues, et menant des opérations dans tous les types d'environnements imaginables : les scénarios potentiels sont presque illimités.

Cela signifie que la base du succès pour toute force armée est l'agilité. Mais compte tenu de la taille et de l'ampleur des tâches auxquelles les armées sont confrontées, la différence entre volonté et capacité réelle à être agile est conséquente.

Pas de méthode unique pour devenir agile

La question subsidiaire est la suivante : « Que faut-il pour permettre aux forces armées d'être plus agiles » ? Malgré les nombreuses initiatives qui ont pu être prises en ce sens, il n'y a pas de solution « miracle ». C'est précisément en raison des nombreuses variables impliquées qu'il n'existe pas de route toute tracée pour gagner en agilité. Pourtant, il existe un dénominateur commun qui différencie les forces agiles de celles qui ne le sont pas : les infrastructures disponibles.

Les forces armées les plus agiles disposent des infrastructures nécessaires pour permettre l'interopérabilité entre les membres de la coalition, indépendamment de l'objectif de la mission ou des contraintes géographiques. Elles constituent l'épine dorsale sur laquelle repose le partage de données à tous les niveaux de commandement. C'est la clé pour que la personne adéquate dispose de l'information nécessaire au moment opportun, afin de permettre les initiatives sur le terrain.

Modifier la chaîne de commandement

La dispersion des forces sur le terrain tend à démontrer qu'une chaîne de commandement monolithique ne fonctionne plus. La nécessité d'encourager des initiatives sur le terrain au niveau du commandant n'a pas seulement fracturé la chaîne traditionnelle, elle l'a complètement effacée. C'est l'approche occidentale de la guerre au XXIe siècle, que nous observons aujourd'hui dans le conflit en Ukraine.

Les Ukrainiens, soutenus par les dirigeants d'autres États européens, ont adopté cette approche. Il s'agit d'une stratégie déterminante pour fluidifier les opérations, autant offensives que défensives, et qui explique partiellement pourquoi nous entendons continuellement parler de succès sur le terrain, aussi modestes soient-ils. Cette fluidité détonne d'autant plus que les forces russes continuent d'opérer avec une structure de commandement très rigide, qui ne leur permet pas de faire preuve de la flexibilité ou de l'agilité nécessaire pour réagir efficacement. À ce propos, cette analyse détaillée[6] particulièrement pertinente.

Une fédération de nuages

La question suivante serait logiquement qu'entendons-nous par infrastructure et qu'est-ce que cela implique ? Pour être clair, nous parlons d'une fédération de nuage. Il s'agit d'un ensemble de structures de *Cloud*s que l'on agrégerait pour créer une architecture multi-*Cloud*. Cela garantit que les données pertinentes sont hébergées, stockées et partagées au bon endroit, en capitalisant à la fois sur les avantages respectifs du secteur public, du secteur privé, et des technologies du *Edge computing*, sans une dépendance excessive à l'égard de l'un. En outre, cela permettrait de renforcer l'interopérabilité entre les nations et les membres d'une coalition.

6. As Major General (rtd.) Mick Ryan « *A tale of three generals - how the Ukrainian military turned the tide* », Engelsberg Ideas, 14/10/2022, URL : https://engelsbergideas.com/essays/a-tale-of-two-generals-how-the-ukrainian-military-turned-the-tide/

Ce type d'architecture en nuage permettrait aux différentes nations et forces de se brancher sur le réseau global ou partagé ou sur des réseaux de commandement plus spécifiques, tout en offrant la résilience nécessaire pour ajuster l'activité selon les besoins. C'est là que réside l'apport principal d'une architecture multi-*Cloud*. Il s'agit d'un cycle de traitement de l'information de l'arrière vers l'avant, de façon interconnectée, qui constituerait les fondations de l'agilité des forces armées.

Le multi-*Cloud* dans une coalition

Prenons l'exemple d'une coalition entre le Portugal, l'Espagne et le Royaume-Uni. Le Royaume-Uni serait la nation cadre et mettrait à disposition son architecture *Cloud* sur laquelle le Portugal pourrait brancher son propre *Cloud* et l'Espagne faire de même. Il s'agit d'un multi-*Cloud* qui permettrait à l'information de circuler de la source portugaise ou espagnole vers le système de *Command and Control* britannique. Ces informations pourraient être traitées en amont et transformées en renseignements exploitables sur le terrain presque en temps réel. À la fin de l'opération, les forces portugaises et espagnoles pourraient se déconnecter et conserver l'intégrité de leurs données et renseignements.

Faire du multi-*Cloud* une réalité

Encore récemment, des jalons ont été posés pour faire du multi-*Cloud* une réalité. En décembre 2022, le département américain de la Défense (*U.S. Department of Defense* - DoD) a attribué le contrat *Joint Warfighting Cloud Capability*[7] (JWCC) - l'outil d'acquisition du DoD - permettant d'acquérir directement des offres de *Cloud* à tous les niveaux de classification pour servir des missions de tout niveau.

