VAUBAN PAPERS

avisa partners

vmware

WWW.VAUBAN-SESSIONS.ORG

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 Avisa Partners 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 Avisa Partners 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 major de 19 nations alliées, de l'OTAN, de l'Union européenne, et de l'industries de défense.

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

À PROPOS D'
AVISA PARTNERS

Avisa Partners est une société mondiale d'intelligence, d'affaires internationales et de cybersécurité. **La branche Cybersecurité et Stratégie d'Avisa Partners** 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 :
www.avisa-partners.com

avisa partners

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 :
www.vmware.com/company

vmware

COLLECTION

VAUBAN PAPERS

SOMMAIRE

WWW.VAUBAN-SESSIONS.ORG

VAUBAN SESSIONS

VAUBAN PAPERS

#1 LA DONNÉE AU CŒUR DU COMBAT COLLABORATIF

avisa partners vmware

WWW.VAUBAN-SESSIONS.ORG

PRÉFACE

Il y a 20 ans, la « révolution dans les affaires militaires » (RMA) fut décrite comme une approche moderne de l'art de la guerre plaçant l'information au cœur des opérations militaires comme moteur de l'adaptation et de l'efficacité des forces armées. En fait, c'est durant la décennie que la RMA a trouvé sa pleine dimension grâce à l'avènement d'une véritable transformation numérique tirant elle-même parti de technologies de pointe au service de nouveaux concepts. Il est désormais possible de générer, partager, exploiter de vastes quantités de données et d'assurer une dissémination rapide et globale de l'information. Cela permet, en particulier, d'améliorer et d'accélérer le processus de décision en l'appuyant sur un renseignement actualisé et de plus en plus sur l'assistance de moteurs d'intelligence artificielle adaptés. L'efficacité de cette transformation numérique repose tout particulièrement sur l'aptitude à bâtir des réseaux de commandement et conduite des opérations à la fois sécurisés et adaptables. Ceux-ci doivent pouvoir répondre à la diversité des cadres d'engagement opérationnels des forces armées en assurant une connectivité fiable pour l'ensemble des acteurs et en permettant une diffusion sélective des informations pertinentes au bon moment au bon utilisateur. Il est ainsi possible d'optimiser la contribution et la collaboration de chaque acteur de la chaîne opérationnelle, combattant au sol, marin, aviateur, experts de l'espace ou de la cyberdéfense mais aussi celle de systèmes d'armes dirigés à distance, de systèmes dotés d'une certaine autonomie et d'une multitude de capteurs. Ce fonctionnement en réseau généralisé doit permettre aux commandeurs de sélectionner en temps quasi réel la meilleure combinaison des effets militaires qu'il souhaite produire, qu'ils soient cinétiques ou non, pour atteindre ses objectifs opérationnels. Il s'agit là de l'essence même du combat collaboratif qui doit de plus permettre, par conception, la mise sur pied de coalitions multinationales en s'appuyant sur une interopérabilité numérique éprouvée et sur une forte capacité d'adaptation. Le succès du combat collaboratif repose sur une profonde transformation des méthodes de développement, d'acquisition, de mise à niveau, de modernisation et de soutien des capacités militaire. Il doit aussi pouvoir s'appuyer sur la promotion d'une innovation collaborative impliquant ensemble les utilisateurs opérationnels et l'industrie afin de tirer rapidement le meilleur parti des technologies numériques les plus avancées au service des opérations.

Ce premier document fait partie d'une série de publications issues de la dynamique des « entretiens Vauban ». Ceux-ci visent à partager les meilleurs pratiques de la transformation numérique opérationnelle en créant un cadre collaboratif élargi englobant l'ensemble des domaines d'action dans une approche multinationale, associant les acteurs publics militaires et civils et les partenaires industriels.

Général (2S)
Jean-Paul Paloméros

Ancien Commandant suprême allié Transformation (SACT) de l'OTAN et Conseiller Sénior chez Avisa Partners

LA DONNÉE AU CŒUR DU COMBAT COLLABORATIF

Depuis une dizaine d'années, on constate un retour des logiques de puissance et de la compétition interétatique qui ne permet plus d'exclure l'hypothèse d'un conflit armé majeur. Dans ces conditions, l'enjeu pour les forces armées est d'acquérir la supériorité opérationnelle avec des moyens humains et matériels plus efficaces mais en nombre réduit et en devant réagir dans des délais de plus en plus courts. Pour cela, le commandement, confronté à des environnements physique, cyber et électromagnétique contestés, doit disposer d'une appréciation de situation actualisée, la plus fiable possible qu'il puisse partager en temps quasi-réel avec tous les acteurs concernés. Dès lors il lui est possible d'adapter son dispositif dans les délais les plus brefs avec une efficacité maximale.

Engagée depuis environ 20 ans par la société civile comme par les forces armées, la transformation numérique représente une composante clé de cette efficacité. Elle peut apporter aux forces armées la souplesse, la réactivité, et la manœuvrabilité indispensables pour concentrer les efforts et emporter la décision. L'emploi des technologies numériques (internet des objets, intelligence augmentée, *Cloud*, etc.) permet de concevoir un mode de combat « collaboratif » permettant de prendre l'ascendant sur l'adversaire.

La transformation numérique des Armées : une nouvelle donne pour le combat collaboratif

La capacité pour les combattants à agir de la manière la plus collective et coordonnée possible a toujours été l'un des fondements de la supériorité des armées face à leurs adversaires. Cette efficacité est fondée sur la communication entre les différents niveaux de commandement et la conjugaison des différents effets. La numérisation des forces armées permet d'optimiser la manœuvre grâce au partage en temps quasi réel de l'information et à la mise en réseau de l'ensemble des acteurs du champ de bataille, tant de manière horizontale (niveau tactique) que verticale (niveau stratégique).

Cette connectivité accrue a deux incidences directes sur la conduite des opérations :

- Une remontée et un renvoi des informations plus rapides entre les niveaux tactique et stratégique ;
- Une connaissance et une compréhension élargies du champ de bataille, qui doivent permettre de réduire le « brouillard de la guerre ».

Ces éléments peuvent concourir à la supériorité opérationnelle par :

- La détection et l'anticipation quasi instantanée des manœuvres de l'adversaire, grâce aux remontées d'information des capteurs techniques et humains ;
- La prise de décision plus éclairée et plus précise grâce à une évaluation partagée et une actualisation en temps quasi réel de la situation ;
- L'accélération des mouvements de concentration et déconcentration des forces par un partage amélioré de la situation et une transmission immédiate des ordres dans les systèmes de commandement ;
- Une meilleure synchronisation des effets, par exemple de la puissance de feu (tirs de missile, artillerie par exemple) selon l'évolution du champ de bataille.

Sans déroger au principe de concentration des efforts, c'est-à-dire frapper le plus fort possible les points faibles du dispositif adverse, le combat collaboratif dans sa version numérisée procure donc simultanément une plus grande rapidité d'exécution de la manœuvre et un impact décuplé. De surcroît, le combat collaboratif peut se décliner en « interarmées » *(joint warfare)* ou être conduit dans plusieurs domaines *(Multidomain warfare)* : air, terre, mer, espace et cyber.

La donnée et le réseau, organes vitaux du combat collaboratif

Si la numérisation constitue un apport indéniable à la fluidité de la conduite des opérations, elle repose sur deux facteurs essentiels : l'existence et la disponibilité des données et la capacité des réseaux à les acheminer.

> COLLECTE ET TRAITEMENT DES DONNÉES

Dans un contexte militaire, les données désignent l'ensemble des informations factuelles pouvant être collectées sur le terrain à l'aide de capteurs humains et techniques. Depuis le début du XXI^{ème} siècle, la numérisation des plateformes et des équipements a engendré une multiplication des capteurs et en conséquence un accroissement exponentiel des masses de données générées.

Pour que ces données deviennent un avantage opérationnel et non un facteur de surcharge cognitive, il faut également leur donner un sens et les rendre utilisables par les différents échelons de la chaîne de commandement. Le combat collaboratif nécessite par conséquent de disposer d'infrastructures informatiques performantes et sécurisées pour traiter ces données et en tirer des éléments concourant à une meilleure appréciation des situations.

> LE RÉSEAU, CLÉ DE VOÛTE DU COMBAT COLLABORATIF

Pour pouvoir être utilisées et valorisées, les données doivent donc pouvoir être échangées entre le terrain et les centres de commandement. Les données remontées du terrain permettent au commandement une meilleure appréciation de la situation pour pouvoir prendre les plus adaptées et conduire la manœuvre en conséquence. Disposer de réseaux puissants, sécurisés et résilients représente donc une condition indispensable pour que la transformation numérique contribue pleinement à la supériorité opérationnelle des forces armées.

Le caractère critique des réseaux pour les opérations place ainsi la guerre électronique et la cyberdéfense au cœur des enjeux du combat collaboratif : il s'agit de garder la maîtrise de son réseau et d'être capable de neutraliser celui de l'adversaire pour provoquer sa paralysie.

Enjeux et défis du combat collaboratif

Les technologies numériques suivant des cycles d'innovation rapides, la transformation numérique des armées nécessite une (r)évolution permanente. Les défis posés sont autant techniques qu'humains :

> DÉFIS TECHNIQUES

- Classer et diffuser les données traitées selon un critère de pertinence représentatif du besoin de chaque niveau hiérarchique (droit et besoin à en connaître) ;
- Accroître la connectivité et l'interopérabilité entre les différents outils et systèmes d'information, et les rendre résistants aux conditions opérationnelles ;
- Développer des interfaces numériques simples et claires pour prévenir l'infobésité et la paralysie cognitive.

> DÉFIS OPÉRATIONNELS

- Adapter les systèmes de commandement à l'accélération du tempo des opérations ;
- Préparer les Armées à combattre en mode dégradé, c'est-à-dire être en mesure de poursuivre les opérations quand les systèmes d'information sont inutilisables, que soit pour des motifs intentionnels (ex : cyberattaques) ou non intentionnels (ex : perte de liaison).

> DÉFIS HUMAINS

- Prévenir la paralysie décisionnelle pouvant être entraînée par la surcharge informationnelle ;
- Conserver le principe de subsidiarité face à la complexité de l'espace informationnel ;
- Concevoir l'apport de la numérisation comme une aide à la décision restant subordonnée au commandement humain.

AUTEURS

Axel Dyèvre, *Associé, Avisa Partners*

Séverin Schnepp, *ancien Consultant, Avisa Partners*

LA DONNÉE AU CŒUR DU COMBAT COLLABORATIF

Le commandement à l'ère du numérique. Cette question était déjà au programme de préparation à l'école de guerre dans les années 2000. L'armée de Terre est aujourd'hui engagée dans sa mise en œuvre concrète.

La bataille se remporte dans le domaine guerrier et dans la sphère de l'intelligence. Elle débute dès la phase de compétition, se cristallise lors de la phase de confrontation et s'exacerbe lors de l'affrontement. La bataille se joue et se gagne dans le narratif, l'initiative, les flux, l'intégration et l'insertion, la légalité et la légitimité. L'information et les données sont au cœur de ces dilemmes tactiques, opératifs et stratégiques.

Notre adversaire fait de la localisation des postes de commandement (PC) son objectif principal de renseignement. Le PC peut être neutralisé techniquement dès la phase de compétition, inhibé psychologiquement par des actions hybrides lors de la phase de confrontation et détruit physiquement dans un délai inférieur à 72 heures lors de l'affrontement. Un poste de commandement a pour but principal de permettre au commandant opérationnel de prendre les bonnes décisions à temps. Il se structure et organise son fonctionnement pour à la fois diminuer son empreinte au sol et dominer l'adversaire dans le duel de l'esprit. Les nouvelles conflictualités nous imposent de réduire les vulnérabilités des PC et d'optimiser les potentialités offertes par les nouvelles technologies afin de créer les conditions de la victoire physique.

Le Corps de Réaction Rapide - France (CRR-FR) mène des études sur le nouveau concept de PC de niveau 1 pour répondre à ces deux défis. L'objectif est de rendre plus agile le processus de décision et d'organiser les cellules du PC en conséquence. La difficulté consiste à maintenir la permanence du commandement tout en réduisant les fonctions opérationnelles présentes dans la zone d'action. Il s'agit de conduire des opérations aussi bien au contact que dans la profondeur avant et arrière dans un environnement contesté dans tous les domaines.

Cependant, les capacités SIC ont un impact direct sur l'organisation et le fonctionnement du poste de commandement. La maîtrise de la numérisation et de l'intelligence artificielle permet de décider opportunément en captant les informations utiles à la prise de décision. Il faut donc rallier les moyens SIC en tenant compte des avancées technologiques, être réaliste tout en étant économe sur la ressource demandée. De plus, l'environnement de guerre électronique, électromagnétique et cyber est contraint et contesté.

Pour cela, le poste de commandement doit disposer de Systèmes d'Information Opérationnelle et de Commandement (SIOC) fiables et ergonomiques qui lui permettent de garantir les flux nécessaires à la planification et à la conduite, de disposer de réseaux difficilement attaquables, d'être interopérable en particulier avec les Alliés et d'augmenter sa réactivité en disposant des outils techniques d'aide à la décision et d'exploitation des données.

