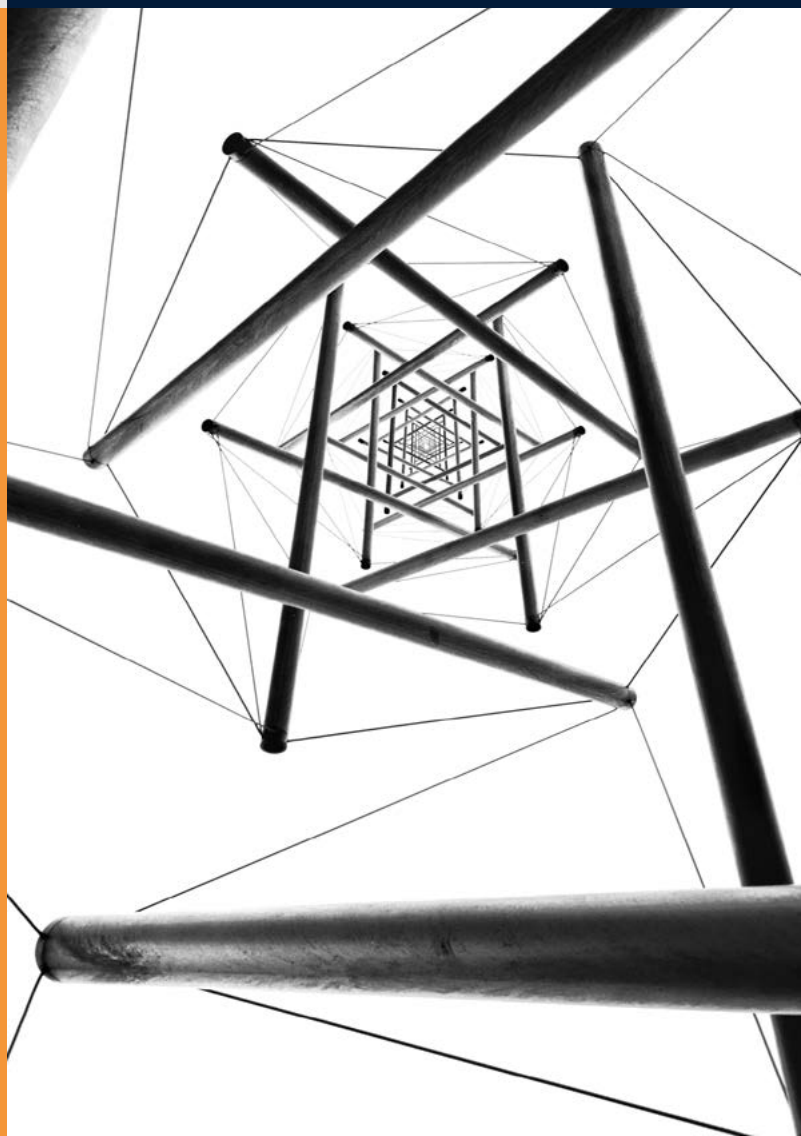
ceis

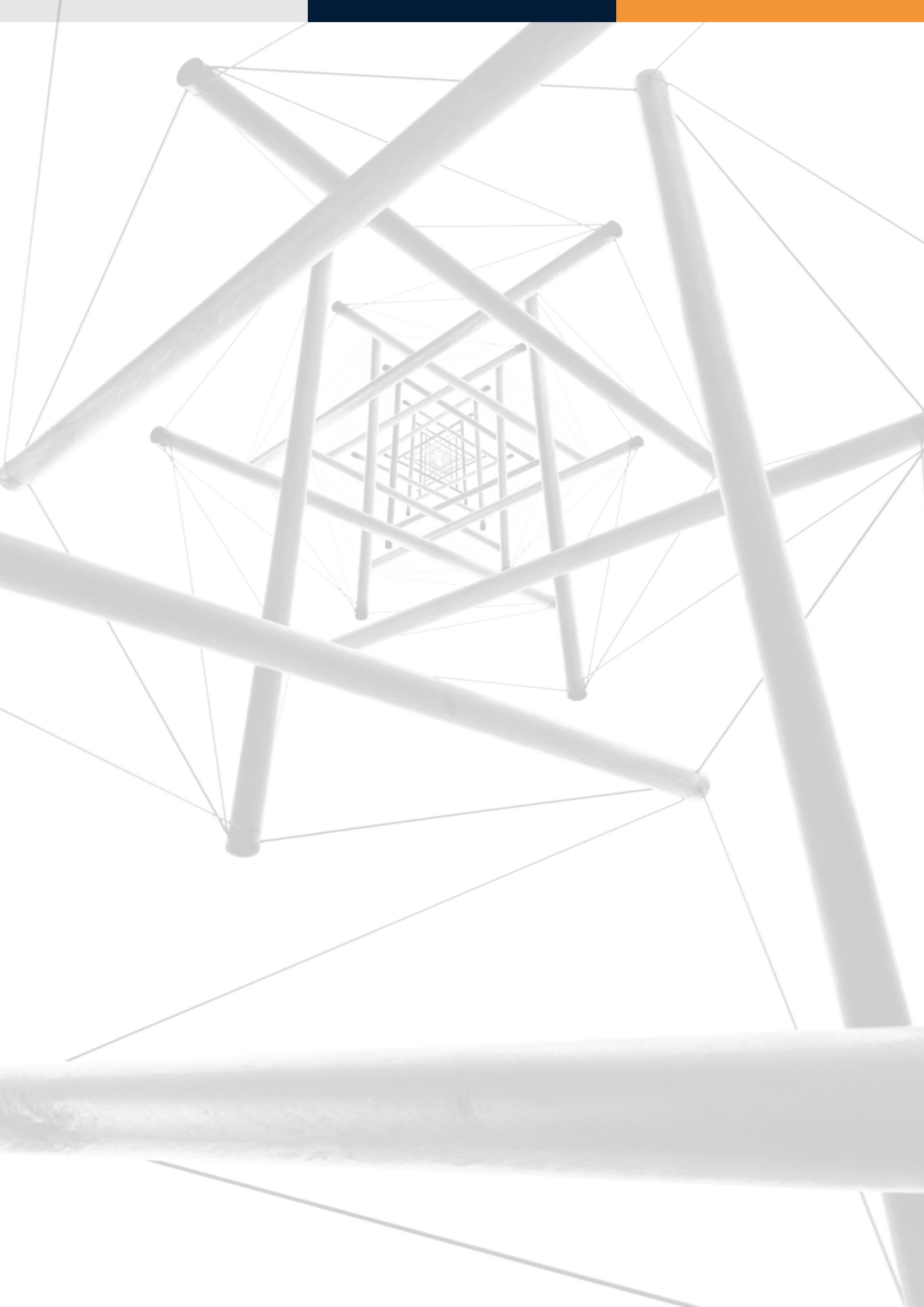
TRANSFORMATION NUMÉRIQUE DES ARMÉES



Une (r)évolution permanente

Par Axel Dyèvre, Florence Ferrando, Séverin Schnepp.

Préface par le **Général (2S) Jean-Paul Paloméros, Conseiller** Senior chez CEIS-Avisa Partners, Ancien Commandant Suprême de l'OTAN, Ancien Chef d'État Major de l'Armée de l'Air.



CEIS, membre du groupe Avisa Partners, est une société de conseil spécialisée dans les secteurs de souveraineté et leur transformation numérique. CEIS assiste ses clients dans leur développement en France et à l'international et contribue à la protection de leurs intérêts. Pour cela, les consultants de CEIS associent systématiquement vision prospective et approche opérationnelle, maîtrise des informations utiles à la décision et accompagnement dans l'action.

Les idées et opinions exprimées dans ce document n'engagent que les auteurs et ne reflètent pas nécessairement la position de CEIS ni du groupe Avisa Partners.

Ce Livre Blanc est le fruit d'un partenariat entre CEIS et VMware. CEIS demeure responsable des propos engagés dans cette publication, développés en indépendance.

Table des matières

Synthèse **5**

Préface : La Transformation Numérique au cœur des Opérations **6**

Transformation numérique : l'évolution permanente **8**

Principe de la virtualisation 8

Que peut-on virtualiser ? 10

Gains opérationnels pour les Armées **11**

Renforcer la cybersécurité des systèmes 15

Enjeux de la transformation numérique **16**

Évolutivité et maintenance 16

Maîtrise des données 17

Standards et certifications 17

Nexium Defence Cloud **18**

Conclusion : perspectives futures **19**

Publications récentes **20**

Synthèse

« La révolution numérique en cours a d'ores et déjà transformé à une allure vertigineuse notre quotidien et notre accès à l'information. Elle est également un moteur de transformation puissant pour le monde du travail, pour l'administration et plus largement pour les mécanismes de prise de décision. »[1]

Les technologies sur lesquelles la transformation numérique s'appuie sont en évolution permanente, ce qui s'accommode mal avec les cycles traditionnels des programmes d'armement. À l'heure du combat connecté et collaboratif, les Armées doivent pourtant pouvoir adopter au plus vite les meilleures technologies et innovations afin d'assurer leur suprématie opérationnelle et informationnelle. L'OTAN dans son « *Framework for Future Alliance Operations* » insiste donc sur l'importance de la collaboration avec le secteur de la recherche et le secteur privé - qui tirent l'innovation dans le domaine numérique - pour que les Armées puissent conserver un avantage technologique décisif.