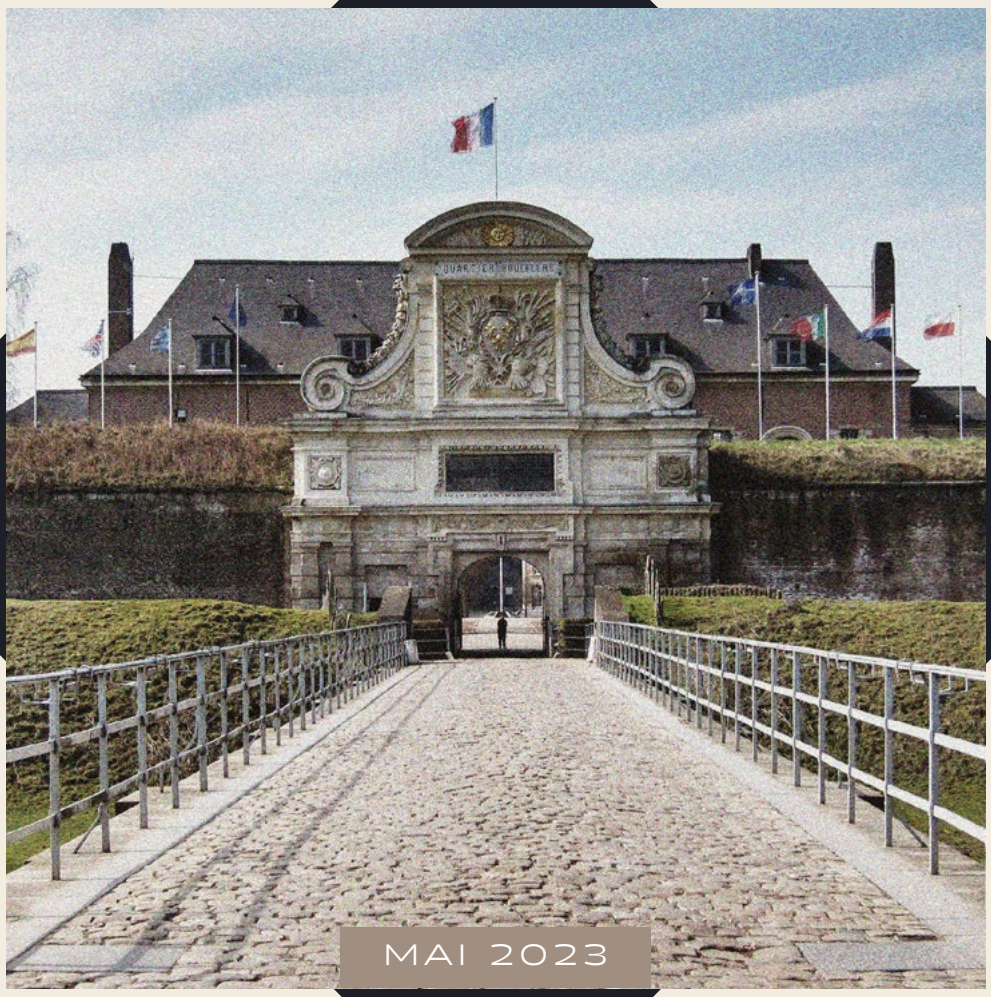
Le contrat JWCC permet au département de la Défense américain d'avoir un accès direct aux quatre principaux fournisseurs de *Cloud* - AWS, Google, Microsoft et Oracle - dont VMware est la pierre angulaire. Cela signifie que les militaires américains auront la possibilité d'acquérir, dans le cadre d'un contrat unique, des capacités telles que la disponibilité et la résilience des services en tout temps et en tout lieu, la gestion centralisée et le contrôle distribué, une facilité d'utilisation, la parité commerciale, l'élasticité de l'infrastructure informatique, de stockage et de réseau, l'analyse avancée des données, la sécurité renforcée et les dispositifs tactiques avancés.

Les chefs militaires ne devraient pas craindre l'intégration de systèmes existants, ni d'adopter une architecture multi-*Cloud*. Les forces les plus performantes et les plus agiles le font déjà avec succès. Si elles n'adoptent pas cette approche, il ne fait aucun doute qu'avec le temps, les opérations militaires deviendront de plus en plus fragiles et le progrès sera inexorablement freiné. Ou pire encore, cela pourrait mettre en péril à la fois l'intégrité de la mission, mais surtout la vie des soldats.

7. AUS Department of Defense « *Department of Defense Announces Joint Warfighting Cloud Capability Procurement* », 07/12/2022, URL : https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/

VAUBAN
SESSIONS

#8 LES DÉFIS DU DÉPLOIEMENT D'UN *CLOUD* TACTIQUE AU SERVICE DU COMBAT COLLABORATIF



MAI 2023

Forward

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

PRÉFACE

S'il fallait encore le prouver, la guerre en Ukraine démontre combien la formation, l'initiative, la créativité des combattants au plus près de l'action constituent aujourd'hui une force sur laquelle toute armée moderne se doit de capitaliser. Pour tirer le plein parti de cet atout précieux, il convient de concevoir la collaboration de tous les acteurs à tout niveau de commandement et d'exécution au sein d'un réseau d'information dynamique, performant, fiable.