Ce sont les conditions nécessaires pour permettre au commandement de conserver la supériorité d'exécution en imposant son rythme et en déroulant sa manœuvre sans laisser de répit à l'adversaire.

AUTEUR

Général de Corps d'Armée

Pierre Gillet

Commandeur du Corps de Réaction Rapide France (CRR-FR)

LA DONNÉE AU CŒUR DU COMBAT COLLABORATIF

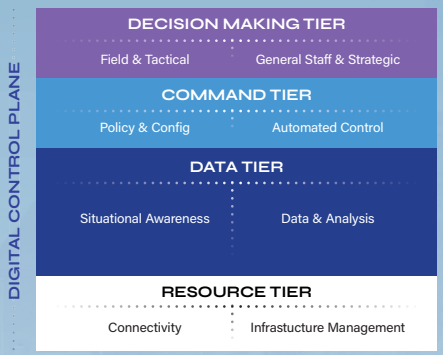
VMware Research aspire à soutenir les forces armées dans leur transformation numérique et dans le développement du combat collaboratif. Nous développons une architecture informatique multi-niveaux, le *Military Digital Control Plane* ou MDCP (plan de contrôle numérique à des fins militaires), qui comprendra plusieurs paliers hiérarchiques. Le MDCP doit permettre d'optimiser le périmètre, la capacité et la performance de la chaîne opérationnelle tout en offrant une interface plus intuitive et ergonomique aux utilisateurs. Le contrôle de la collecte, du traitement et de l'exploitation des flux de données, à l'image de notre système nerveux, procurera aux Armées un avantage décisif dans l'atteinte de leurs objectifs stratégiques et opérationnels.

Les réseaux de télécommunication mondiaux se dématérialisent et s'appuient chaque jour de plus en plus sur des systèmes de logiciels connectés. Ce modèle d'architecture réseau, appelé *software-defined networking* ou SDN, permet de découpler le plan de données du plan de contrôle. Le plan des données permet de faire circuler les données de mission dans les « tuyaux » de l'organisation. Le plan de contrôle, quant à lui, configure ces « tuyaux », c'est-à-dire leurs capacités en vertu des politiques qui régissent les données. En séparant les deux plans, les architectes réseaux sont désormais capables d'atteindre des débits sensiblement plus élevés tout en optimisant, en sécurisant et adaptant les réseaux aux besoins des utilisateurs.

VMware Research s'est inspiré du concept de SDN pour pousser encore plus loin la séparation des différentes fonctions dans la construction du MDCP. Dans cette nouvelle approche, 4 domaines se superposent : les ressources, ; les données, la direction, et la prise de décision. Le plan de contrôle du réseau est ainsi amélioré pour le concentrer sur « l'intelligence de la donnée », c'est-à-dire l'aptitude à répartir le flux de données et d'information entre les domaines et les différents niveaux de l'organisation militaire. Chaque niveau pris individuellement comporte également des variables et critères adaptés aux fonctions et préoccupations des différentes parties prenantes.

Dans l'espace des données, l'innovation est omniprésente à tous les niveaux. Le concept MDCP encourage la séparation des fonctions, et permet aux différents niveaux d'évoluer séparément et rapidement, tout en maintenant une capacité de connexion et de collaboration entre eux. VMware Research reste ancré dans la réalité opérationnelle et l'interconnexion des niveaux hiérarchiques. Ainsi, le MDCP nourrit chaque niveau avec les informations nécessaires et appropriées. Il facilite la communication entre les différents domaines mais également au sein de chacune des fonctions opérationnelles. Le résultat est une gestion des données plus dynamique, plus globale et mieux contrôlée.

Les fonctions et caractéristiques de chaque niveau du MDCP seront détaillés dans les prochaines publication. Pour introduire ces travaux, il convient tout d'abord de décrire le fonctionnement du MDCP dans son ensemble. Le niveau des ressources (*Resource Tier*) désigne à peu près l'environnement actuel du *Cloud* hybride s'appuyant sur une connectivité globale intégrant les terminaisons périphériques, et assurée par différentes infrastructures de calcul et de capteurs. Une fois ces éléments en place, il devient possible de développer le niveau des données (*Data Tier*) en tirant parti des innovations commerciales qui révolutionnent l'exploitation des données dans une dynamique concurrentielle. Trop souvent encore, les opérations permises par l'agilité multi-*cloud* sont entravées par l'inertie du traitement des donnée. La création d'un niveau spécifique (*Data Tier*) permettant le traitement des flux de données virtualisées, pilotés par des moteurs d'intelligence artificielle, vise à alimenter de manière sélective les autres niveaux du MDCP. Cette approche beaucoup plus souple répondrait ainsi de manière ciblée tant aux besoins opérationnels prévus, qu'aux exigences spécifiques de chaque mission ou encore aux limites techniques des moyens de communication d'extrémité. Le niveau de direction (*Command Tier*) doit permettre d'assurer une gestion toujours plus virtualisée de l'activité numérique, allant d'opérations abstraites à des contrôles de sécurité et d'accès aux données basés sur des politiques spécifiques. L'ensemble serait alimenté par les mises à jour automatisées par ML émanant du niveau des données (*Data Tier*).



En fin de compte, les niveaux de ressources (*Resource Tiers*), de données (*Data Tiers*) et de direction (*Command Tiers*) visent tous à permettre une optimisation de la prise de décision, pour assurer la mission essentielle de Commandement et Contrôle inhérente à toute organisation militaire. Au fil du temps, l'évolution des systèmes de C2 s'est faite par extension de périmètre et ajout de fonctions s'étendant jusqu'au C4ISR et même au-delà. Ce faisant, elle s'est quelque peu écartée du besoin fondamental de commandement et de contrôle des opérations. L'approche MDCP fournit au contraire un niveau décisionnel (*Decision Making Tier*) puissamment virtualisé pour mobiliser les résultats de l'analyse des données et la connaissance de la situation opérationnelle (*Data Tiers*) au profit des décideurs stratégiques aussi bien qu'aux commandements tactiques. Cette nouvelle approche soutenue par des applications innovantes se concentre sur le besoin de l'utilisateur et sur la nature des missions à accomplir. Grâce aux importants flux de données abreuvant le MDCP, les décideurs peuvent recevoir des renseignements actualisés et pertinents, mais aussi transmettre leurs intentions et leurs ordres via un système intégré, capable de s'adapter aux réalités opérationnelles. Cette identification plus précise des différents niveaux du MDCP associé à leur couplage interactif permettra d'accélérer l'introduction des innovations techniques, de s'adapter à la complexité grandissante de l'environnement numérique. Pour les futurs commandeurs, elle procurera surtout les moyens de mieux contrôler leurs systèmes de commandement et de communication et de profiter d'une grande maîtrise de l'information.

La finalité du MDCP est de maximiser le périmètre et les performances de chaque niveau par la spécialisation et l'innovation en boucle courte, tout en permettant une configuration et une gestion à grande échelle par des moyens de programmation de logiciels plus souples (déclaratifs). Le concept de niveaux coordonnés présenté ici sera une nouvelle phase importante dans l'industrialisation des technologies de l'information. VMware Research travaille activement à des interfaces informatiques déclaratives, inspirées de Kubernetes et de techniques de virtualisation connexes. Cette approche dynamique et innovante nous permettra à court termes de développer des systèmes toujours plus proches du besoin de l'utilisateur. dotés d'interfaces homme/machine, performantes dans le but de faire des données le cœur vibrant de toute organisation.

AUTEURS

David Tennenhouse

Ancien Chief Research Officer, VMware

Robert Ames

Senior Director, Emerging Technology, VMware

Lewis Shepherd

Senior Director, Research & Emerging Technologies Strategy, VMware

VAUBAN SESSIONS

VAUBAN PAPERS

#2 LES DONNÉES AU SERVICE DU COMBATTANT : ENJEUX ET OPPORTUNITÉS

avisa partners vmware

WWW.VAUBAN-SESSIONS.ORG

PRÉFACE

La transformation numérique que vivent les forces armées touche aujourd'hui tous les niveaux de commandement, de contrôle mais aussi de plus en plus, au niveau tactique, le combattant quel que soit son champ et son domaine d'action, terrestre, maritime, aérien, spatial, cyberespace ou encore l'espace de l'information.

De longue date, la numérisation des systèmes d'armes a constitué un axe d'innovation et de modernisation des capacités opérationnelles. Elle a permis des progrès notables que ce soit pour la connectivité des forces, l'appréhension en temps réel de la situation tactique, l'identification des objectifs, la précision des armements, la miniaturisation des différents sous-systèmes opérationnels.

De réels efforts d'intégration ont permis d'exploiter au mieux l'état de l'art de cette numérisation au service de l'efficacité d'ensemble des opérations militaires.

Cependant les limites et les contraintes de cette transformation numérique opérationnelle sont clairement apparues à l'aune du retour d'expérience des opérations et des exercices. Ainsi, les capacités, la continuité et la fiabilité des moyens de communication constitue plus que jamais un impératif mais aussi, bien souvent, une limite alors que les besoins d'échanges d'informations ne cessent de croitre. De même, alors que le monde civil voit une modernisation constante de ses moyens de communication au rythme effréné des innovations technologiques, la mise à disposition rapide des forces armées de moyens aussi avancés demeure un réel défi. La transformation numérique doit en effet prendre en compte les besoins de rusticité, de cybersécurité, mais aussi répondre au besoin vital d'interopérabilité au sein des forces nationales mais aussi entre alliés.

Cependant, aujourd'hui une étape importante de la numérisation opérationnelle se dessine, celle de la généralisation de la donnée comme un élément essentiel du savoir et du pouvoir, comme un moteur de l'innovation, comme un bien précieux qu'il faut faire fructifier, savoir exploiter et partager.

Dans la suite de la première publication de la série « Vauban Papers » de portée générale, l'objectif de ce deuxième document est d'aborder les enjeux et les défis de la transformation numérique opérationnelle au niveau tactique. Il s'agit d'évaluer les bénéfices attendus à ce niveau de la mise à disposition et de l'exploitation des gigantesques flux de données générées par les nombreux capteurs de terrain, par les combattants eux-mêmes et par leurs nouveaux systèmes d'armes. Il s'agit aussi de déterminer l'apport potentiel des nouvelles capacités qu'offre l'informatique en périphérie de réseau *(edge computing)* en particulier pour tirer le plein parti de capteurs intelligents de nouvelle génération, au plus près du combattant.

L'exploitation généralisée des données au niveau tactique représente aujourd'hui une opportunité opérationnelle indéniable et sans doute un facteur de changement majeur. Encore faut-il bien en mesurer les fragilités et savoir y répondre que ce soient les risques de « *data* dépendance » ou encore les questions de fiabilité et de cybersécurité associées.

C'est à ce prix que la transformation numérique apportera une contribution essentielle au combat collaboratif.

Général (2S)
Jean-Paul Paloméros

Ancien Commandant suprême allié Transformation (SACT) de l'OTAN et Conseiller Sénior chez Avisa Partners

LES DONNÉES AU SERVICE DU COMBATTANT : ENJEUX ET OPPORTUNITÉS

Le combat collaboratif demande un partage continu en temps quasi réel des données collectées sur le champ de bataille. Une fois celles-ci traitées, les acteurs de la chaîne de commandement disposent d'une vision complète de la situation opérationnelle, permettant aux différents niveaux de prendre des décisions avec le meilleur niveau d'information possible. Dans cette « bulle numérique », les capteurs embarqués[1] par les forces déployées jouent un rôle déterminant pour alimenter les systèmes d'informations et de communication (SIC). En retour, les combattants déployés peuvent s'appuyer sur l'actualisation régulière de la situation opérationnelle pour faciliter et optimiser la conduite de leurs missions.

Mais si les avantages offerts par les nouvelles technologies en opération sont évidents (ex : détection de l'adversaire et/ou neutralisation de ses capacités), leur emploi ne saurait affranchir les combattants des exigences opérationnelles d'adaptabilité, d'agilité et de résilience. En effet, l'environnement géophysique tout comme les actions de l'ennemi peuvent empêcher ou limiter l'usage de ces technologies. Les forces doivent dès lors être prêtes à conserver leurs capacités opérationnelles dans des conditions dégradées ou un environnement contesté.

Les données au service des unités tactiques

L'actualisation continue de la situation opérationnelle locale *(Local Operational Picture - LOP)* et commune *(Common Operational Picture - COP)* permet de faciliter la planification et la conduite collaborative de l'opération. Il s'agit en effet de générer la vision la plus juste et la plus complète de la situation opérationnelle, en identifiant tant les positions des troupes amies *(Blue Force Tracking),* que celles ennemies *(Red Force Tracking)*[2]. Le partage en quasi-temps réel des LOP et COP présente un double avantage pour le niveau tactique :

- Une plus grande efficacité - rapidité et impact - dans la planification comme dans la conduite des opérations grâce à une situation actualisée de manière plus rapide et précise.

- Une plus grande sécurité en conduite grâce à une meilleure connaissance des menaces et des risques.