Et pour gagner l'agilité et la souplesse nécessaires pour intégrer l'évolution permanente des technologies numériques, une solution innovante consiste à découpler les solutions logicielles qui évoluent très vite du matériel physique (hardware) des systèmes d'information, qui évolue naturellement moins vite. L'usage de ces technologies, dites « *de virtualisation* », permet des gains opérationnels importants :

- Réduction du poids, de l'encombrement et des consommations énergétiques
- Réduction du soutien nécessaire
- Facilitation du déploiement et de la montée en puissance
- Souplesse d'emploi et agilité accrues
- Renforcement de la cybersécurité des systèmes d'information

Mais si les avantages sont nombreux, l'emploi de la virtualisation par les forces armées doit impérativement s'inscrire dans une réflexion stratégique globale prenant en compte tous les paramètres techniques, organisationnels et financiers.

1 Source: « Ambition numérique du ministère des Armées » (France)

Préface : La Transformation Numérique au cœur des Opérations

Dans un monde secoué par des crises soudaines et durables, simultanées, imbriquées, les Armées sont confrontées à des exigences renouvelées. Il leur faut tout à la fois faire preuve de grande réactivité et de capacité à durer, s'adapter face à des stratégies hybrides, dissymétriques s'appuyant sur une large gamme de modes opératoires des plus rustiques aux plus sophistiqués, et tirant parti de techniques éprouvées (IED[2] par exemple) aussi bien que des technologies de pointe (en particulier dans le cyberespace). Il leur faut aussi se préparer à la résurgence de conflits mettant en cause des grandes puissances dotées d'importants arsenaux modernisés et développant des capacités de rupture, à l'exemple des armes hypersoniques. Dans cet environnement géostratégique, les attentes des décideurs politiques et des citoyens sont fortes et ce d'autant plus que des efforts financiers importants sont consentis pour moderniser nos Armées. Celles-ci, à défaut de pouvoir augmenter de manière significative leurs formats quantitatifs pour répondre aux nombreuses sollicitations, doivent sans cesse améliorer leur efficience, tant dans leur préparation opérationnelle qu'en opération. A ce titre la réussite de leur transformation numérique représente un enjeu crucial.

La numérisation des systèmes d'armes n'est certes pas récente, pas plus que la mise en réseau des systèmes de commandement à tous niveaux, stratégiques, opératifs ou tactiques ou encore l'acquisition et l'exploitation du renseignement quel qu'en soit son origine. Cependant, en l'état, on ne peut que constater l'écart qui se creuse entre la révolution numérique de notre société, et la démarche incrémentale vécue par nos armées. Le monde civil peut en effet s'appuyer tout à la fois sur l'essor exponentiel des technologies « *digitales* », sur le dynamisme des grands acteurs américains, voire chinois du numériques portés par un marché captif et sur la créativité sans limite des concepteurs et des utilisateurs. Les Armées, doivent, elles, gérer l'emploi de systèmes d'information opérationnels éprouvés, certifiés, sécurisés mais limités, et dans l'ensemble peu évolutifs, tout en tirant le meilleur parti d'opportunités technologiques porteuses de modernisation aux meilleurs standards du monde civil. C'est là le défi numérique auxquels sont confrontées les forces armées modernes. Pour améliorer leur réactivité, leur souplesse d'emploi, gagner la bataille du renseignement et de l'information, adapter leurs réseaux de commandement, de contrôle et d'exécution en connectant de manière dynamique l'ensemble des acteurs, réduire leur logistique, le tout dans un environnement sécurisé, il leur faut conduire et réussir leur transformation numérique au cœur des opérations.

La coopération entre les Armées et l'industrie au sens large du terme représente une des clés de la réussite de cette transformation numérique opérationnelle. Celle ci doit reposer sur des principes simples : primauté du besoin opérationnel, maîtrise des risques partagée, expérimentation en boucle ouverte, aptitude à la reconfiguration et résilience des systèmes, souplesse logistique, sécurisation de bout en bout. A ces principes fondamentaux s'ajoute pour les pays alliés et ceux amenés à travailler en coalition le besoin impératif d'interopérabilité. Celle-ci était jusqu'ici garantie par l'application de standards communs (STANAG), mais l'on mesure la difficulté de définir des normes communes dans un espace numérique en perpétuelle évolution, sinon à s'enfermer dans des logiques de systèmes propriétaires et d'en accepter les contraintes en termes de dépendance. On le voit, la transformation numérique opérationnelle n'est pas qu'un enjeu technologique, elle est avant tout conceptuelle et amène à se poser des questions fondamentales en termes d'exercice du commandement, du contrôle et de l'exécution des opérations. Il s'agit également de maîtriser les flux de données et d'informations, et de manière plus générale d'autonomie stratégique.