Le précédent numéro (7) des Vauban Papers « apport du *Cloud* aux fonctions de C2 » a permis de mettre en évidence l'intérêt et les conditions d'emploi du *Cloud computing* au sein de la chaîne opérationnelle. En résumé, il s'agit de tirer le meilleur parti des flux de données issues des différents capteurs, de les organiser et de permettre ainsi aux décideurs de prendre un ascendant informationnel sur l'adversaire. Pour exploiter et même amplifier cet avantage dans les différents domaines de combat, l'emploi du *Cloud computing* au sein d'un véritable réseau tactique est une voie séduisante. Ainsi, chaque unité de combat pourrait à la fois, en permanence, contribuer à une évaluation de situation tactique rafraichie et en bénéficier. À l'image de certains réseaux spécifiques actuels (emploi des drones, appui aérien, liaisons de données tactiques, etc.) le partage d'information au sein du *Cloud* tactique permettrait d'optimiser l'emploi des moyens disponibles à un moment et un endroit donné et de maximiser les effets produits. La gestion dynamique des données permise par le *Cloud computing* ne se limite pas à l'emploi des moyens, elle doit aussi permettre d'améliorer l'identification des forces engagées, de réduire les risques de tirs fratricides, elle touche aussi au soutien médical du combattant ou encore à la logistique opérationnelle.

Pour passer de la théorie à la pratique, déployer et mettre en œuvre ces réseaux de combat tactique, de nombreux défis doivent être relevés et des expérimentations en conditions opérationnelles exigeantes doivent être conduites. La disponibilité de moyens de communication performants en tout point du théâtre d'opérations constitue évidemment un pré-requis que peuvent résoudre au moins en partie les nouvelles technologies de l'information à condition de les rendre robustes aux techniques de brouillage les plus modernes. Ce point met en évidence le besoin d'une redondance raisonnable des moyens de communication et la nécessité d'envisager dans tous les plans d'opérations et donc pour l'entraînement des forces des modes dégradés. Il s'agit aussi d'éviter autant que possible que la connexion au *Cloud* de combat ne devienne un critère indispensable de participation aux opérations. C'est une question ouverte : le *Cloud* de combat tactique doit-il devenir un moyen d'accélérer, d'optimiser les opérations multi-domaines ou deviendra-t-il une fin en soi ?

La technologie, aussi puissante soit elle, ne peut être le seul moteur de la transformation numérique opérationnelle. Seule une coopération étroite, guidée par le besoin opérationnel, nourrie d'expérimentations réalistes, mais aussi d'échecs, peut permettre de développer en toute confiance le *Cloud* de combat tant au niveau du commandement et du contrôle des opérations qu'à celui de l'exécution.

Il ne faudrait pas que le brouillard digital se substitue, ou pire, nourrisse le brouillard de la guerre.

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

LES DÉFIS DU DÉPLOIEMENT D'UN *CLOUD* TACTIQUE AU SERVICE DU COMBAT COLLABORATIF

CONTRIBUTEURS

Axel DYÈVRE
Associé
FORWARD GLOBAL

Martin DE MAUPEOU
Directeur
FORWARD GLOBAL

Marin MESSY
Analyste
FORWARD GLOBAL

« *Nous avons toujours pratiqué le combat collaboratif, c'est le système de transmission de l'information qui a changé* ». Lieutenant-colonel LUDOVIC, Commandant en second du 1er Régiment d'infanterie de marine français.

Les dernières années ont vu l'adoption rapide de services centralisés d'informatique en nuage (*Cloud*) par le secteur privé. Ce mode de fonctionnement s'est révélé économiquement et opérationnellement intéressant pour beaucoup d'entreprises. Le fonctionnement en *Cloud* permet en effet de disposer d'une infrastructure informatique dont les coûts peuvent être variabilisés en adaptant le dimensionnement de son infrastructure de manière souple et quasi-immédiate aux besoins de l'organisation, que ce soit en besoin d'espace de stockage, de capacités de traitement, mais aussi du nombre d'utilisateurs de logiciels. En outre, les technologies du *Cloud* ont contribué à accélérer la mise en réseau d'objets physiques connectés et le développement de nouveaux services et usages de partage et d'accès à toujours plus de données et d'informations.

Pour permettre la mise en réseau des acteurs et des moyens sur un théâtre d'opérations, le *Cloud* tactique traduit l'intérêt des armées à appliquer cette logique aux opérations militaires. Si aujourd'hui, on en est encore au stade des prototypes et des tests, l'enjeu principal à résoudre est de permettre aux forces de continuer à remplir leurs missions, même en « mode dégradé », c'est-à-dire même dans des zones où la communication avec un *Cloud* centralisé n'est pas possible, que ce soit du fait de la géographie ou de l'action de l'ennemi. En effet, à la différence du secteur privé qui a développé et popularisé les concepts et offres *Cloud*, les armées engagées en opérations donc celles ayant besoin de ressources « tactiques » - doivent pouvoir remplir leurs missions en permanence, quel que soit l'état des réseaux. À la croisée entre logique centralisée et décentralisée, hybridant plusieurs ressources, le *Cloud* tactique vise donc à répartir les données et leur traitement, et donc la puissance de calcul, entre les différents niveaux engagés (P.C., blindés, soldats, etc.) pour permettre un fonctionnement autonome si nécessaire.

Les exigences d'un théâtre d'opérations peuvent sembler en première approche difficilement compatibles avec l'usage de moyens fonctionnant en *Cloud*. D'une part du fait de la nature externalisée et centralisée du *Cloud* et, d'autre part, à cause du défi que représente son déploiement pour des scénarios caractérisés par une infrastructure temporaire et mobile ainsi qu'un environnement contraint et dégradé. Pour ces raisons et en dépit des progrès dans le domaine de la connectivité, le « *Cloud computing* », reste pour l'instant déployé, au sein des armées, principalement dans un environnement non-contraint et non en opération. Travaillant depuis plus d'une décennie sur le sujet, l'*US Army* n'a ainsi annoncé le déploiement d'un premier *Cloud* sur un théâtre extérieur que récemment (2022), les expérimentations ayant jusqu'à présent été conduites sur le territoire américain[1].