Conséquence directe de l'actualisation plus rapide de la situation ami-ennemi, le rythme des opérations s'en trouve considérablement accéléré.

Soutenir et protéger les combattants : une exigence de connectivité & de cybersécurité

Si la transformation numérique apporte aux forces armées des avantages opérationnels indéniables, la multiplication des communications et l'augmentation des volumes de données échangés présentent aussi des risques qui, à défaut d'être nouveaux, sont considérablement renforcés :

- Une dépendance accrue aux ondes du spectre électromagnétique pour assurer la connectivité de leurs moyens, alors que les conditions naturelles peuvent bloquer ou limiter l'usage de ces ondes.

- Une surface d'exposition accrue aux actions de l'ennemi dans le champ de la guerre électronique et des attaques dans le champ cyber pouvant endommager, corrompre ou exposer les données et les systèmes d'information.

Ainsi, si les forces armées doivent disposer de capacités leur permettant de conduire le combat en mode collaboratif pour prendre l'avantage sur leurs adversaires, elles doivent aussi - avec ces mêmes moyens - être en mesure de combattre dans un environnement dégradé et/ou contesté sans que leur efficacité opérationnelle n'en soit trop amoindrie. Le relief du terrain, les actions de guerre électronique[3], ou la destruction

1. Disposés sur les combattants, les véhicules, et les drones.

2. En localisant notamment les différents centres de gravité du système adverse comme les postes de commandement, les infrastructures logistiques, les regroupements de forces et les points de passage de celles-ci.

3. Comme le brouillage des ondes radio par lesquelles les communications et les transferts de données sont opérés.

de composantes critiques du réseau par le feu ennemi, sont autant de causes susceptibles de priver les unités engagées de moyens de communication. Les actions de l'ennemi dans le champ cyber peuvent aussi porter sur les protocoles, les couches système ou les données elles-mêmes. Dans tous les cas, la disponibilité, la complétude et l'intégrité des données échangées peuvent être remises en cause. Il faut donc que les capacités soient dimensionnées en fonction de ces nouveaux enjeux, et que les doctrines d'emploi et l'entraînement soient adaptés pour préparer le combattant à y faire face.

Si le secteur civil n'est pas confronté aux mêmes enjeux, certaines solutions qui y sont développées peuvent toutefois être adaptées et durcies pour les usages militaires. Les armées peuvent notamment profiter des progrès fait dans le domaine du *edge computing*[4], cette méthode informatique consistant à collecter et traiter la donnée localement, au plus proche de l'utilisateur, en intégrant dans les appareils électroniques (*edge devices*) des capacités de traitement (intelligence embarquée)[5]. Dans cette approche décentralisée de la gestion des données, l'emploi du *edge computing* au profit des armées doit s'accompagner du développement d'un véritable « internet des objets » (*IoT*)[6] militaires. Au sein de celui-ci, les équipements individuels et collectifs doivent disposer de leurs capacités propres de stockage et de calcul informatique pour pouvoir fonctionner de manière autonome, quelles que soient les circonstances. Les bénéfices du *edge computing* pour les organisations militaires sont triples[7] :

- **Réduction du volume des échanges et réduction de l'exposition à la latence :** toutes les données ne sont pas remontées à un serveur central. À l'inverse, le traitement local rend la disponibilité des résultats plus rapide.

- **Renforcement de la cybersécurité des données :** le caractère décentralisé du *edge computing* rend plus difficile la possibilité de neutraliser simultanément l'ensemble des appareils en périphérie (contrairement à un serveur[8]). Mais le *edge computing* revient pour les hackers à augmenter le nombre de « portes d'entrée » disponibles, requérant un haut niveau de cybersécurité sur tous les appareils[9]. Dans le cas où un virus informatique infecterait une partie du réseau, il est possible d'introduire des protocoles de sécurité afin d'isoler les parties compromises (segmentation) et d'empêcher la progression du virus sur d'autres appareils. Le risque de capture par l'ennemi des moyens connectés renforce aussi le besoin d'authentification et de chiffrement maximum en local des données.

- **Flexibilité et modularité dans la gestion des données :** en combinant *edge & cloud computing*, les armées peuvent allouer les ressources disponibles selon les besoins, permettant d'étendre les capacités de collecte et de calcul. Afin de tirer le meilleur parti de ce « *cloud* tactique » combinant les avantages du *cloud* et la souplesse de l'*IoT*, les armées doivent développer une gestion efficiente des données. En pratique, cela signifie définir celles qui doivent être toujours disponibles localement et celles qui doivent être échangées et à quel rythme, sachant que les besoins peuvent évoluer selon les phases d'engagement et les conditions.

D'un point de vue opérationnel, l'emploi du *edge computing* pour les unités tactiques permet :

- Une plus grande mobilité, car les troupes sont moins dépendantes du réseau.

- Une discrétion accrue des mouvements avec une réduction des échanges de communications et de données.

- Une plus grande rapidité dans l'exécution de la mission, grâce à un traitement des données au plus près du besoin.

- Une plus grande flexibilité permettant des reconfigurations rapides des dispositifs, la dépendance à des instances centralisées étant réduites.

4. En français « informatique en périphérie »

5. Le *edge computing* s'oppose au *Cloud computing* qui consiste à transférer et traiter la donnée sur un serveur plus éloigné - nécessitant un réseau fiable et ininterrompu pour permettre la circulation des données.

6. « *Internet of Things* » ou « *IoT* »

7. « *The benefits, potential and future of edge computing* », VxChange, 29/04/2021, URL

8. Notamment les attaques de type DDoS ou « déni de service » (*Distributed denial of service*) qui visent à rendre un serveur, un service ou une infrastructure indisponible via la saturation de la bande passante du serveur, un épuisement des ressources systèmes de la machine - Voir « Qu'est-ce que l'anti-DDoS », OVH, URLbande passante du serveur, un épuisement des ressources systèmes de la machine - Voir « Qu'est-ce que l'anti-DDoS », OVH, URL

9. En l'occurence, le maillon le plus faible de la chaîne cyber détermine la capacité de résistance de l'ensemble.

PROJET LELANTOS[10]
DÉVELOPPEMENT D'UN POSTE DE COMMANDE TACTIQUE MOBILE

Au-delà des opérations de combat, la numérisation du champ de bataille nécessite également de disposer d'un poste de commandement (PC) tactique plus mobile, afin de réduire le risque d'être détecté. En ce sens, le projet Lelantos[11] conduit par l'Allied Rapid Reaction Corps (ARRC) de l'OTAN est particulièrement novateur au regard de l'agilité qu'il apporte au PC tactique de l'ARRC (ARRC TAC). Ce dernier consiste en un container expansible (*Mobile Expandable Container Configuration - MECC*) transporté sur un camion afin de pouvoir le déplacer rapidement selon l'évolution des opérations et du dispositif. Ce centre de commandement souple et modulaire peut être déployé et mis en œuvre de manière très rapide avec un personnel rapide, contribuant à la sécurité des opérations et à la survivabilité du PC qui en est équipé.

Préparer les combattants au champ de bataille numérisé

Pour que les avantages induits par la transformation numérique l'emportent sur les risques et défis qu'elle peut présenter, il est crucial pour les forces d'apporter des réponses adaptées à un certain nombre d'enjeux.

> DÉFIS TECHNIQUES

- Développer des appareils dotés d'une intelligence embarquée pour optimiser la circulation des données, tout en prenant en compte les contraintes techniques de taille et poids, de consommation énergétique, de signature thermique, et de dissipation de chaleur.

- Renforcer la sécurité et cybersécurité des équipements pour s'assurer qu'ils ne présentent pas de danger en cas de perte ou de capture par l'ennemi. Les protocoles de sécurité peuvent par exemple provoquer la destruction logique ou physique de l'appareil ou du système compromis, ou encore altérer les données accessibles à des fins d'intoxication de l'adversaire.

- Assurer la continuité de service de l'infrastructure : si une brique du réseau n'est plus fonctionnelle, l'architecture réseau doit permettre de minimiser la dépendance à des nœuds critiques et donner la meilleure garantie de haute disponibilité de service à tout moment.

- Maîtriser la traçabilité des chaînes d'approvisionnement pour contrôler la cybersécurité des équipements et composants technologiques sensibles[12].

> DÉFIS OPÉRATIONNELS

- Maintenir un haut niveau de discrétion : les équipements électroniques des unités tactiques doivent réduire au maximum leurs signatures sonores, électromagnétiques et thermiques pour empêcher la détection par l'adversaire.

- Disposer des moyens de neutraliser, compromettre et intercepter les SICs de l'ennemi : les unités au niveau tactique doivent être appuyées par des capacités offensives de guerre électronique et cyber pour réduire ou supprimer les capacités opérationnelles adverses.

- Se préparer à combattre en mode dégradé ou en environnement électromagnétique et cyber contesté : les forces doivent être en mesure de poursuivre leurs opérations et de mener à bien leur mission, ce qui suppose un entraînement préalable à ces conditions dégradées, outre l'entraînement à l'usage optimal des systèmes de combat collaboratif.

> DÉFIS HUMAINS

- Développer des interfaces ergonomiques et faciles à lire : le combattant, quel que soit son niveau dans la chaîne de commandement, doit disposer d'équipements lui permettant de réduire sa charge cognitive. Les équipements doivent délivrer les informations transmises de manière instinctive, sans besoin de réflexion et d'analyse, son attention devant rester concentrée sur son environnement et la conduite de sa mission.

- Développer au sein des SIC des briques logicielles permettant d'identifier plus vite des anomalies issues d'erreurs humaines ou technique dans les données collectées (ex. : mauvais relevé GPS ou compte-rendu erroné) et proposer des solutions pour réduire les risques associés aux données erronées[13].

AUTEURS

Axel Dyèvre, *Associé, Avisa Partners*

Séverin Schnepp, *ancien Consultant, Avisa Partners*

10. *« Corps innovation: exponentially increasing survivability, command and control »*, OTAN, 14/12/2020, URL

11. *« Innovating, Ready for the Future »*, Allied Rapid Reaction Corps, 01/12/2021, URL

12. *Cybersecurity by design*

13. *Johan Schubert & Al, « Artificial intelligence for decision support in Command and Control Systems »*, Swedish Defence Research Agency (FOI), URL

En septembre 1915, l'armée britannique perdait plus de 50 000 hommes lors de la Bataille de Loos. Au même moment, le premier char d'assaut sortait des chaînes de production en Angleterre. Peu de gens à l'époque auraient pu prévoir l'impact considérable du blindage sur la conduite des opérations. Il devint évident dès la bataille de Cambrai en 1918 que cette technologie dominerait le combat conventionnel, le blindage constituant un changement de paradigme profond.

Le monde a évolué, mais le progrès technologique suit désormais une courbe exponentielle. Nous sommes entrés au cœur de l'ère de la donnée. La défense traverse un changement de paradigme de la même ampleur que celui amené par *« Little Willy »* et ses successeurs. Quatre domaines clés méritent une réflexion : l'impact de la numérisation sur la conduite des opérations ; sur nos personnels ; sur nos structures ; et sur la « paix ».

La numérisation de la guerre

L'avènement d'un « nouveau » domaine avec le cyber espace est l'une des facettes de la transformation numérique, mais ne reflète pas sa totalité. L'intelligence artificielle (IA) divise les opinions : certains la craignent, tandis que d'autres sont tout à fait disposés à transférer une partie de la décision des humains aux machines. Quoi qu'il en soit, l'IA deviendra un facteur central du combat, qui apportera sans doute un avantage non nul à ceux qui sauront le plus vite s'y adapter. L'intelligence artificielle permet d'accélérer le rythme des opérations, en mettant en oeuvre des moyens et une vitesse d'exécution à grande échelle dépassant les capacités de l'adversaire. Si la conduite de la guerre va rester un concept fondamentalement simple — et la capacité à prendre et garder l'initiative un élément essentielle de la victoire — les interactions entre les États adverses et leurs forces deviendront plus complexes et dépasseront les capacités de l'homme seul. La capacité d'acquérir, de traiter, de comprendre et d'agir sur les données, tant dans des environnements physiques que virtuels, sera mise à rude épreuve par la complexité des engagements, sauf à s'appuyer sur la puissance de traitement de l'informatique moderne. De mon point de vue d'officier de cavalerie, il ne s'agit pas d'oublier l'importance du matériel, mais de mieux prendre en compte l'interaction entre « capteurs » et « tireurs ». La numérisation engendre une forme de délégation pour optimiser la prise de décision et mettre en œuvre les capacités à une vitesse dépassant l'adversaire. Des logiciels, mis au point par une base industrielle de défense toujours plus performante, permettent d'acquérir, suivre et éliminer des menaces tactiques sans intervention humaine. L'objectif doit rester un monde dans lequel ceux qui exercent le commandement peuvent utiliser les données pour obtenir un avantage, dans lequel les calculs et les variables stratégiques — comme le *schwerpunkt* dans la défense de l'adversaire — émanent de calculs informatiques en temps quasi-réel. L'art du commandement — le « moment *Kingfisher* » de Lawrence — étant d'avoir le courage de prendre des risques ou de mener des actions décisives. C'est là que le jugement humain l'emporte sur les algorithmes : tromper, feinter, exploiter, consolider, etc.

