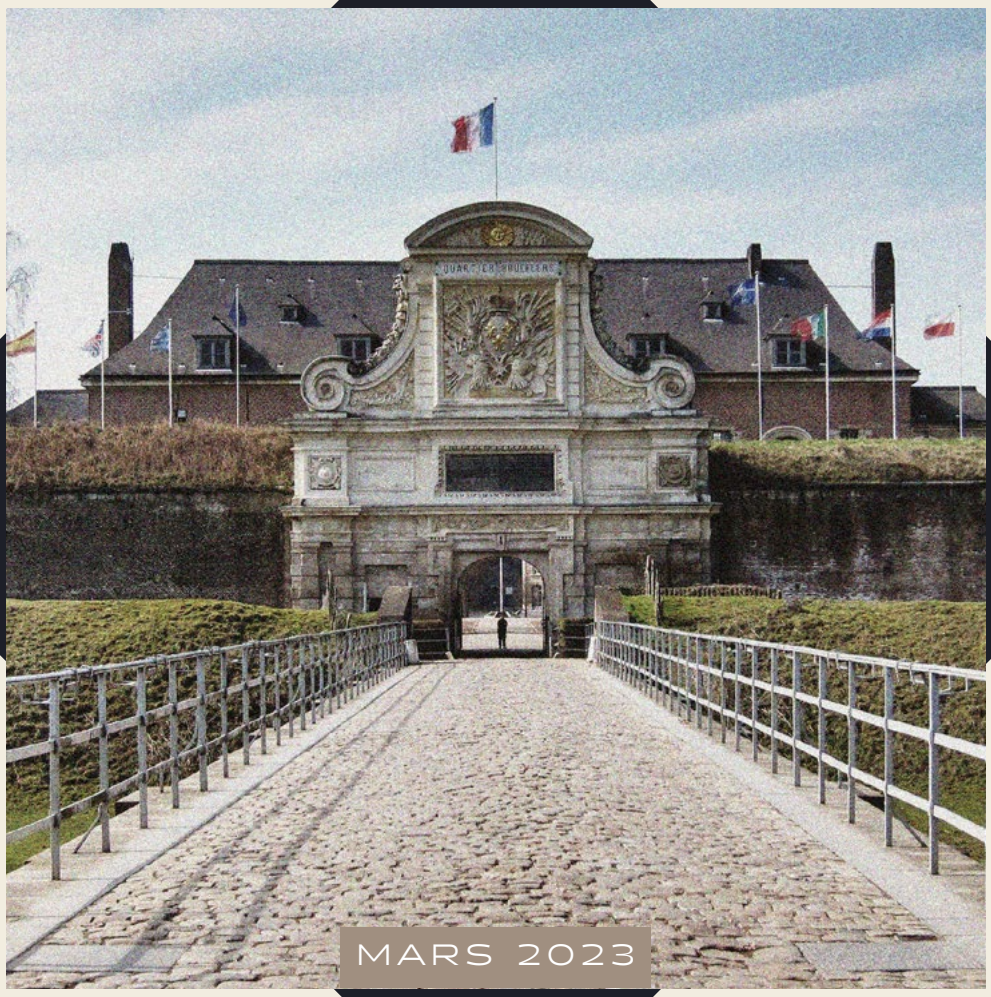
VAUBAN
SESSIONS

#5 MODÈLES DE SERVICES *CLOUD* POUR LA DÉFENSE



MARS 2023

Forward

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

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

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

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

À PROPOS DE FORWARD GLOBAL

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

PLUS D'INFORMATIONS SUR :
forwardglobal.com

Forward

À PROPOS DE VMWARE

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

PLUS D'INFORMATIONS SUR :
vmware.com/company

vmware

COLLECTION

VAUBAN PAPERS

PRÉFACE

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.

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.

Forward

vmware