À l'instar de cette initiative et au vu des besoins croissants d'accès rapide à de grandes quantités d'informations, la question n'est plus de savoir si les armées vont devoir se pencher sur la question de mettre en place des *Clouds* tactiques hybridant des ressources localisées et distantes. Elle est surtout de déterminer comment ils pourront être déployés compte tenu des contraintes opérationnelles particulières qui présideront à leur mise en œuvre dans un contexte militaire.

Stocker, transmettre et exploiter la masse de données « en temps réel »

Avec la numérisation des armées, le soldat individuel, la plateforme de combat, le système d'armes deviennent désormais autant d'agents de collecte et de transmission de données vers l'échelon supérieur. Équipés de capteurs, ils sont parties intégrantes du réseau et donnent accès à des données d'environnement et d'instructions. La capacité à traiter et à partager ces données puis à faire circuler une information stockée et archivée contribue à valoriser de la connaissance ou de l'expérience et permet d'en donner l'accès en tout temps et en tout lieu aux différents acteurs.

1. Jaspreet Gill « *Army "well on its way" to first OCONUS cloud in Indo-Pacific* », Breaking Defense, 14/01/2022, URL : https://breakingdefense.com/2022/01/army-well-on-its-way-to-first-oconus-cloud-in-indo-pacific/

LES DÉFIS DU DÉPLOIEMENT D'UN *CLOUD* TACTIQUE AU SERVICE DU COMBAT COLLABORATIF

Alors que les liaisons de données tactiques actuelles telles que la Liaison 16 montrent leurs limites en termes de débit, le *Cloud* tactique traduit la volonté de donner aux plates-formes et aux unités de combat la possibilité d'accéder au volume massif de données stockées et de les valoriser grâce à l'application d'algorithmes avancés.

Un des apports possibles les plus perceptibles du *Cloud* au niveau tactique concerne la tenue de situation « en temps réel ». Avec le *Cloud*, la différence majeure par rapport aux moyens actuels est l'accélération du processus de remontée, de valorisation et de partage des données géo-référencées au sein d'une « bulle tactique ». La position de chaque unité, amie ou ennemie, est retransmise en direct automatiquement sur une représentation cartographique commune à tous. Le déploiement des véhicules connectés dans le cadre du dispositif français Barkhane a ainsi confirmé la pertinence de la diffusion instantanée et simultanée d'ordres graphiques aux différentes unités, par exemple pour la transmission d'itinéraires de contournement suite à l'identification d'IED.

Pour la manœuvre, le partage de situation « en temps réel » présente de nombreuses plus-values opérationnelles telles que :

- → Une meilleure couverture de zone permettant de contrôler un périmètre élargi ;
- → Une réduction des risques de tirs fratricides, en rendant le ciblage plus précis et décisif ;
- → Une meilleure coordination des différentes unités engagées, permettant de réarticuler plus aisément le dispositif.

De manière générale, la connaissance et le partage de situation renforcés permettent une fluidification de la manœuvre, des appuis et soutiens. On peut imaginer par exemple que les unités de maintenance disposent en direct de l'état des différents véhicules sur le terrain, et donc puissent optimiser la répartition des stocks et minimiser les temps d'indisponibilité. La logistique de théâtre en serait également grandement simplifiée, disposant d'une vision actualisée en permanence du niveau de munitions, carburant, et nourriture, permettant là aussi l'optimisation des flux logistiques.

Répondre au défi du champ de bataille connecté

L'usage du *Cloud* est simple sur le territoire national où il reposera sur une infrastructure technique et un environnement maîtrisés. Ce n'est évidemment pas le cas sur un théâtre d'opération où les infrastructures de communication peuvent s'avérer inexistantes, insuffisantes ou non-sécurisées. L'enjeu est ici de garantir, d'une part, la disponibilité du réseau et, d'autre part, une bande passante suffisante pour faire transiter d'importants volumes de données (en tenant compte du chiffrement des données qui augmente les volumes).

Ainsi, l'usage du *Cloud* sur un théâtre nécessite un réseau gérant la mobilité et assurant les communications tactiques nécessaires aux forces déployées en utilisant les technologies radio-logicielles. Or, les réseaux de communications militaires ont été construits dans un premier temps pour acheminer de la voix, en utilisant une structure hiérarchisée. Il s'agissait également de raccorder des entités géographiques qui étaient peu mobiles. Ces réseaux ont ensuite été adaptés pour transporter de la donnée, mais sans revoir leur architecture globale. Le défi reste donc de taille pour répondre à la demande de connectivité actuelle et faire circuler tout type de données (imagerie, vidéo, messagerie instantanée, etc.).

Au-delà des capacités offertes par les satellites pour garantir la confidentialité des communications et couvrir des zones isolées, la combinaison d'autres moyens est envisagée pour réduire la latence (le délai de transmission des données) et augmenter les débits de données échangées : le déploiement de réseaux tactiques projetables reposant sur des serveurs et relais portatifs, la réutilisation des infrastructures de communication existantes (sur des théâtres urbains) ou encore l'emploi de ballons haute altitude stationnaires.

Depuis plus d'une vingtaine d'années, l'innovation dans le domaine des communications est en grande partie venue du secteur civil : les réseaux mobiles, et notamment les réseaux cellulaires, sont devenus en quelques décennies une composante majeure du développement des technologies de l'information et de l'accès aux données.