Renforcer l'autonomie et l'efficacité des personnes

Ne craignez pas l'obsolescence. : l'art de la guerre restera une entreprise fondamentalement humaine. Il convient cependant pour nous commandeurs de garder en mémoire une statistique souvent citée sur le marché du travail civil : 86% des métiers qu'exerceront les écoliers d'aujourd'hui n'ont pas encore été inventés. Malgré l'orgueil de cette affirmation, nous devons anticiper et rester agiles : la technologie va changer le visage des armées.

Les machines feront ce que fait l'homme aujourd'hui, mais n'est-ce pas là l'occasion d'employer nos forces de manière nouvelle ? Il serait présomptueux de dire

comment exactement, mais on pourrait envisager, tel l'analogie de la *« Three Blocks Warfare »* de Krulaks, que les machines soient plus impliquées dans la conduite des opérations de front en utilisant l'IA d'une part, et qu'une partie des forces se concentre sur les efforts critiques de maintien de la paix et de stabilisation de l'autre. La victoire étant plus difficile à maintenir qu'à obtenir.

Changements structurels

L'impact sur les forces s'accompagne d'un impact sur les structures. Nous devrons être agiles dans l'adaptation de nos structures au potentiel de la numérisation, plutôt que de plier la numérisation à l'ordre actuel. C'est folie que de limiter un logiciel à des conventions anachroniques de gestion des forces. Nous devrons identifier les dénominateurs communs chevauchant l'ancien et le nouveau, puis déterminer comment ceux-ci s'assemblent pour former les structures à venir. Notre compréhension de la « composition » et de la « jonction » des échelons des opérations portera tant sur la programmation que sur les organigrammes du C2. Un système de systèmes agnostique pourrait être l'objectif pour arriver à une chaine capteur-tireur réellement efficace : la hiérarchie tient moins à un processus linéaire qu'à des conditions prédéfinies - comme par exemple les possibilités de tir en terrain libre par opposition à celles en milieu urbain et comment la programmation pourrait définir les « règles » et les critères pour les forces déployées.

La « paix »

D'un point de vue économique, la donnée fait désormais partie des « marchandises » les plus échangées. Les méta-données fournissent aux banques, compagnies d'assurance, entreprises et gouvernements un avantage dans leur prise de décision. La valeur des données est telle qu'elle fait désormais l'objet d'une concurrence entre États pour les acquérir, les influencer, telle que révélée par le débat sur l'accès d'entreprises chinoises et la 5G. On peut penser que la « paix », entre concurrents, va changer de visage avec une phase de « façonnage » indéfinie avant une crise indéfinie. Une phase pendant laquelle il faudra collecter et stocker des données sur l'adversaire pour obtenir un avantage informationnel avant une crise ou un conflit. On obtient de l'IA ce que l'on y met, et nous verrons un intérêt croissant pour la constitution de banques de données en amont des conflits, afin d'assurer ou de refuser l'avantage à qui tirera le premier. Cela affectera ce qui constitue la concurrence, la crise et la dissuasion, et sur les différents niveaux du combat. Et provoquera une réflexion sur les théories qui ont défini notre approche occidentale de la guerre depuis le Traité de Westphalie.

Nous vivons une époque intéressante et passionnante. Nous ferions bien de nous rappeler que ceux qui doutaient de la valeur des « chevaux de fer » ont fini par en dépendre.

AUTEUR

Général

Sir Edward Smyth-Osbourne KCVO CBE

Ancien Commandeur de l'Allied Rapid Reaction Corps (ARRC)

LES DONNÉES AU SERVICE DU COMBATTANT : ENJEUX ET OPPORTUNITÉS

Dans l'article inaugural de cette série[14], nous avons présenté le Military Digital Control Plane ou MDCP (plan de contrôle numérique à des fins militaires). Conçu comme une architecture hiérarchisée, le MDCP intègre les différents domaines qui contribuent à la transformation numérique opérationnelle. Ainsi le MDCP doit-il permettre d'optimiser le périmètre, la capacité et la performance de chacun de ces ensembles dans leur discipline respective, tout en offrant aux utilisateurs une interface plus ergonomique et intuitive. Ce deuxième article se concentre sur le niveau central, celui des données (*Data Tier*). Il s'agit en particulier d'identifier les défis et les opportunités que représentent ces données au niveau tactique. De plus, certains éléments indissociables du traitement des données et qui touchent aux fonctions de direction et de contrôle de l'ensemble du MDCP sont également abordés.

En premier lieu nous partons du principe que l'entité concernée dispose d'un niveau de ressources (*Resource Tier*) entièrement fonctionnel, assurant une connectivité totale et une gestion globale, dynamique et efficace des ressources disponibles (*Hybrid cloud*, terminaisons périphériques, infrastructures de calcul et capteurs). Ces conditions sont fondamentales pour la réussite de la transformation numérique opérationnelle. Une fois ces éléments en place, il est possible de concevoir les données au sein d'un ensemble cohérent et capable de s'adapter aux besoins de l'organisation. Cet ensemble des données ne doit pas être contraint par des frontières physiques, au contraire, il doit permettre la circulation intelligente des données dans l'organisation, des capteurs aux applications et aux utilisateurs, en passant par les analyses et les bases de données, et inversement. Tout comme notre sang circule dans notre corps, les données de l'organisation du futur circuleront au moment choisi, selon les besoins, et par le cheminement le plus adapté. Ces flux de données seront guidés par le cerveau - dans ce cas, le niveau de direction et contrôle (*Command Tier*), lui-même piloté par le niveau de décision (*Decision-Making Tier*). La circulation et l'échange des données refléteront précisément la politique et les intentions et de l'organisation telles qu'exprimées par le commandement qui pourra s'appuyer sur le plan de contrôle numérique pour synchroniser les différents domaines, évalue et gérer l'efficacité de la configuration de l'ensemble du dispositif.

Aujourd'hui, les systèmes classiques d'exploitation des données présentent une forte inertie qui oblige les organisations à faire évoluer régulièrement leurs applications pour pallier ce manque d'agilité. Le développement d'un niveau de données indépendant mais intégré au sein du MDCP, permet de répondre à cette contrainte en particulier pour répondre aux besoins du niveau tactique. Ainsi il est possible de concevoir des capteurs déployés à la périphérie et capables de collecter des données de nature différentes, des fréquences radio à la vidéo en temps réel et bien d'autres champs d'application. Dans la logique du MDCP, Il appartiendra au niveau des ressources de prendre en charge les capteurs eux-mêmes, en configurant leur connectivité et en assurant leur sécurité. C'est également au niveau des ressources que seront alloués les moyens les plus appropriés pour traiter les données et assurer leur traitement en ligne. Il sera également possible d'intégrer des sous-systèmes préétablis directement au niveau des capteurs

Dans ces conditions, les données générées par le capteur pourront être analysées en temps réel, référencées et conditionnées en fonction des besoins de l'organisation.

Quels sont les avantages de cette nouvelle approche ? Aborder globalement les données au sein d'un ensemble cohérent tel que le définit le MDCP doit permettre d'identifier les contraintes de l'environnement au niveau tactique et de s'en affranchir de manière dynamique.

Ainsi prenons le cas d'un capteur déployé sur un navire disposant d'une connectivité limitée. La gestion des ressources au niveau local doit faciliter l'utilisation des capacités de calcul/mémoire « cache » disponibles de manière sélective. De même, une analyse dynamique des modèles de bandes passantes utilisées sur le navire doit permettre de synchroniser et optimiser l'emploi des moyens

14. Voir Vauban paper n°1, « La donnée au coeur du combat collaboratif », contribution de Robert Ames, Lewis Shepherd & David Tennenhouse

de communications en fonction des différents scénarios opérationnels possibles. Avec un ensemble des données entièrement fonctionnel, l'utilisateur n'a pas besoin de se soucier de l'interface directe à ce niveau. À l'inverse, de concert avec le niveau des ressources, l'ensemble des données utilise l'apprentissage automatique (*machine learning*) et l'intelligence artificielle pour approfondir sa connaissance des ressources disponibles, ainsi que des exigences et des attentes de l'organisation.

Les données collectées circulent ainsi dans toute l'organisation, selon les besoins. En fait, le système bénéficie de la séparation des tâches en fonction des niveaux, et donc de l'intégration rapide des innovations et de l'industrialisation qui touchent chacun d'entre eux. Il devient ainsi capable de s'adapter dynamiquement bien au-delà des limites actuelles. Dans ces conditions, le système dans son ensemble dispose d'une compréhension instantanée de son fonctionnement qui va bien au-delà des capacités d'analyse humaines. Cependant, il faut souligner qu'il demeure toujours soumis à l'intention et à la volonté de l'être humain, telles qu'elles sont exprimées par le niveau de direction/contrôle. Les différents niveaux opèrent ainsi de façon coordonnée pour atteindre les objectifs et répondre aux exigences de l'attribution des tâches, de la collecte, du traitement, de l'exploitation et de la diffusion de l'information. Il est ainsi possible d'obtenir au niveau tactique les résultats souhaités, en s'adaptant aux perturbations ou anomalies et aux évolutions quotidiennes de l'environnement opérationnel.

La révolution numérique se poursuit à un rythme soutenu, portant avec elle l'impression persistante que les capacités, les performances et les exigences augmentent de manière exponentielle et sans limite visible. Dans ce tumulte, on ne s'est pas assez intéressé au concept de rupture portant sur la puissance des données par elles-mêmes. VMware Research pense que grâce à une organisation hiérarchisée comprenant des structures de conduite et de contrôle appropriées, une transformation numérique adaptée, portée par la mise en valeur de l'ensemble des données peut pleinement bénéficier à tous les niveaux de la chaîne opérationnelle, en particulier à celui du combattant.

AUTEURS

David Tennenhouse

Ancien Chief Research Officer, VMware

Robert Ames

Senior Director, Emerging Technology, VMware

Lewis Shepherd

Senior Director, Research & Emerging Technologies Strategy, VMware

VAUBAN SESSIONS

VAUBAN PAPERS

#3 LES DONNÉES AU SERVICE DU C2

avisa partners vmware

WWW.VAUBAN-SESSIONS.ORG

PRÉFACE

L'INTÉGRATION DES DONNÉES :

UN PUISSANT LEVIER DE TRANSFORMATION DU COMMANDEMENT ET DE LA CONDUITE DES OPÉRATIONS, UN DÉFI TECHNICO-OPÉRATIONNEL MAJEUR, UNE NOUVELLE APPROCHE DE LA SATISFACTION DU BESOIN OPÉRATIONNEL.

La question de l'intégration des données de nature très disparates, produites par de multiples capteurs humains ou techniques, n'est pas récente. Jusqu'à une période assez proche, la réponse classique a constitué à créer au sein des chaines de commandement et conduite des opérations (C2) de multiples organismes spécifiques chargés de trier, d'évaluer, d'interpréter, et de fusionner ces données opérationnelles pour alimenter les décideurs.

Ceux-ci ont dès lors été confrontés à un choix délicat : exploiter de manière systémique le potentiel de renseignement que recèlent les informations issues de ces masses de données en augmentation exponentielle ou, à partir de leur propre expérience et de leur appréciation de la situation, opérer un tri ciblé au risque de ne pas exploiter certains signaux faibles mais cruciaux. De ce choix dépend aussi l'issue de la bataille de l'information face à des adversaires toujours plus entreprenants et imprédictibles. Ce défi opérationnel majeur auquel sont confrontées tant les forces armées nationales que les organisations multinationales (OTAN, UE, coalitions....) appelle une réponse structurée, concertée, mais urgente, alliant les compétences opérationnelles à l'emploi des technologies numériques les plus avancées.

Soyons clairs, il ne s'agit pas de superposer les unes aux autres, l'objectif est bien de les intégrer. La faculté à réussir cette osmose constitue l'épine dorsale d'une véritable transformation numérique des armées modernes, à commencer par leurs structures et systèmes de C2. Depuis la fin de la guerre froide, les capacités de C2 des forces armées ont évolué pour répondre aux besoins d'engagements très dynamiques face à un large spectre de menaces dans les milieux classiques Terre, Air, Mer mais aussi de plus en plus dans l'espace exo-atmosphérique dans le cyberespace ou dans la sphère informationnelle.

Au niveau du commandement, l'intégration de ces différents domaines, l'évaluation des menaces qui en émanent et la mise en synergie des actions qu'ils permettent représentent un véritable défi.

Face à ces évolution majeures une approche classique du « Command Control » et les méthodes habituelles d'expression et de satisfaction du besoin opérationnel ne sont plus adaptées. En effet, il s'agit désormais de pouvoir centraliser une vaste quantité de données de natures diverses, de les organiser, d'en tirer l'essence pour conduire les opérations en temps réel. Il s'agit également de tirer le plein parti d'analyses en temps réfléchi pour améliorer la compréhension de situation, apprendre des erreurs commises, adapter rapidement la manœuvre, réorienter les efforts, identifier les centres de gravité de l'adversaire. Pour atteindre cette réactivité, cette agilité, cette efficacité, sans omettre un haut niveau de sécurité et de résilience, les nouveaux systèmes de C2 doivent s'adapter aux besoins évolutifs des commandants opérationnels (et non l'inverse). Leur sécurité et leur résilience doivent être intégrées dès leur conception.

