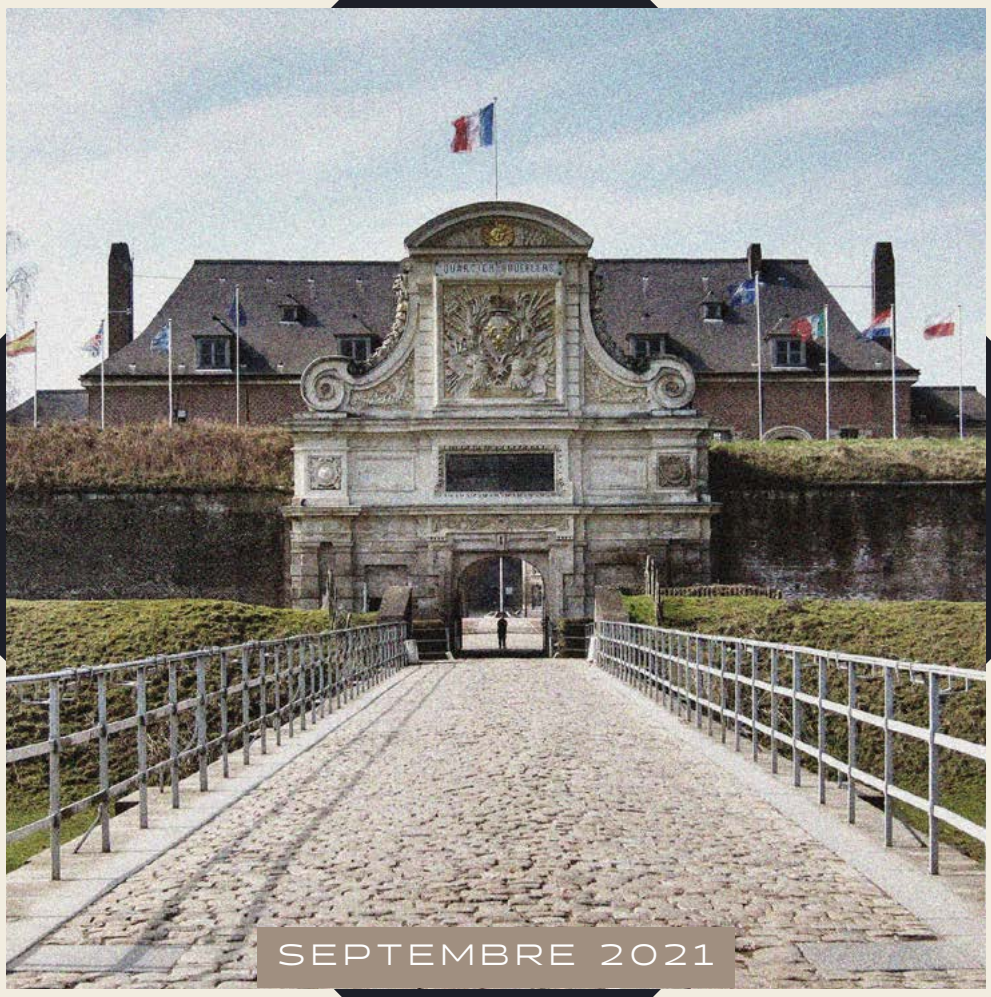
VAUBAN
SESSIONS

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



SEPTEMBRE 2021

Forward

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

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

Ces notes sont à la fois le résultat et la poursuite des discussions menées dans le cadre des Vauban Sessions 2021 et 2022, conférence annuelle organisée par Forward Global et le Corps de Réaction Rapide - France (CRR-Fr) à la citadelle Vauban de Lille. L'édition 2022 a rassemblé plus de 150 représentants d'États 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'Forward Global ou de VMware. Forward Global demeure responsable des propos engagés dans cette publication, développés en indépendance.

À PROPOS DE FORWARD GLOBAL

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

PLUS D'INFORMATIONS SUR :

forwardglobal.com

Forward

À PROPOS DE VMWARE

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

PLUS D'INFORMATIONS SUR :

vmware.com/company

vmware

COLLECTION

VAUBAN PAPERS

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'i novation 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 Forward Global

LES DONNÉES AU SERVICE DU COMBATTANT : ENJEUX ET OPPORTUNITÉS

CONTRIBUTEURS

Axel DYÈVRE
Associé
FORWARD GLOBAL

Séverin SCHNEPP
Consultant
FORWARD GLOBAL

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 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.

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.

LES DONNÉES AU SERVICE DU COMBATTANT : ENJEUX ET OPPORTUNITÉS

Si le secteur civil n'est pas confronté aux mêmes enjeux, certaines solutions qui y sont développées peuvent tout fois 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.

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.

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

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]

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

DATA WARS

RÉFLEXIONS SUR L'IMPACT DE LA TRANSFORMATION NUMÉRIQUE POUR LES FORCES ARMÉES ET LA CONDUITE DES OPÉRATIONS

CONTRIBUTEUR

Sir Edward SMYTH-OSBOURNE KCVO CBE
Commandant
ALLIED RAPID REACTION CORPS (ARRC)

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 œuvre 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.

LES DONNÉES AU SERVICE DU COMBATTANT : ENJEUX ET OPPORTUNITÉS

CONTRIBUTEURS

David TENNENHOUSE
Chief Research Officer
VMWARE

Robert AMES
Senior Director, Emerging Technology
VMWARE

Lewis SHEPHERD
Senior Director, Research & Emerging Technologies Strategy
VMWARE

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

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

et optimiser l'emploi des moyens 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.

Forward

vmware