LES DÉFIS DU DÉPLOIEMENT D'UN *CLOUD* TACTIQUE AU SERVICE DU COMBAT COLLABORATIF

Ces avancées, jusqu'à l'arrivée récente de la 5G, permettent d'améliorer la connectivité et la fiabilité, d'augmenter les débits et de réduire la latence. De plus en plus numérisés, les systèmes d'information et les systèmes d'armes militaires sont impactés par ces évolutions dont les armées peuvent tirer parti en confrontant leurs besoins spécifiques aux progrès technologiques. Par exemple, l'architecture des réseaux de communication, entièrement revue avec l'arrivée des réseaux IP (*Internet Protocol*), fournit des architectures distribuées, décentralisées et virtualisées, permettant de gérer la résilience, une plus grande centralisation des applications, et d'amener les infrastructures au plus près des utilisateurs. La mise en oeuvre de cette architecture tout IP, en permettant l'échange d'informations entre tous les points du réseau, est une des conditions essentielles au champ de bataille connecté.

Maîtriser la sécurité d'un environnement interconnecté

Inhérents au fonctionnement en *Cloud*, l'interconnexion des systèmes, la centralisation et le transfert des données représentent autant de failles de sécurité possibles qui nécessitent des mesures et doctrines d'emploi maîtrisées et partagées. Nécessitant des systèmes plus ouverts, le *Cloud* crée mécaniquement des fenêtres de vulnérabilité et augmente la surface d'attaque. Par ailleurs, la virtualisation des ressources et le déport d'une partie des capacités de calcul vers les terminaux connectés (« *Edge computing* ») augmentent la taille du logiciel considérablement, ce qui participe également à l'augmentation de la surface d'attaque et impose d'intégrer la cybersécurité comme dimension structurante dès la conception des systèmes.

Au niveau tactique, les communications sont en plus exposées à un environnement magnétique extrêmement contraint du fait des menaces de brouillage ou de leurrage. Les équipements et les plateformes seront toujours plus attaqués du fait de cette « hyperconnectivité ». Ils devront donc avoir été conçus pour encaisser et retarder les effets d'agressions et reposer sur un réseau fortement sécurisé. L'utilisation systématique du chiffrement des données est une première réponse.

Au-delà du chiffrement, la cybersécurité nécessite de concevoir et de mettre en oeuvre des mesures de sécurité depuis la conception des systèmes militaires (spécifications techniques) jusqu'à leur usage (doctrines et concepts d'emploi), en passant par leur déploiement et leur paramétrage. Cette exigence de cybersécurité s'applique à différents niveaux :

- **Sécurisation physique** des serveurs et systèmes connectés physiquement accessibles par l'ennemi. Ce qui permet bien sûr leur neutralisation ou destruction physique, mais également leur capture, offrant un potentiel point d'entrée pour compromettre le réseau.
- **Sécurisation logicielle** : les composants embarqués au sein des systèmes connectés offrent des points de vulnérabilités supplémentaires.
- **Sécurisation des communications** : le « *Cloud computing* » implique d'opérer une nécessaire ouverture tout en assurant la sécurisation des infrastructures et protocoles de transit des données ; la surveillance des réseaux est à cet égard essentielle.
- **Sécurisation applicative** : les plateformes d'agrégation des données et les applications utilisées pour leur exploitation peuvent être l'objet de cyber-attaques exploitant leurs failles.

Placer le mode dégradé et le facteur humain au cœur de la réflexion doctrinale

Comme pour l'introduction de toute nouvelle technologie sur le champ de bataille, se pose avec le « *Cloud computing* » l'enjeu de l'intégration doctrinale de ce nouvel environnement technique en situation de combat réel. Comme évoquée, la mise en place d'un mode de fonctionnement en *Cloud* se heurte, sur les théâtres, à des obstacles naturels, une bande passante bridée, des problématiques d'alimentation énergétique, ou encore à l'action de l'ennemi. Face à un adversaire disposant de capacités avancées de guerre électronique, il n'est pas assuré de disposer librement des fonctions avancées fournies par le réseau. En conséquence, l'ensemble des capacités de partage de l'information ne peuvent être disponibles que de façon sporadique et partielle.

Il en découle de la nécessité de penser le mode dégradé dans le concept d'emploi du *Cloud* tactique pour assurer la continuité opérationnelle des forces en cas de déconnexion temporaire ou de perte du réseau.

Second élément clé, le facteur humain doit être replacé au coeur de la pensée doctrinale dans ce contexte d'évolution des outils et des moyens. Si le « *Cloud computing* » peut améliorer la performance au combat, l'humain reste la première variable dans le cadre du combat, qui par nature est une situation de stress intense impliquant une disponibilité cognitive réduite. Sous le feu, les soldats ne peuvent traiter qu'une quantité limitée de données, et donc ont tendance à pratiquer une sélection ciblée des informations afin d'éviter la surcharge cognitive.

Tout en augmentant la capacité d'accumulation, d'exploitation et de partage des données, le fonctionnement en *Cloud* - couplé à l'intelligence artificielle - peut et doit contribuer à obtenir les meilleures représentations de l'information pour pouvoir – dans le temps de l'action - établir les bonnes priorités, éliminer l'information non-pertinente et orienter la prise de décision. De plus, l'augmentation de la dispersion géographique - permise par des outils et des technologies de plus en plus décentralisés - peut entraîner un renforcement de l'isolement du combattant, et donc une perte de lien tactique entretenu habituellement par une forte proximité physique et psychologique. Ces dimensions cognitives et psychologiques, tout autant que les dimensions techniques et sécuritaires, sont à prendre en considération dans les réflexions relatives à l'usage du *Cloud* au niveau tactique.