Les nouvelles technologies du numérique peuvent répondre aujourd'hui à ce défi, à la condition expresse de développer ces nouveaux systèmes et les moteurs d'intelligence artificielle qui les alimentent, en pleine synergie entre utilisateurs et concepteurs.

C'est l'un des objets de cette troisième publication de la série « Vauban Papers » : promouvoir le travail d'équipes intégrées constituées d'opérationnels et d'industriels du numérique, animées par l'expression du besoin opérationnel et par l'expérimentation et le développement de solutions adaptées, agiles, fiables et ouvertes sur l'interopérabilité avec les systèmes de C2 existants et futurs.

Général (2S)
Jean-Paul Paloméros

Ancien Commandant suprême allié Transformation (SACT) de l'OTAN et Conseiller Sénior chez Avisa Partners

Les structures de Commandement et Contrôle (ou C2) sont au cœur de la planification et de la conduite des opérations militaires. Véritables centres névralgiques, leur efficacité repose sur l'échange continu d'informations entre les différents échelons de la chaîne de commandement. Depuis une vingtaine d'années, la numérisation fondée sur la collecte, l'infovalorisation et la dissémination d'informations offre de nouvelles perspectives pour le C2. La conjugaison de l'hyperconnectivité des forces et de la puissance de calcul et de traitement accrue des ordinateurs (notamment le *Cloud Computing*) permet d'accélérer et d'enrichir considérablement la planification et la conduite des opérations, la connaissance de la situation opérationnelle, ou encore la détection des menaces. L'emploi des technologies numériques libère également (en théorie) la charge cognitive du personnel et des décideurs afin qu'ils ne se concentrent que sur les activités essentielles.

Mais si la transformation numérique du poste de commandement (PC) ouvre un nouveau champ des possibles, elle s'accompagne aussi de défis techniques, opérationnels et humains.

La numérisation des structures de C2 : savoir plus vite et mieux

Pour fonctionner, les PC doivent disposer d'une vision à jour de la situation opérationnelle, bâtie à partir des informations remontées du terrain. À partir de ces éléments, le chef militaire peut ensuite planifier et conduire l'action, émettre les ordres vis-à-vis des différents niveaux hiérarchiques, et anticiper au mieux les actions possibles de l'adversaire.

La transformation numérique permet de décupler les capacités de planification et de conduite des PC. D'une part, la multiplication des capteurs embarqués et déployés sur le champ des opérations - combinée au développement de réseaux de transmission toujours plus performants (en débit comme en latence) - permet d'avoir une vision toujours plus fidèle de la réalité du terrain et de mener un combat réellement collaboratif. L'information en temps quasi réel permet effectivement au PC de mieux anticiper les menaces et mieux suivre l'évolution des opérations, permettant au chef de compter sur une plus grande réactivité des forces.

D'autre part, la puissance de calcul et de traitement des moyens informatiques d'aujourd'hui (qu'ils soient embarqués sur les plateformes et les capteurs, comme dans les PC) peut également être mise à profit pour calculer des scénarios en quasi temps réel et ainsi améliorer la capacité de prise de décision du chef par une présentation plus exhaustive des options possibles et de leurs conséquences. Le recours au calcul algorithmique permet en effet d'accélérer et de faciliter le tri des données collectées, mais également de réduire l'impact des biais cognitifs humains dans cette phase d'analyse et de projection.

Défis techniques du PC numérisé

Pour tirer parti des avantages offerts par la transformation numérique, les structures de C2 doivent également prendre en compte les enjeux inhérents au traitement des données. En résumé, il ne s'agit pas seulement d'avoir plus d'informations, au risque de paralyser la prise de décision[15], mais d'avoir de meilleures informations. En ce sens, la collecte et le traitement des données sont des étapes cruciales au sein du PC puisqu'elles peuvent influencer la prise de décision du chef. Les armées doivent dès lors disposer d'infrastructures et d'architectures informatiques performantes capables de transformer d'importants volumes de données en informations utilisables, et ce en un temps limité pour maintenir l'avantage opérationnel de l'information en temps quasi réel. Ces mêmes infrastructures doivent être dotées d'un haut niveau de cybersécurité pour les mettre à l'abri d'une action de l'ennemi.

Trois autres défis techniques doivent également être pris en compte :

- **La dépendance aux réseaux :** la non-disponibilité momentanée ou continue du réseau, qu'elle soit le résultat d'un dysfonctionnement ou de l'action de l'ennemi, empêche alors toute communication montante ou descendant avec les différents échelons.

- **L'interopérabilité des systèmes :** ce point est particulièrement crucial dans les opérations contemporaines qui se mènent très souvent dans le cadre de coalition où les alliés peuvent être équipés de systèmes très différents.

- **La souveraineté technologique :** les structures de C2 étant critiques dans la conduite des opérations, elles nécessitent une autosuffisance technique et logistique et l'établissement de relations de confiance avec les industriels qui les fournissent.

15. Le risque de l'infobésité est en effet d'attendre la prochaine information pour avoir une connaissance toujours plus parfaite de la situation et en fin de compte retarder toujours plus la décision.

Discrétion et survivabilité du PC

Un PC demeure une cible prioritaire, car sa neutralisation réduit de facto l'efficacité opérationnelle du dispositif déployé. Avec la numérisation, la multiplication des échanges de données engendre un accroissement des transmissions et donc de la signature électromagnétique des PC. L'enjeu pour les forces adverses devient alors de repérer la source de ces échanges afin de la neutraliser la plus rapidement possible.

Pour réduire les risques de détection, les PC modernes doivent par conséquent être conçus pour maximiser leur agilité, qu'elle soit physique (mobilité) ou technique (discrétion électromagnétique). Plusieurs options s'offrent ainsi aux décideurs :

- Devenir résilient : par exemple en enfouissant sous terre les PC pour les rendre plus résistants aux coups directs.
- Devenir mobile : il est possible d'accroître l'imprévisibilité en étant en mouvement continu, que ce soit sur terre et dans les airs.
- La discrétion peut également prendre la forme de leurres et d'opérations d'intoxication de l'ennemi (faux poste de commandement, génération de faux signaux électromagnétiques).

Les structures de C2 de demain

Alors que les missions des PC demeurent inchangées[16], leur exposition aux attaques devient plus grande dans le contexte géostratégique actuel : là où autrefois les obstacles à la conduite des opérations étaient naturels (distance, reliefs), l'ennemi est désormais capable de les créer artificiellement (ex : brouillage, prise de contrôle des systèmes d'information). Le retour des conflits de haute intensité accroît en effet le spectre des menaces pesant sur les structures de C2 : guerre aérienne, guerre électronique, missiles balistiques, missiles de croisière, etc.

En juin 2020, dans sa *« Vision stratégique 2030 »* pour l'Armée de Terre française, le Chef d'État Major de l'Armée de Terre, le Général Thierry Burkhard, désormais Chef d'état-major des Armées (juillet 2021), mettait en avant le fait que *« les conflits de demain mêleront actions de combat, guerre de l'information, actions cyber et rétorsion économique. Ces actions seront conduites de manière synchronisée, brutale ou insidieuse (…) un conflit de haute intensité entre États redevient donc possible dans tous les champs de la confrontation »*[17].

Ces nouveaux risques et menaces doivent donc être pris en compte dans la conception et la mise en œuvre des structures de C2, tout en poursuivant l'accroissement de leurs capacités. Le PC du futur devra ainsi prendre en compte les caractéristiques suivantes :

- **Modularité** : fractionnement géographique du PC (répartition dans plusieurs lieux) à différentes distances de la ligne de front.
- **Technologie** : optimisation de la gestion des données pour accroître la qualité des informations et des ordres transmis au chef & accroissement de l'interopérabilité (capacité à se connecter à différents systèmes).
- **Mobilité** : déploiement & démontage rapide du PC pour faciliter les opérations de relocalisation, ce qui exige un encombrement minimum pour un recours au moins possible de personnel, et un temps de mise en œuvre opérationnelle le plus court possible, ce qui nécessite d'employer les technologies adéquates.
- **Discrétion** : la réduction de la signature électromagnétique, de la consommation énergétique, et de l'empreinte thermique devient prioritaire pour réduire le risque d'être détecté et la vulnérabilité aux frappes qui en découle.
- **Résilience** : tenir compte du retour des menaces liées au combat de haute intensité (guerre électronique et cybernétique, combat de longue distance, frappe aérienne, coup de main…) en incluant plusieurs niveaux de protection physiques et cyber.

AUTEURS

Axel Dyèvre, *Associé, Avisa Partners*

Séverin Schnepp, *ancien Consultant, Avisa Partners*

16. (1) Traiter et synthétiser les informations issues de flux de données collectés sur le champ de bataille ; (2) Générer une vision globale et systématique de la situation opérationnelle ; (3) Distribuer et relayer les informations et les ordres entre les différents opérations de la chaîne de commandement.

17. « Supériorité opérationnelle 2030 : vision stratégique du chef d'état-major de l'armée de Terre », 08/07/2020, URL

DÉFIS ET OPPORTUNITÉS DES DONNÉES POUR LE C2

La transformation numérique des postes de commandement implique l'amélioration de la fonction de commandement et de contrôle (C2) grâce à l'adoption de systèmes flexibles et adaptables, à l'évolution de la doctrine et des technologies perturbatrices émergentes[18] telles que l'intelligence artificielle (IA), l'apprentissage machine (*machine learning*) et l'informatique quantique. Les progrès technologiques dans le domaine des systèmes d'information et de communication marquent en effet un tournant, d'autant que le secteur privé innove aujourd'hui à un rythme toujours plus rapide. C'est pourquoi les gouvernements et leurs forces armées s'efforcent d'adapter leurs politiques d'acquisition pour tirer profit de ces avancées technologiques.

La numérisation peut renforcer la capacité de l'OTAN à recueillir et traiter des informations, à prendre des décisions et à automatiser certains processus routiniers. Maintenir le rythme de la transformation numérique des structures de C2 est fondamental, car cela permet d'acquérir et de conserver un avantage technologique sur l'adversaire. Cette transformation présente tant des défis que des possibilités :

- Les réseaux, essentiels pour permettre la communication et la connaissance de la situation en temps réel, nécessiteront des algorithmes de réhabilitation de l'intelligence artificielle (IA) pour continuer à fonctionner efficacement contre la dégradation, les défaillances et les actions hostiles. Il est en effet nécessaire que les déploiements puissent bénéficier d'un important degré de résilience et d'adaptation. La létalité des armes conventionnelles et innovantes (i.e. cyber) implique d'une part de réduire la présence physique sur le terrain et d'autre part d'améliorer la redondance des systèmes C2, au moyen de systèmes modulaires et évolutifs répartis en plusieurs éléments et nœuds de commandement géographiquement dispersés.

- Le future champ de bataille d'opérations multi-domaines sera peuplé d'une myriade de capteurs et nécessitera une énorme bande passante pour permettre l'exploitation en temps voulu des informations collectées. Aujourd'hui, les logiciels de compression des données sont essentiels et l'IA est indispensable pour faire face à la surabondance d'information. Les méthodes de récupération de l'information (*information retrieval*) et de gestion du big data peuvent être utilisées pour traiter d'énormes quantités de données, facilitant ainsi un triage plus efficace à des fins d'évaluation. L'utilisation de ces techniques pourrait être bénéfique pour fournir les bonnes informations au niveau approprié.

- L'IA et le *machine learning* peuvent aider à exploiter la grande quantité de données qui inondent les systèmes C2 pendant qu'ils traitent les informations pour construire une image opérationnelle exhaustive. Ces méthodes peuvent améliorer la prise de décision et soutenir la fonction C2. Le *machine learning* peut ainsi permettre d'établir des modèles de données avec des instructions spécifiques pour l'exécution d'une tâche. Les risques fondamentaux des algorithmes de *machine learning* peuvent inclure l'amplification des biais humains, la révélation accidentelle d'informations privées ou secrètes, la fourniture de données fausses ou malveillantes. L'IA peut contribuer au processus d'évaluation des opérations en aidant l'état-major à analyser les tendances et à prévoir les possibilités et les évolutions des scénarios.

- Les progrès de l'informatique quantique pourraient permettre aux systèmes de C2 d'améliorer la résilience des PC grâce à des méthodes de cryptage des communications. Les ordinateurs quantiques utilisent les propriétés uniques des atomes et des photons pour résoudre des équations mathématiques complexes plus rapidement que les ordinateurs traditionnels. Cette « suprématie quantique » permettrait aux utilisateurs d'ordinateurs quantiques de transmettre et de traiter rapidement des données sécurisées entre les capteurs et les systèmes C2 par le biais de l'internet des objets militaires *(Internet of Military Things - IoMT)*, offrant un cryptage quasi impénétrable.

