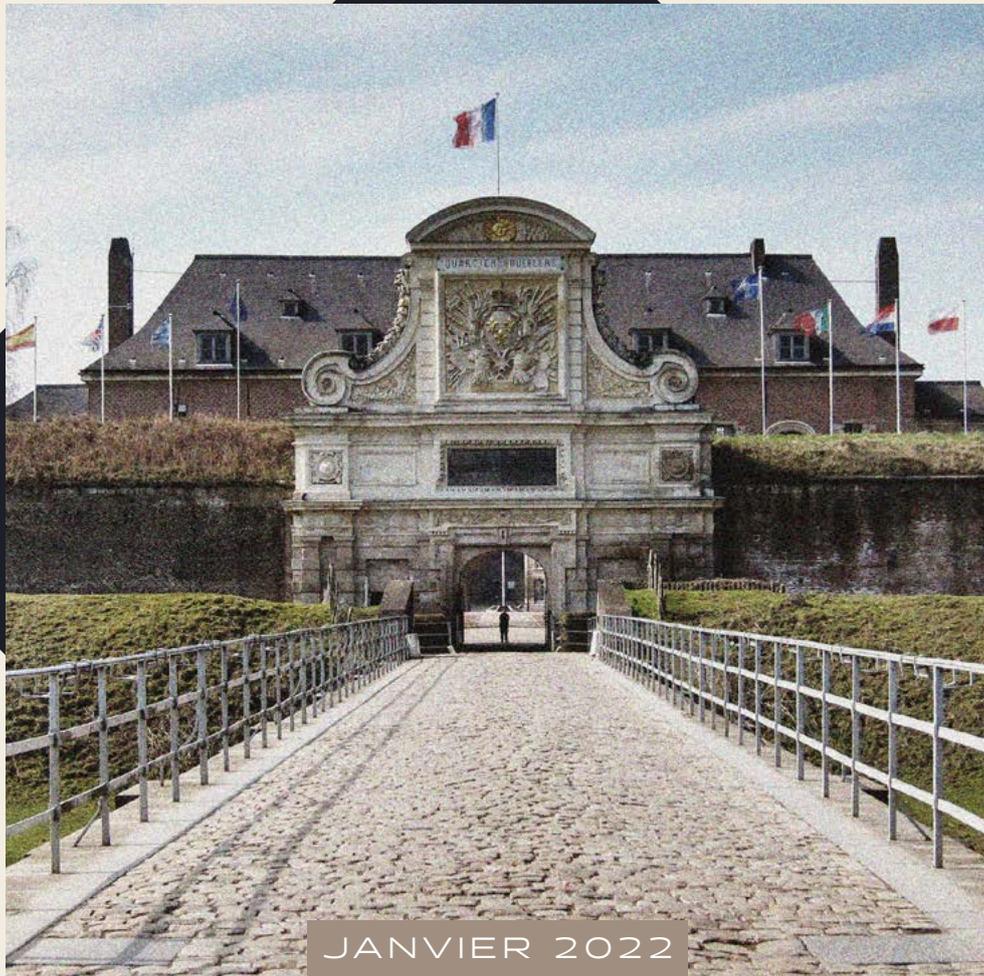




#3 LES DONNÉES AU SERVICE DU C2



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'industrie 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 Cybersécurité et Stratégie de Forward Global** accompagne ses clients publics et privés dans leur prise de décision, leur gestion du risque, leur transformation numérique, leur prospection et leur rayonnement en France, en Europe et dans le monde. Ses consultants combinent une vision prospective avec une approche métier et une connaissance opérationnelle des secteurs dans lesquels ils opèrent.

PLUS D'INFORMATIONS SUR :

forwardglobal.com

Forward 

À PROPOS DE VMWARE

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

PLUS D'INFORMATIONS SUR :

vmware.com/company

vmware®

COLLECTION VAUBAN PAPERS

PRÉFACE

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 chaînes 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 cyberspace 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 évolutions 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 Forward Global*



LES DONNÉES AU SERVICE DU C2

CONTRIBUTEURS



Axel DYÈVRE
Associé
FORWARD GLOBAL



Séverin SCHNEPP
Consultant
FORWARD GLOBAL

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 découpler 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 décision¹, 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 descendante 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

1. 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 **leurre 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 inchangées², 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* »³.

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

2. (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)
3. « 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

CONTRIBUTEUR



**Général de Corps d'Armée
Guglielmo Luigi MIGLIETTA**
Commandant

CORPS DE DÉPLOIEMENT RAPIDE - ITALIE (NRDC-ITA)

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 émergentes⁴ 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 futur 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'exécu-

tion 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

La numérisation est essentielle à la maîtrise 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.

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

LES DONNÉES AU SERVICE DU C2

CONTRIBUTEURS



Robert AMES
Senior Director,
Emerging Technology
VMWARE



Lewis SHEPHERD
Senior Director, Research &
Emerging Technologies Strategy
VMWARE

Dans les deux publications précédentes⁶, 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 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 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.

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

LES DONNÉES AU SERVICE DU C2

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.



PLUS D'INFORMATIONS SUR :
VAUBAN-SESSIONS.ORG