LES DÉFIS DU DÉPLOIEMENT D'UN *CLOUD* TACTIQUE AU SERVICE DU COMBAT COLLABORATIF

CONTRIBUTEUR

Isidoros MONOGIOUDIS
PROJECT OFFICER POUR LES TECHNOLOGIES DE L'INFORMATION
AGENCE EUROPÉENNE DE DÉFENSE

L'atout principal du *Cloud computing* dans le monde militaire est d'améliorer la connaissance de la situation et donc la prise de décision. Au niveau tactique en particulier, des ressources informatiques spécifiques sont requises là où les solutions utilisées dans le civil ne sont pas adaptées aux conditions particulières d'usage du *Cloud computing* en opération. C'est ce que traduit l'expression « *Cloud* tactique ». Les concepts suivants sont étroitement liés au *Cloud computing* dans un environnement militaire :

- Les systèmes C4ISR facilités par un *Cloud* tactique : ce type de *Cloud* reflète la capacité à collecter et à traiter des données au plus près du champ de bataille afin d'améliorer la connaissance de la situation tactique et de permettre une vision commune (COP - *Common Operational Picture*) en temps réel disponible du niveau tactique (soldat) au niveau stratégique.
- La gestion de l'information provenant de sources hétérogènes : la nature des réseaux militaires et des composants numériques nécessite de collecter et d'agréger des informations provenant de sources différentes. Ce qui nécessite un traitement et une gestion appropriés.
- L'amélioration du cycle de l'information par l'utilisation des outils de l'intelligence artificielle (IA) et du *Big Data* qui offrent différents outils et méthodes pour valoriser les données disponibles.
- L'aide à la décision par l'IA et le *Big Data* qui permettent d'utiliser les résultats des étapes précédentes, depuis la collecte jusqu'au traitement, pour soutenir la prise de décision.

Pour les besoins militaires en milieu tactique, l'utilisation d'un *Cloud* conventionnel pose certains problèmes et difficultés qui doivent être résolus. Parmi ces problèmes, le plus important est probablement le manque de fiabilité des réseaux de communication déconnectés, intermittents et à faible bande passante (DIL - *disconnected, intermittent, low-bandwidth*) entre les utilisateurs au niveau tactique et le *Cloud*, dans un contexte où les multiples relais de communication et l'architecture, *a priori* centralisée, d'un *Cloud* risquent d'augmenter la latence (ou délai de transmission). Les informations fournies par une unité sur le terrain à une autre unité peuvent mettre longtemps à être disponibles. Les utilisateurs évoluent dans un environnement très dynamique et ne peuvent pas se permettre d'attendre les réponses aux demandes d'informations ou d'accès à un service à distance (réponses parfois issues d'autres utilisateurs pourtant déployés dans une zone voisine).

Le *Cloud* tactique est une combinaison entre un *Cloud* central, des capacités de calcul embarquées sur les capteurs et plusieurs niveaux possibles de *Clouds* (ou serveurs donc) intermédiaires distribuées entre le *Cloud* et les capteurs. Dans ce réseau hiérarchisé, plus un serveur intermédiaire est haut dans la hiérarchie, plus sa capacité de traitement et de stockage est importante, puisqu'il est censé prendre en charge un plus grand nombre de capteurs à la périphérie du réseau. À l'inverse, plus un serveur intermédiaire est élevé dans la hiérarchie plus le temps de latence sera important pour communiquer avec les capteurs en périphérie du réseau. Par conséquent, le déploiement des micro centres de données (ou *cloudlets*) en complément du *Cloud* centralisé fournit une gamme de capacités de calcul à différentes distances géographiques (et logiques) des dispositifs connectés à la périphérie.

Cette infrastructure intermédiaire (ou *Fog computing*), organisée et hiérarchisée adéquatement, peut offrir une gamme plus large de niveaux de service, en prenant en charge des applications qui ne peuvent pas être prises en charge par le *Cloud computing* seul. Une infrastructure *Fog* peut prendre en charge des applications ayant des exigences de qualité de service variées, car les applications peuvent s'exécuter au niveau hiérarchique offrant la capacité de traitement adéquate et répondant aux exigences de latence. Une autre conséquence d'un traitement des données plus proche de la périphérie est de réduire l'utilisation de la bande passante circulant entre le *Cloud* centralisé et la périphérie.

LES DÉFIS DU DÉPLOIEMENT D'UN *CLOUD* TACTIQUE AU SERVICE DU COMBAT COLLABORATIF

La connectivité entre plusieurs niveaux dans une architecture *Cloud* peut être possible grâce à plusieurs technologies de réseau, y compris les technologies filaires et sans fil, la 5G pouvant améliorer considérablement les performances du réseau.

Certains résultats d'études ont montré les avantages de la mise en œuvre d'un *Cloud* tactique :

→ **Unités combattantes** :

- Reconnaissance automatique des menaces à l'aide du traitement vidéo en temps réel à la périphérie ;
- Évaluation précoce des risques et alertes automatiques ;
- Informations accrues pour le combattant, la vidéo est traitée et enrichie d'informations obtenues par l'application de l'IA, presque en temps réel ;
- Si le combattant en périphérie dispose d'un système pour afficher des informations tactiques, il pourra facilement visualiser l'image commune opérationnelle (COP) enrichie avec ces informations.