18. Technologies qui devraient atteindre un niveau de maturité dans les vingt prochaines années.

La numérisation est essentielle à la maitrise des technologies émergentes pour l'OTAN. Son adoption doit permettre à l'Alliance de conserver les compétences de base nécessaires à la défense collective, à la sécurité coopérative et à la gestion des crises, tout en améliorant sa capacité à anticiper les menaces non-militaires et à tirer profit de la coopération avec les parties prenantes. La numérisation nécessite le développement d'une industrie des données reposant sur des canaux de données robustes, des centres de développement d'algorithmes et une main d'oeuvre associée, et de structures de stockage qui fonctionnent de façon harmonisée pour toute l'Alliance. Le stockage, le partage et le traitement d'énormes quantités de données en temps réel nécessitent dès lors une approche à l'échelle d'une entreprise qui se connecterait à internet via des réseaux 5G de confiance. D'un point de vue technologique, l'objectif opérationnel consisterait à associer un internet des objets militaires (IoMT) à une structure de C2 reposant sur l'IA afin de soutenir les commandeurs. Les principaux défis à la mise en œuvre de ce système seraient alors la disponibilité des données, l'interopérabilité des systèmes fournis par les plateformes multi-capteurs publiques et militaires, et la complexité des algorithmes cryptographiques à utiliser.

AUTEUR

Général de Corps d'Armée

Guglielmo Luigi Miglietta

Commandant du Corps de Déploiement Rapide - Italie (NRDC-ITA)

LES DONNÉES AU SERVICE DU C2

Dans les deux publications précédentes[19], nous avons présenté le *Military Digital Control Plane* ou MDCP (plan de contrôle numérique à des fins militaire) ainsi que les liens entre les différents domaines de son architecture. Nous nous sommes notamment concentrés sur les niveaux de données (*Data Tiers*), concept central à cette architecture capable, grâce à un couplage et une orchestration intelligente des données, de séparer entre les différents niveaux les préoccupations de l'organisation et in fine de traduire en actions opérationnelles les objectifs stratégiques. L'accent sera ici mis sur les caractéristiques et les considérations opérationnelles du MDCP.

Souvenez-vous de notre analogie pour expliquer le niveau des données : les données circulent au sein de l'organisation comme le sang circule dans notre corps. Si le niveau des données est le sang du système, alors le niveau de direction et contrôle (*Command Tier*) et le MDCP sont les équivalents du cerveau et du système nerveux. Ensemble, ces deux niveaux reflètent les besoins, intentions, politiques et règles de l'organisation tout en tenant compte des niveaux des données et le niveau des ressources (*Resource Tiers*).

Le rôle du niveau de direction et contrôle (*Command Tier*) est de servir d'interface entre les utilisateurs et consommateurs humains du système. Pendant des décennies, il y a eu un un écart important entre le domaine informatique et les styles et modes de communication des êtres humains utilisant ces systèmes. Pour que l'intention de l'organisation soit reflétée dans le système, une expertise approfondie était nécessaire pour retranscrire ces besoins en configurations de système et de sécurité, en applications et en en politiques informatiques. En réalité, ces retranscriptions manquaient souvent leur cible, comme en témoignent les nombreux échecs. Avec l'avènement de l'architectures de grandes échelles et de Kubernetes, de nouvelles configuration déclaratives des systèmes ont vu le jour.

Ainsi, le développeur d'applications ne prescrit plus un nombre spécifique de systèmes, de régions de disponibilité ou d'autres détails. Il indique plutôt au système les caractéristiques dont son application a besoin, telles que la disponibilité, l'échelle, l'équilibrage des charges et les pare-feu, alors que le système, qui a désormais une meilleure compréhension de ses réalités physiques, fournit les ressources de manière appropriée. Au fur et à mesure que les besoins évoluent, le système s'adapte en conséquence, en augmentant ou en diminuant l'échelle, ce qui était auparavant difficile. Ce concept se reflète également dans une certaine mesure dans les réseaux définis par logiciel (*Software Defined Networking*) et les réseaux étendus définis par logiciel (*Software Defined WANs*), qui permettent à l'organisation de configurer, connecter et de sécuriser selon la fonction, plutôt que de se fier à des règles fragiles de source, de destination et de port IP qui ont autrefois déconcertaient les architectes de réseau et étaient souvent terriblement en retard sur la réalité déployée.

Si nous étendons le concept d'interface et de gestion de systèmes déclaratifs, nous pouvons alors prévoir que le niveau de direction et de contrôle (*Command Tier*) permettra à l'organisation et à ses décideurs de définir clairement ses priorités, de rationaliser ses ressources et de maximiser leur utilisation pour la conduite de la mission. Les informations et renseignements nécessaires à une prise de décision efficace transiteront par l'organisation et ses applications pour informer et éclairer les décideurs. En outre, le niveau de direction et de contrôle fournira des interfaces et intuitives pour déclarer, appliquer et évaluer les politiques, qu'il s'agisse de sécurité, de partage d'informations ou même de l'utilisation licite et prévisible de l'intelligence artificielle et/ou des systèmes d'armes. Grâce à un niveau de données robuste et correctement automatisé, il est également possible d'appliquer avec soin les flux de données dans l'ensemble de l'organisation. Ces données peuvent être bien comprises, conformes aux normes internationales en vigueur, refléter avec précision et appliquer les régimes de confidentialité actuels.

19. Voir Vauban Paper #1 « La donnée au coeur du combat collaboratif » et Vauban Paper #2 « Les données au service du combattant : enjeux et opportunités ».

Pour revenir à notre analogie, l'équivalent de notre système nerveux central est le MDCP dans cette architecture. En effet, il parcourt logiquement tous les niveaux de l'organisation, de la même manière que notre moelle épinière part du tronc cérébral et descend vers nos organes vitaux pour se connecter par les nerfs à nos extrémités. Dans le domaine numérique, le MDCP exécute les ordres dans l'ensemble de l'architecture, créant des flux, connectant de nouvelles régions, réparant les défaillances et supprimant celles qui sont obsolètes. À l'instar de notre système immunitaire, il réagira de manière autonome (selon les règles de l'organisation) pour faire face aux attaques virales ou autres anomalies. Grâce à sa connexion à l'ensemble du système, le MDCP dispose de la capacité d'agir, de réagir et d'informer le niveau de direction et de contrôle (*Command Tier*) pour obtenir des informations et des orientations supplémentaires.

VMware Research voit un potentiel considérable dans l'utilisation du concept de MDCP. La conception de systèmes s'inspire souvent de la biologie, car notre corps est un véritable système de systèmes reposant sur des fonctions de commandement, de contrôle, de messagerie et de réponse. Avec la séparation des préoccupations proposée par le MDCP, il devient possible de se concentrer et d'innover dans ce domaine, tout en assurant la connexion, l'interopérabilité et la pertinence grâce à une utilisation efficace des normes. La beauté de la virtualisation et de l'abstraction, qui sont au cœur de l'existence de VMware, réside dans le dépassement des limites matérielles, laissant place à la puissance de la mise en commun des ressources, de la mise à l'échelle et d'une configuration et gestion beaucoup plus efficaces des systèmes complexes. À l'avenir, une organisation prospère exploitera des concepts tels que ceux décrits ici pour fonctionner dans les boucles OODA de ses concurrents grâce à une gestion opérationnelle omniprésente et efficace soutenue une innovation comme le MDCP.

AUTEURS

Robert Ames

Senior Director, Emerging Technology, VMware

Lewis Shepherd

Senior Director, Research & Emerging Technologies Strategy, VMware

VAUBAN SESSIONS

VAUBAN PAPERS

#4 C2 AUGMENTÉ : CONJUGUER ART DU COMMANDEMENT ET NOUVELLES TECHNOLOGIES

avisa partners vmware

WWW.VAUBAN-SESSIONS.ORG

PRÉFACE

TRANSFORMATION NUMÉRIQUE OPÉRATIONNELLE, LA MARCHE EN AVANT.

La Transformation numérique des forces Armées constitue à la fois un objectif de progrès dans la conception, la conduite et l'exécution des opérations militaires mais aussi un puissant levier pour adapter la préparation des forces armées aux nouveaux défis géostratégiques, aux risques et menaces qui en découlent. Les trois premières publications de la série « Vauban Papers » ont permis d'établir l'état des lieux de cette transformation, son impact sur l'exécution des opérations au niveau des combattants et en dernier lieu les grands enjeux qu'elle comporte pour l'exercice du commandement.

De ces réflexions étayées par les séminaires « Vauban », organisés sous l'égide du Corps de Réaction Rapide Français (CRRFR), il ressort clairement que la réussite de la transformation numérique opérationnelle repose sur une combinaison dynamique de facteurs humains, technologiques et industriels. Pour produire ses effets, cette interaction, doit être soutenue par une réflexion approfondie portant sur des évolutions conceptuelles (Combat multi domaines, rôle des postes de commandements, répartition des responsabilités des niveaux opératifs et tactiques, développement de « combat *Clouds* »...) et sur les apports et les limites de l'automatisation des fonctions opérationnelles permise par le développement de l'Intelligence Artificielle (IA).

Une première conclusion découle de cette analyse, l'opérationnalisation de la transformation numérique appelle un effort innovant, collectif, collaboratif qui doit permettre de s'affranchir de méthodes classiques inadaptées et de développements capacitaires séquentiels longs et fastidieux. Il s'agit ici tout au contraire de créer une dynamique incrémentale qui place l'utilisateur final au cœur du dispositif.

Cette nouvelle approche doit viser à tirer le meilleur parti des technologies numériques les plus avancées, issues du marché, en les intégrant dès la conception des nouveaux systèmes dans une logique de démonstration/développement. Dans cette perspective, l'utilisateur opérationnel soutenu par les experts industriels doit pouvoir éprouver les nouveaux concepts, imaginer des solutions innovantes, et, in fine, retrouver la maîtrise des systèmes qu'il met en œuvre et de leur évolution. Soyons clairs, il ne s'agit pas pour les armées d'assurer l'ensemble du cycle de conception, développement, exploitation, maintien en condition opérationnelle (dont mise à niveau) des systèmes d'informations qui intègrent les technologies numériques les plus avancées. Ce n'est pas là leur métier, d'ailleurs même l'armée américaine ou encore l'armée britannique l'ont reconnu en décidant de co-innover et coopérer avec l'industrie pour assurer le succès de leur transformation numérique. Il s'agit bien de déterminer les compétences qui sont indispensables aux forces armées pour comprendre, spécifier le besoin opérationnel, superviser, faire évoluer, assurer la sécurité de leurs systèmes d'information. Le maintien de l'interopérabilité de ces systèmes que ce soit entre les différentes armées d'un même pays, entre Alliés de l'OTAN, ou encore entre membres d'une même coalition internationale représente un autre défi qu'il faut relever dès la conception des nouveaux systèmes. Les nouvelles technologies de l'information telles que la virtualisation permettent désormais d'envisager cette interopérabilité d'une manière beaucoup plus dynamique que par le passé en créant par exemple différents espaces de confidentialité concentriques en fonction de la classification voulue par les décideurs (nationale, OTAN, coalition...). La capacité de collaboration entre les différents acteurs de la transformation numérique au service du besoin opérationnel est bien la clé de son succès. Cette édition l'illustre parfaitement au travers d'une réflexion de fond sur les conditions d'intégration de l'intelligence artificielle dans un processus d'aide au commandement.

Général (2S)
Jean-Paul Paloméros

Ancien Commandant suprême allié Transformation (SACT) de l'OTAN et Conseiller Sénior chez Avisa Partners

C2 AUGMENTÉ : CONJUGUER ART DU COMMANDEMENT ET NOUVELLES TECHNOLOGIES

Les publications précédentes de cette série ont mis en évidence les opportunités et défis techniques, opérationnels, humains engendrés par la numérisation des Armées. Ce nouvel opus entend poursuivre la réflexion menée jusqu'alors en se focalisant sur une question stratégique : comment conjuguer de façon durable et pertinente l'art très humain du commandement avec l'emploi des nouvelles technologies ?

L'augmentation continue de la puissance de calcul des ordinateurs, leur miniaturisation, l'amélioration des performances logicielles et la multiplication des capteurs sont autant d'éléments qui, conjugués à la réduction de la latence et la vitesse croissante des réseaux de flux d'informations, participent à l'explosion de la quantité de données collectées sur le terrain, à l'accélération de leur transmission et à la facilitation de leur traitement au sein des structures de C2. Cette conjugaison de facteurs contribue à améliorer la coordination en temps réel des forces sur le terrain.

L'emploi de technologies de valorisation et de traitement des données permet d'envisager la conduite d'un combat interactif et collaboratif par différents acteurs et via de multiples plateformes qui agissent au sein d'un environnement opérationnel devenu multidimensionnel. Face aux menaces asymétriques et au retour des conflits de haute intensité, cette maîtrise de l'information est un prérequis pour assurer réactivité et supériorité opérationnelle.

La dimension « quasi-temps réel » : un nouveau paradigme temporel pour le C2

La transformation numérique permet l'accélération et l'automatisation de certaines tâches. S'appuyant sur la remontée d'informations du terrain déjà traitées, la visualisation de la situation ami-ennemi et le calcul de scénarios d'évolution possibles, le chef militaire peut compter sur une vision en quasi-temps réel de la situation opérationnelle, mais aussi sur des éléments de réflexion et de projection.

