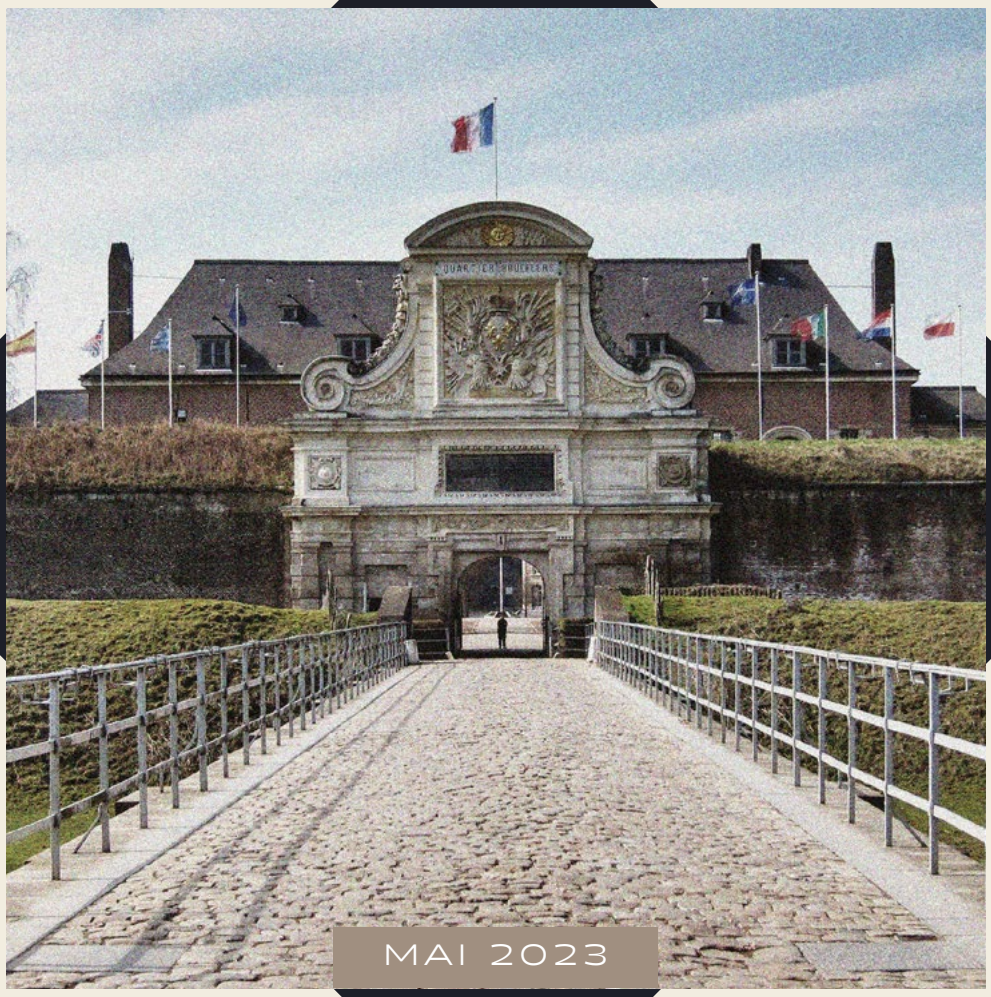
VAUBAN
SESSIONS

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



MAI 2023

Forward

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

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

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

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

À PROPOS DE FORWARD GLOBAL

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

PLUS D'INFORMATIONS SUR :
forwardglobal.com

Forward

À PROPOS DE VMWARE

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

PLUS D'INFORMATIONS SUR :
vmware.com/company

vmware

COLLECTION

VAUBAN PAPERS

PRÉFACE

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