→ **Utilisateurs stratégiques/opérationnels** :

- L'opérateur aura accès à la COP complète, en ajoutant les informations qui intéressent l'analyste, issues directement des niveaux intermédiaires dans l'architecture ;
- Il/elle recevra des rapports/alertes de renseignement automatiques générés par les plateformes tactiques. Ces rapports peuvent être partagés avec d'autres acteurs selon les procédures standards ;
- Cette vision commue du théâtre est automatiquement construite, en parallèle, avec les informations disponibles au niveau stratégique (OSINT, *Coalition Share Information* et informations tactiques).

L'un des concepts clés du *Cloud* tactique est l'Internet des objets militaires (IoMT - *Internet of Things or Military Things*) qui traduit tout simplement l'application des technologies et des concepts de l'*Internet of Things* (IoT) dans le domaine militaire. À ce jour, le déploiement des technologies liées à l'IoT par les militaires s'est principalement concentré sur les applications pour les systèmes C4ISR - soit les systèmes permettant le commandement et la conduite des opérations - et de conduite du feu. Les technologies IoT ont également été adoptées dans certaines applications pour la gestion logistique, la formation et la simulation.

L'IoMT interconnecte les capteurs, les effecteurs et les données. Ces données peuvent renseigner, entre autres, sur ses propres forces, celles des adversaires, les conditions environnementales et les attitudes de la population. Les capteurs et effecteurs peuvent être surveillés ou non, câblés ou sans fil. Certains appareils du marché de l'IoT sont conçus pour des environnements industriels extrêmes et seraient donc relativement bien adaptés aux environnements militaires.

Globalement, le concept de l'IoMT est largement motivé par l'idée que les futures batailles militaires seront dominées par l'intelligence artificielle et la cyber-guerre et se dérouleront probablement dans des environnements urbains. En créant un écosystème miniature de technologies intelligentes, capable de distiller des informations sensorielles et de gérer de manière autonome plusieurs tâches à la fois, l'IoMT est conçu à l'origine pour réduire une grande partie de la charge physique et mentale à laquelle les combattants sont confrontés dans un contexte de combat.

Pour prendre de bonnes décisions, il faut avoir une connaissance approfondie du champ de bataille et une image précise de la situation. Les informations dont un commandant a besoin pour prendre des décisions efficaces ont augmenté de façon exponentielle, ce qui signifie que les commandants rassemblent souvent des volumes de données diverses pour appréhender l'espace de bataille.

L'importance des données dans la guerre moderne pose deux défis distincts pour un commandant : gérer le volume de données produit et intégrer de nombreux types de données dans une vision cohérente de l'espace de bataille.

LES DÉFIS DU DÉPLOIEMENT D'UN *CLOUD* TACTIQUE AU SERVICE DU COMBAT COLLABORATIF

Les applications militaires de fusion de données intègrent non seulement des vidéos, mais aussi des images fixes, du renseignement d'origine électromagnétique, du renseignement humain, des capteurs terrestres, des rapports de champ de bataille, des données cartographiques et une multitude d'autres sources de données.

L'utilisation de l'IoT dans les communications opérationnelles est restreinte par les limites techniques de la bande passante et de la robustesse des réseaux de communications mobiles. Cependant, avec la technologie 5G, les vitesses seront plus que suffisantes pour une véritable application IoT avec une bande passante améliorée et une latence proche de zéro pour une collecte et un traitement des données précis et opportun.

L'Agence européenne de défense a pour objectif de définir les besoins technologiques en matière de *Cloud computing* pour les opérations de défense en analysant les concepts de *Clouds* tactiques, d'IoMTs, de collecte et d'analyse de données à partir de capteurs multiples par IA, de mise en œuvre de la 5G par le biais d'une étude en cours qui a débuté en 2019 et qui doit s'achever en 2023. Ces concepts se traduiront par une plateforme/démonstrateur de prototype pilote qui tentera de mettre en évidence les avantages du *Edge computing* et l'amélioration significative des performances dans le processus de *Situation Awareness*. La mise en œuvre ultérieure peut être abordée dans le cadre de l'AED avec des projets *ad hoc* adaptés aux exigences opérationnelles et techniques identifiées.

***Avertissement** : Cet article est une version courte d'une présentation sur le thème « Cloud tactique avec des capacités IoMT » tenue dans le cadre du projet CLAUDIA (Cloud Intelligence for Decision Making Support and Analysis), mis en œuvre en 2022.*

LES DÉFIS DU DÉPLOIEMENT D'UN *CLOUD* TACTIQUE AU SERVICE DU COMBAT COLLABORATIF

CONTRIBUTEUR

Joe BAGULEY
Vice-president & Chief Technology Officer EMEA
VMWARE

Se tourner vers l'*Edge* pour prendre l'avantage sur le terrain

Sur le champ de bataille moderne, la visibilité est primordiale et la capacité à naviguer dans le brouillard de guerre dépend de la capacité des commandants à tous les niveaux, et pas seulement des généraux, à avoir une vue d'ensemble du champ de bataille. Cela signifie que chacun doit être en mesure de savoir où se trouvent les forces, ce qu'elles font et comment elles se comportent.