Pour comprendre l'impact de la transformation numérique sur les structures de C2, un parallèle peut être fait avec l'évolution du GPS y compris dans son emploi grand public. L'idée n'est pas là de comparer ce qui n'est pas comparable, mais de retracer ce qu'a été la « transformation digitale » des fonctions « cartographie » et « navigation » dans le domaine grand public, pour illustrer la progressivité des étapes de cette évolution. Même si l'on a tendance à l'oublier, le GPS grand public — comme beaucoup d'appareils et services numériques — a suivi des évolutions qui ont amené des changements de matériels et d'usages complets sur près de 30 ans ponctués par 4 générations différentes de types de terminaux :

- **Début des années 90 :** première génération de terminaux avec écrans LCD permettant la réception de coordonnées et de reporter la position sur une carte papier.
- **Fin 90 — début 2000 :** apparition d'appareils intégrant une cartographie numérique sur laquelle étaient reportées les coordonnées sur un terminal numérique cartographique « statique ».
- **Courant des années 2000 :** capacité embarquée des GPS pour calculer des itinéraires sur des terminaux de guidage, mais avec des données « froides ou figées » (ex. : routes, types de transport utilisés). Le GPS est alors capable de calculer un itinéraire et de fournir des informations supplémentaires (ex. : distance, temps du trajet).
- **Années 2015 :** Avec notamment l'explosion du smartphone, des réseaux mobiles et les nouvelles versions des signaux des différents systèmes de positionnement

Désormais, les terminaux GPS peuvent, en plus des données froides qu'ils utilisaient déjà, recevoir en temps réel des données chaudes, évolutives (trafic, embouteillages, travaux, météo, accidents, déviation). Alimentés en temps réel, ils peuvent en permanence recalculer leurs itinéraires et proposer au conducteur un nouvel itinéraire optimisé ou plus adapté à des besoins spécifiques (trouver du carburant, faire des courses, trouver un restaurant).

Toutes choses égales par ailleurs, depuis le début des années 90 et les balbutiements de l'informatique embarquée, les systèmes de C2 ont suivi une évolution comparable à cet exemple. Et là où, il y a quelques années, l'informatisation consistait en l'utilisation en parallèle de moyens classiques (cartes papier, chaîne de cadres de transmission des ordres) et d'ordinateurs, aujourd'hui, les postes de commandement reçoivent et analysent simultanément des données froides (infrastructures principales, caractéristiques géographiques, prévisions météorologiques) et des données chaudes (météorologie temps réel, position ami-ennemi, postes de commandement, infrastructures déplaçables, chaînes logistiques, regroupements des forces, points de passage) tant dans la phase de planification que dans celle de conduite des opérations. Les moyens de communication et de transmission des ordres comme les outils d'analyse et de visualisation sont numérisés. Et la puissance embarquée des capteurs et des plateformes permet de remonter de l'information ayant de plus en plus de valeur ajoutée et requérant donc des moyens d'exploitation de plus en plus puissants pour en tirer la quintessence.

Placer l'utilisateur final au cœur de la transformation

En partant du postulat que ces mêmes données sont correctement sécurisées et stockées afin de prévenir toute « infoxication », il est aisé d'imaginer dans les prochaines années que les technologies employées seront de plus en plus capables de suggérer au chef militaire des propositions d'action (ou un arbre de choix) fondées sur l'analyse de scénarios plausibles ou réels (ex. : RETEX). Mais alors que l'expression « intelligence artificielle » est porteuse de beaucoup d'approximations et de fantasmes, il faut rappeler que les ordinateurs, même les plus puissants, ne sauraient se substituer à l'art du commandement, reposant sur la formation, l'entraînement et l'expérience individuelle. Comme il en est avec tout outil, ces nouvelles possibilités bien utilisées peuvent augmenter la vitesse et la pertinence des décisions prises, de la même manière qu'elles peuvent se révéler de redoutables pièges cognitifs. Sans parler du fait que pour des raisons naturelles (relief.....) ou consécutives à des attaques (guerre électronique, cyber...), les flux de données peuvent être interrompus ou corrompus. Pour filer la métaphore du GPS, de même que la lecture de la carte « papier », et l'usage de la boussole ou du sextant resteront des connaissances indispensables sur le terrain, les C2 numérisés — et les unités déployées — devront pouvoir fonctionner en mode dégradé. Et comme pour un GPS, où l'intuition et la connaissance sensorielle de l'utilisateur peut l'amener à prendre une décision contraire à la recommandation, aucun système de C2 numérisé, si puissant soit-il, ne remplacera l'intelligence et la capacité d'arbitrage dans l'incertitude du chef.

L'art du commandement

En opération, le commandement s'exerce dans un environnement évolutif, flou, pressant, en résumé « incertain ». Le chef ne peut espérer appuyer sa décision sur une « connaissance parfaite » de la situation. Il doit au contraire faire face à un adversaire qui cherche à dissimuler ses intentions et à adapter en conduite ses plans et l'utilisation de ses moyens. Il est également confronté à des paramètres naturels comme la météo, ou humains tel le comportement des populations. Il doit donc décider dans l'incertitude en tâchant de dissiper « le brouillard de la guerre ». Ainsi, le chef doit arbitrer entre les différentes hypothèses et scénarios et prendre ses décisions en se fondant sur les informations à sa disposition (données chaudes et froides, intentions de l'ennemi) et sur son expérience et son intelligence. C'est dans ce cadre que doivent être conçus les différents systèmes d'aide au commandement.

Intelligence humaine et augmentée

L'emploi de technologies numériques vise à faciliter le cycle de collecte, de traitement et d'exploitation des données. Elles sont potentiellement de précieux outils d'aide au commandement. Ainsi, l'intelligence « artificielle » (ou augmentée) générée par les algorithmes peut permettre — si elle est correctement paramétrée et que la situation permet de l'alimenter en données fiables — de réduire l'incertitude et d'améliorer la connaissance de la situation opérationnelle. Pour autant, elle ne saurait décider à la place de son utilisateur. Pour mieux appréhender le commandement à l'ère numérique, il faut en réalité distinguer ici deux types :

- **L'intelligence humaine :** elle désigne l'aptitude d'un individu à comprendre, réfléchir, connaître, adapter son comportement à une situation, et choisir des moyens d'action en fonction des circonstances. Cette intelligence se matérialise par des capacités cognitives permettant à l'individu de créer des cheminements complexes et d'inclure à tout moment de nouvelles variables susceptibles d'orienter la prise de décision.

- **L'intelligence artificielle ou augmentée :** elle se matérialise par une rapidité d'exécution de certaines tâches (tri, calcul, identification, détection) et repose sur un programme défini. À aucun moment, une intelligence digitale ne prend de « décision » au sens cognitif du terme. Elle applique des règles dont la complexité et la rapidité peuvent donner l'illusion d'un raisonnement, mais qui restent un enchaînement logique.

En pratique, ces deux formes d'intelligence ne sont pas concurrentes, mais bien complémentaires : lorsque les données pertinentes sont disponibles, l'ordinateur sera plus rapide que l'humain pour exécuter une tâche de calcul. Si ces données sont indisponibles ou inexploitables, seul l'humain peut décider en évaluant une situation incertaine et arbitrant entre plusieurs hypothèses bâties sur des données incomplètes ou à la fiabilité incertaine.

Le commandement à l'ère numérique

Les technologies dites d'« Intelligence artificielle » ne peuvent en aucun cas se substituer à la capacité de décider d'un chef militaire :

- Leur connaissance de l'environnement et leur fonctionnement sont limités par la quantité et la qualité des données reçues. Ainsi, une variation de flux peut fausser le résultat final, tandis que des données de qualité médiocre altéreront le niveau de granularité et la pertinence de l'analyse. Le commandement repose sur la capacité à prendre des risques sur la base d'éléments incomplets ou contradictoires : par conception, un ordinateur ne peut en aucun cas répondre seul à ce besoin. Enfin, comme analysé dans les Vauban Papers précédents, les technologies numériques amènent de nombreuses contraintes matérielles, comme la consommation électrique, la dissipation de chaleur et la capacité de stockage. Ces limites sont sans cesse repoussées, mais sans atteindre le fonctionnement optimal du cerveau humain pour ce qui touche à la prise de décision. Ce qui a amené un chercheur majeur du domaine, Luc Julia — créateur de Siri puis VP R&D de Samsung — à déclarer « Les méthodes de ces intelligences demandent une énergie folle. C'est une aberration. Sachant qu'avec nos 20 watts, nous pouvons parler, manger, faire plein d'autres choses. La machine, elle, ne fait que jouer au jeu de Go. On voit donc que cette intelligence « artificielle » n'a rien à voir avec l'intelligence humaine ».

- Les technologies d'IA sont incapables de tenir compte de variables exogènes à leur code, ne disposent pas des 5 sens, ce qui amoindrit leur capacité à retranscrire de manière fidèle une situation complexe. Un humain peut être non linéaire dans son raisonnement, dans la mesure où l'enchaînement de sa réflexion se fait par des connexions biochimiques infiniment plus complexes que du traitement massif de données. Cela lui donne une capacité d'adaptation aux changements de situations, mais aussi une résilience face à l'adversité et aux injonctions contradictoires. Aucun ordinateur ne serait capable de dire comme le Général Foch dans son message au Grand Quartier Général, lors de la première bataille de la Marne, 6 au 9 septembre 1914 : *« Mon centre cède, ma droite recule, situation excellente, j'attaque. »*

- En outre, contrairement aux humains, les ordinateurs ne sont pas dotés de capacités d'extrapolation ou de corrélation. Ils n'ont pas de prédispositions (connaissances) générales leur permettant de générer des cheminements complexes, c'est-à-dire mettre bout à bout plusieurs actions.

On le voit, le commandement demeure donc une spécificité et une prérogative humaine, c'est-à-dire un art dans lequel le chef militaire doit conserver son autonomie d'évaluation et de décision. C'est d'autant plus vrai que la conduite de la guerre demeure un acte humain complexe qu'aucun ordinateur ne saurait appréhender dans sa globalité à travers des chiffres et des algorithmes.

Pour reprendre l'analogie du GPS, un conducteur peut décider de ne pas prendre en compte l'information de son GPS, soit parce que dans son environnement l'information remontée n'est pas totalement exacte, soit parce que sa courbe d'expérience lui fait penser différemment.

Les technologies n'ont donc pas vocation à arbitrer : elles se contentent d'exécuter le programme prévu et elles ne sont ni plus ni moins qu'une aide à la décision.

Un défi : conjuguer l'art du commandement et les nouvelles technologies

L'IA, utilisée au sein des C2, peut indéniablement constituer un atout au service de l'efficacité et de la supériorité opérationnelle des forces armées.

Tout d'abord, la numérisation continue permet de simplifier l'architecture des systèmes utilisés dans les différentes phases du C2 (anticipation, planification, conduite, analyse des effets ex post) : les données « temps réel » peuvent devenir des éléments précieux pour alimenter le retour d'expérience (RETEX) et alimenter le cycle de planification. De même les éléments de calcul préalables de préparation de planification peuvent devenir des éléments concourant à la conduite en temps réel des opérations s'ils sont enrichis par des données pertinentes et fiables.

Pour être pleinement exploitées, ces technologies doivent être développées et intégrées dans la perspective des besoins opérationnels, elles doivent également faire l'objet d'un processus d'appropriation et d'acceptation par les utilisateurs. Trop souvent encore, ces évolutions sont présentées comme concurrentes ou même comme des substituts de l'intelligence et de la capacité de décision humaine, alors qu'elles ne sont en réalité qu'un outil qui permet d'augmenter celles-ci. C'est en devenant « intelligence augmentée », c'est à dire « intelligence de l'Homme augmentée par la machine » que les technologies dites d'intelligence artificielle deviendront de réels systèmes d'aide à la décision. Cela résoudra également les débats éthiques et moraux souvent associés à ces questions en ramenant la machine à sa juste place de système automatisé, certes très évolué, et qui laissera toujours l'intention et la décision à son utilisateur humain.

AUTEURS

Axel Dyèvre, *Associé, Avisa Partners*

Séverin Schnepp, *ancien Consultant, Avisa Partners*

Marie Ketterlin, *Analyste, Avisa Partners*

LA COMPLEXITÉ DU C2 DANS LES OPÉRATIONS MULTI-DOMAINES

L'accélération du rythme de partage d'information et de la prise de décision est un défi permanent pour l'OTAN. Ce constat, exprimé dans les publications de l'organisation, a été confirmé lors du webinaire annuel 2020 du C2COE, au cours duquel la complexité du commandement et contrôle des opérations multi-domaines a été soulignée.

Maîtriser la complexité du partage des informations dans le cadre du processus décisionnel doit figurer à l'ordre du jour du développement des capacités de combat de l'OTAN pour les années à venir.

Le message que nous avons passé durant l'édition 2022 des Vauban Sessions a été façonné par les résultats d'études, les observations et les événements de ces dernières années. Marcel Scherrenburg, notre expert principal en la matière, a présenté nos réflexions sur l'accélération du partage d'informations dans le processus de prise de décision militaire.

Nous avons pu constater que l'une des plus grandes sources de confusion dans le développement du concept « C2 multi-domaine » est la gestion de l'information. La technologie permet d'accéder à l'information et aux moyens de visualisation des données, et elle permettra de communiquer aux moments décisifs, en tout lieu et à tout moment. Néanmoins, les réussites sont rares en termes de lancements réussis de nouvelles technologies au sein de l'OTAN restent rares, indiquant un décalage entre les besoins et les solutions proposées.

Nous avons lors des Vauban Sessions évoqué les questions suivantes : comment les commandeurs et personnels militaires font-ils face à l'accélération du partage d'information ? En quoi le partage d'information est-il essentiel au processus de prise de décision ? Quels sont les besoins au niveau opérationnel pour atteindre la supériorité cognitive dans la prise de décision ? Et la question la plus complexe : comment l'OTAN peut-elle réaliser cela ?

Les observations faites lors d'exercices de l'OTAN montrent que la gestion de l'information dans les quartiers généraux de niveau opérationnel reste un défi récurrent. Les quartiers généraux n'étaient pas entièrement prêts à absorber, filtrer et distribuer le flux massif de données provenant de l'environnement opérationnel. Dans certains cas, cette incapacité à traiter toutes les données a entraîné l'exclusion indésirable d'informations, donnant lieu à une compréhension inexacte de la situation et laissant inutilisées des données essentielles. Cela a par la suite conduit à des décisions imparfaites.

Dans le processus de prise de décision du commandeur, des événements liés dans des domaines multiples, de grandes quantités de données et un manque de relations claires de cause à effet ont rendu nécessaire la reconsidération de la gestion de l'information pour atteindre la supériorité cognitive. Dans un environnement futur incertain, ambigu et complexe, les compétences et connaissances existantes ne suffiront pas pour prendre des décisions fondées.

Pour atteindre la supériorité cognitive ou une compréhension complète de l'environnement opérationnel, il ne suffit pas de disposer de plus de capteurs ou de plus de données. Les véritables avantages cognitifs apparaissent au cours de l'étape de « création de sens » (*sense-making stage*). À ce stade, les données sont projetées dans un contexte et un cadre de mission spécifiques. Pour atteindre cette supériorité cognitive, l'OTAN a besoin de plusieurs types de plateformes de partage d'information, alimentées par des sources multiples, et capables de mettre en œuvre et d'intégrer plusieurs outils de connaissance de la situation et de prise de décision.

À l'avenir, au lieu d'employer davantage de ressources humaines et d'essayer d'accélérer le cycle C2, les commandeurs s'appuieront sur des outils d'aide à la décision basés sur l'intelligence artificielle et d'autres technologies émergentes.

Ces outils sont déjà largement disponibles dans le secteur commercial. Ils fournissent des analyses automatisées, prédictives et prescriptives par l'intégration en temps réel d'ensembles de données en continu. Ces technologies émergentes pourraient remplacer les tâches fastidieuses des officiers d'état-major et contribuer à une meilleure compréhension de la situation, voire à une supériorité cognitive. En conséquence, la compréhension de la situation serait plus complète, permettant une meilleure évaluation des options possibles.

Il est nécessaire de mettre au point un système comprenant « l'information à la demande » ou, à l'avenir, « la compréhension de la situation à la demande », pour soutenir la compréhension de l'environnement opérationnel. Les opérations militaires devant être robustes par principe, il est difficile d'apporter des changements trop importants dans le quotidien. Cela ne devrait pas empêcher l'introduction d'une technologie innovante, mais il s'agit simplement de rappeler que le changement sera au départ mineur et que l'innovation proposée doit s'inscrire dans l'état d'esprit actuel.

L'introduction d'un nouveau concept ne doit pas constituer une rupture vis-à-vis du quotidien existant mais abaisser les barrières d'acceptation en prouvant qu'il est robuste et digne de confiance. La quantité de données, qu'elles proviennent de l'allié ou de l'adversaire, la vitesse des communications, la complexité de l'environnement opérationnel et la diversité des acteurs sont autant d'éléments qui ont augmenté de façon exponentielle. Compte tenu de la complexité des opérations militaires, le commandant interarmées doit être capable de se concentrer sur l'atteinte des objectifs opérationnels et non sur les informations qui pourraient l'en détourner.

L'OTAN doit adopter la technologie, apprendre et s'adapter rapidement pour exploiter pleinement le potentiel des dernières innovations.

L'Alliance doit s'efforcer de parvenir à une compréhension commune et à une familiarité avec les technologies intuitives, à l'instar de la façon dont nous utilisons, par exemple, nos smartphones. Il faut donc un changement de paradigme au sein de l'OTAN et de ses États membres, pour combler le fossé entre les développeurs et l'utilisateur final au siège de l'OTAN, la frontière entre la répétition d'une promesse permanente et l'introduction réussie d'une technologie restant mince.

Nous pourrons alors nous concentrer sur l'essentiel : utiliser le C2 agile pour un processus de décision efficace, synchronisé et bien informé. Il faut aussi tenir compte du facteur humain : la confiance entre les gens, la compréhension des différences culturelles et le travail d'équipe. Après tout, nous sommes une même équipe, nous sommes l'OTAN.

Pour adopter la gestion de l'information en tant qu'outil d'aide à la prise de décision militaire, l'OTAN doit faire évoluer ses technologies, ses procédures et ses capacités. Une question reste cependant en suspens : qui dirige cette évolution ?

Nous n'avons pas saisi la question de de la gestion de l'information au sein de l'OTAN dans son intégralité, puisqu'il s'agit d'un problème complexe qui nécessite un effort collectif dépassant les seules capacités militaires. Les enjeux de ce type nécessitent plus qu'une solution unique, mais une approche globale pour développer de multiples lignes d'effort afin de réduire la complexité sans simplifier à l'excès la phase de « création de sens ».

AUTEUR

Colonel

Mietta Groeneveld

Directrice du Centre d'Excellence C2 de l'OTAN

TIRER PARTI DES TECHNOLOGIES CIVILES POUR LA TRANSFORMATION NUMÉRIQUE DES FORCES ARMÉES

J'ai eu le privilège de participer à l'édition 2022 des Vauban Sessions et d'échanger avec des représentants militaires sur la manière dont les forces armées peuvent tirer profit des technologies civiles pour leur transformation numérique opérationnelle. Je n'ai pas été surpris de constater que bon nombre des conversations, des défis et des innovations qui ont lieu au sein de l'armée - et à tous les niveaux - sont très similaires à ce qui émane du secteur technologique civil. En effet, nous avons beaucoup à apprendre les uns des autres.

Exploiter et tirer profit des volumes massifs de données

À son niveau le plus fondamental, le nœud du problème est de disposer des bonnes données, entre les mains des bonnes personnes et au bon moment. C'est une chose à laquelle les consommateurs se sont habitués avec les applications qui donnent accès à tout, de la biométrie aux services bancaires. Mais les forces armées ne peuvent pas compter sur un magasin où les soldats et les divisions peuvent choisir les applications qui leur conviennent. Elles ont besoin de cohérence, d'uniformité et de l'adoption de technologies fondées sur un système de commandement et de contrôle (C2) de premier ordre. Par conséquent, les chefs militaires doivent se concentrer sur la capacité à exploiter les techniques avancées d'intelligence artificielle et d'apprentissage automatique disponibles aujourd'hui, pour comprendre les données, savoir qui en a besoin, quand, et quelles décisions ces informations vont faciliter.

Comme l'ont présenté Robert Ames et Lewis Shepherd, Senior Directors, National IT strategy chez VMware dans les précédents Vauban Papers, le développement de notre plan de contrôle numérique militaire (MDCP) vise à résoudre ce problème. Il s'agit d'une construction architecturale moderne destinée à informer et à responsabiliser les décideurs. Capable d'exploiter et de capitaliser sur les énormes volumes de données qui circulent dans les organisations militaires, c'est aussi la base sur laquelle les développements les plus récents et les plus pointus de la technologie civile peuvent être incorporés pour offrir d'énormes avantages aux forces armées du monde entier.

La technologie grand public au service d'une guerre efficace

Un trait qui incarne les organisations militaires - et qui l'a fait tout au long de l'histoire - est la résilience. Les équipes doivent être capables de s'adapter à des situations changeantes. Cela signifie que les forces armées ont besoin d'une livraison rapide et fiable sur des systèmes rapides et fiables, capables de s'adapter à l'inattendu ou aux attaques des adversaires. Par conséquent, cela remet en question les normes précédemment acceptées. Il y a quelques années seulement, les dirigeants des organisations voulaient que tout passe par le *Cloud*, mais ce n'est pas dans ce sens que le monde a évolué. Au lieu de se trouver en un seul endroit, la nature hautement distribuée de l'informatique met les données entre les mains des utilisateurs, où qu'ils se trouvent. Des taxis aux cockpits, des trains aux chars, les données résident dans toutes sortes d'endroits, au niveau des appareils. Les centres C2 doivent être en mesure de les saisir en temps réel afin de conserver une longueur d'avance.

Les réseaux et les dispositifs doivent également être déployés de manière sécurisée. Dans le secteur des technologies, on parle de plus en plus des problèmes de confiance et de confidentialité. Il ne s'agit pas seulement de la souveraineté des données ou du respect d'une frontière particulière, mais aussi de la souveraineté des plateformes elles-mêmes et de l'assurance que nous ne sommes pas redevables de la technologie d'autres nations pour être compétitifs, survivre et continuer à fonctionner. C'est une priorité pour l'Europe en ce moment, avec le projet Gaia-X comme fer de lance.

Ceci est essentiel pour les chefs militaires, pour lesquels la compromission des données ou la défaillance du réseau peuvent être catastrophiques. La combinaison

de réseaux hautement distribués, d'équipes opérationnelles dispersées et d'activités coordonnées entre les nations signifie que les frontières de la sécurité ne sont plus physiques, mais virtuelles. Par conséquent, les organisations militaires sont souvent confrontées au défi de construire de nouveaux systèmes hautement sécurisés par-dessus d'anciens systèmes non sécurisés. Elles doivent non seulement être capables de le faire en toute confiance, mais aussi de le faire rapidement. La rapidité du changement signifie que les forces armées ne peuvent pas compter sur des systèmes dont la construction prend des semaines ou des mois. Au contraire, elles doivent transformer très rapidement un équipement de qualité grand public en un dispositif efficace pour la guerre.

« Si ce système est disponible depuis 1960, nous l'utilisons »

Rien n'évolue aussi rapidement ou aussi continuellement que le secteur de la technologie. Et malgré toute l'adoption de la technologie grand public dans les forces armées à ce jour, de nouvelles tendances, de nouveaux outils et de nouvelles techniques apparaissent continuellement, dont les militaires doivent être conscients. C'est notamment le cas des technologies à code faible ou inexistant, qui permettent à des personnes ayant des compétences limitées ou inexistantes en matière de codage de développer leurs propres applications sans l'aide de quiconque. Un mouvement qui a été baptisé « développement citoyen ».

Ce mouvement, qui favorise l'innovation et l'adaptabilité aux situations, est parfaitement adapté aux défis auxquels les forces armées sont confrontées, mais il doit s'appuyer sur un climat de confiance dès le départ. Les soldats de demain, tant sur le terrain qu'au niveau numérique, sont issus d'une génération très différente de celle d'aujourd'hui. Ils seront plus proches de la technologie que jamais auparavant et s'attendront à être beaucoup plus impliqués dans le développement d'applications situationnelles.

Un autre domaine d'intérêt pour les chefs militaires est la manière de relever les défis posés par les systèmes ou équipements existants - un problème qui ne se limite pas aux forces armées. L'une de mes histoires préférées est celle où, il y a 20 ans, j'ai emmené un jeune vendeur de logiciels au ministère britannique de la Défense et il a posé cette question : *« Quels systèmes informatiques utilisez-vous ici ? ».* La réponse fut la suivante : *« Si un système est disponible depuis 1960, nous l'utilisons toujours ».* C'est un défi permanent, tant dans la vie civile que dans l'armée, mais la seule façon de gérer les systèmes ou équipements existants est d'envisager les choses différemment.

La genèse des forces armées

Si les chefs militaires ont beaucoup de choses à apprendre et à comprendre, cette histoire se résume à un thème clé : le changement. Les militaires ont beaucoup à apprendre des technologies civiles : virtualisation, construction sur des plateformes sécurisées, vitesse de développement et de déploiement, utilisation et stockage des données, etc. Mais toutes ces questions ne sont que des satellites de la principale question, qui est : comment pouvez-vous gérer et embrasser le changement ?

Voilà le trait caractéristique des opérations et des organisations avancées d'aujourd'hui et, sous l'impulsion des développements au niveau civil, ce sera la genèse des forces armées numériques.

AUTEUR

Joe Baguley

Vice-president & Chief Technology Officer EMEA, VMware

VAUBAN
SESSIONS

PLUS D'INFORMATIONS SUR :

WWW.VAUBAN-SESSIONS.ORG