Afin de prendre la meilleure décision possible, les commandants militaires se tournent vers l'*Edge* et s'efforcent d'obtenir un avantage sur le terrain.

Pousser l'innovation en première ligne

Les *Clouds* de périphérie et de combat - un ensemble de *Clouds* privés reliant divers éléments du champ de bataille - poussent l'innovation et la numérisation vers la ligne de front, au sens propre comme au sens figuré. Le système *Firefly*[2], qui soutient les forces de l'OTAN, en est un bon exemple. La combinaison de ces technologies fait une réelle différence dans la manière dont les opérations sont menées. Elles permettent au commandant de la mission de disposer des bonnes informations, avec le bon tempo et au bon moment lorsqu'il s'agit de s'engager sur le champ de bataille.

Elles permettent également aux commandants de réagir de manière appropriée grâce aux applications modernes (apps). Aujourd'hui, les applications peuvent être téléchargées et disponibles presque instantanément sur la ligne de front (ou à l'endroit où elles sont nécessaires). En cas de changement de mission, d'environnement ou de menace, les forces peuvent être rapidement équipées d'applications provenant du *Cloud* de combat qui leur permettent de mieux réagir. Le travail que nous effectuons sur Kessel Run[3] avec l'*US Army Futures Command* en est un exemple.

L'*Edge* dans les armées

Toutefois, il n'est pas possible de tirer parti de ces avantages sans une technologie d'*Edge* multidomaine. Il s'agit d'une technologie *Edge* déployée à la fois sur terre, en l'air et en mer. Son impact est la définition de la somme de ses parties car, si tous les domaines ne sont pas connectés et ne communiquent pas, les commandants auront des angles morts et n'auront donc pas une visibilité totale des événements qui se déroulent sur le terrain.

Les technologies d'*Edge* ne sont pas aussi répandues dans les armées que dans d'autres secteurs, comme les télécommunications, en tout cas pas encore. Il est compréhensible que les exigences en matière de sécurité et de fiabilité soient plus strictes, tandis que de nombreuses forces étatiques sont liées par des contrats existants avec des fournisseurs qui peuvent ne pas être en mesure d'offrir une technologie d'*Edge*. D'autres pays ne sont tout simplement pas conçus ou structurés pour tirer parti de cette évolution. La Russie, dont la structure militaire est très monolithique, en est un excellent exemple.

Si le déploiement et les cas d'utilisation des technologies d'*Edge* dans les armées sont pratiquement uniques par rapport à tous les autres secteurs, il y a un aspect qui reste constant, quels que soient le lieu et le mode d'utilisation. Il s'agit de la nécessité de maintenir l'homme au cœur de l'action.

Augmenter le meilleur de l'homme et de la machine

On pense à tort que plus les forces armées seront numérisées, moins il y aura d'interactions et d'interventions humaines. Ce n'est certainement pas le cas ; c'est même tout le contraire. C'est précisément parce qu'une technologie plus avancée est introduite que les humains jouent un rôle de plus en plus vital. Le défi auquel sont confrontées toutes les forces et coalitions est de trouver l'équilibre entre les deux afin de tirer le meilleur de chaque.

2. Agence d'information et de communication de l'OTAN « Agency awards Firefly contrat for deployable communications and information systems », 04/02/2021, URL : https://www.ncia.nato.int/about-us/newsroom/agency-awards-firefly-contract-for-deployable-communications-and-information-systems.html

3. Division Kessel Run « About us », URL : https://kesselrun.af.mil/about/

Tout d'abord, la technologie ne peut pas être considérée comme le seul outil de prise de décision. Si l'art de la guerre consiste à agir rapidement sur la base d'informations précises, et si la technologie est nécessaire pour naviguer dans le brouillard de guerre, l'homme reste le meilleur juge de l'action et le plus fiable. Cela signifie que l'adoption des technologies *Edge* - et d'autres technologies innovantes - enrichit et facilite la prise de décision humaine, en augmentant le potentiel de l'homme et de la machine.

Plus profondément, même en faisant abstraction de l'émotion, de la pression et des enjeux de la guerre, les humains ne font pas suffisamment confiance aux systèmes automatisés. C'est ce que l'on constate aujourd'hui lorsque des dirigeants de grandes entreprises technologiques expriment leur point de vue sur la rapidité de l'adoption de l'IA. Une étude récente[4] s'est penchée spécifiquement sur cette question et a révélé que les décisions entièrement automatisées suscitaient moins de confiance que celles prises par un être humain. En effet, les résultats suggèrent que la confiance dans l'aide à la décision hybride est similaire à la confiance dans la décision humaine seule.

Un facteur déterminant pour les forces en présence

Malgré tous les progrès réalisés par les forces armées en matière d'adoption des technologies, nous restons bien plus proches de la ligne de départ que de celle d'arrivée. Comme le dit l'adage, « *you're never at the end of history, only the middle* » (on n'est jamais à la fin de l'histoire, seulement au milieu).

Il ne fait aucun doute que les futures opérations militaires devront inclure la technologie d'*Edge* sous une forme ou une autre. À tel point qu'elle deviendra un facteur décisif entre les forces armées, et le facteur déterminant entre victoire et défaite.

4. Felix Kares, Cornelius J. König, Richard Bergs, Clea Protzel, Markus Langer « Trust in hybrid human-automated decision-support », International Journal of Selection and Assessment, 01/03/2023, URL : https://onlinelibrary.wiley.com/doi/full/10.1111/ijsa.12423

Forward

vmware