2 *Improvised Explosive Device* ou Engin explosifs improvisés

Face à ces enjeux, les solutions classiques montrent leurs limites, on ne peut plus concevoir comme par le passé des grands systèmes d'information relativement figés, peu adaptables, très contraignants en termes d'entretien, de mises à jour et de coût de possession. De même, pour garantir un niveau satisfaisant d'autonomie stratégique, il faut réduire la dépendance vis à vis d'un seul grand acteur du numérique quel qu'il soit et profiter de la dynamique du marché, des innovations les plus récentes pour conserver la maîtrise des systèmes de commandement et d'information. A ce titre, « *la virtualisation* » du traitement de l'information représente une nouvelle approche propre à garantir l'indispensable souplesse d'emploi, l'aptitude à la reconfiguration et à la mise à niveau, tout en réduisant les coûts d'exploitation et les contraintes logistiques. Sur le principe, et pour simplifier, la virtualisation vise à permettre à différents systèmes d'opérations et d'applications de fonctionner simultanément et indépendamment sur un seul serveur « *hôte* ».

Pour ce faire, la virtualisation exploite le plein potentiel des nouvelles technologies de miniaturisation des composants qui permet de créer des machines virtuelles (VM) dotées de leur propre autonomie et qui fonctionnent sur un seul et même serveur physique. Entre le serveur et les multiples VM, une fine couche de logiciel spécifique dite « *d'hypervision* » permet d'allouer de manière dynamique les tâches à chaque VM en fonction du besoin. On peut facilement mesurer l'intérêt de cette nouvelle approche pour démultiplier l'efficacité de chaque serveur, en réduire le nombre, décupler la résilience du système et offrir un maximum de souplesse d'emploi et de capacité de reconfiguration. A ce titre la virtualisation présente un potentiel intéressant pour garantir l'interopérabilité entre différents systèmes de commandement et d'information, objectif particulièrement important pour toutes les armées qui agissent au sein de l'OTAN ou de coalitions de circonstance.

L'exploitation opérationnelle de la virtualisation est déjà en œuvre dans d'importantes armées comme l'US Navy ou l'US Air force. Il en est de même au sein de la Royal Navy britannique qui a intégré la virtualisation au sein des sous-marins nucléaires d'attaque de dernière génération (ASTUTE). Ces exemples ainsi que d'autres applications opérationnelles sont développés dans le document joint qui se veut à la fois une introduction à la transformation numérique opérationnelle et une analyse argumentée des bénéfices et du potentiel de la virtualisation au service des forces armées.

La virtualisation ouvre la voie à une nouvelle forme de développement et d'emploi des systèmes de commandement, d'information et des équipements de défense qui permettra de satisfaire les besoins de forces armées modernes, au plus près de leurs besoins opérationnels et d'ancrer la transformation numérique au cœur des opérations.

Général (2S) Jean-Paul Paloméros
Conseiller sénior, CEIS-Avisa Partners
Ancien Commandant Suprême Transformation de l'OTAN
(NATO SACT)
Ancien Chef d'État Major de l'Armée de l'Air

Transformation numérique : l'évolution permanente

Depuis les années 1990, la « *transformation numérique* » a engendré une explosion du nombre des dispositifs communicants et des volumes de données : le volume créé est passé de 2 zettaoctets (soit deux milliards de téraoctets) en 2010 à 47 zettaoctets en 2020. La tendance devrait se poursuivre, et les volumes de données créées atteindre 2 142 zettaoctets (Zo)[3] en 2035.

L'infrastructure informatique - réseaux, hardware et software - est donc devenue un élément dimensionnant de la capacité des organisations civiles ou militaires, publiques comme privées, à profiter des gains de performance et d'efficacité opérationnelle engendrés par cette transformation numérique.

Capter l'innovation civile, en particulier dans le domaine du numérique, est donc devenue un enjeu pour les Armées depuis plusieurs années. L'accélération du rythme de l'innovation digitale se traduit notamment par l'arrivée sur le marché de nouvelles solutions logicielles et des applications à un rythme difficilement soutenable pour des systèmes d'armes dont la durée de vie est de plusieurs dizaines d'années.

Les technologies de virtualisation permettent de faire évoluer les couches logicielles de manière beaucoup plus souple, indépendamment de l'infrastructure physique sur laquelle elles sont déployées, offrant par la même occasion la possibilité de faire évoluer les capacités des systèmes d'information de manière incrémentale.

Principe de la virtualisation

La notion d'« *infrastructure informatique* » désigne l'ensemble des moyens matériels et logiciels, à savoir principalement :

- Les serveurs et terminaux informatiques (postes de travail, tablettes)
- Les réseaux
- Les objets connectés (balises, caméras, capteurs divers…)
- Les logiciels et applications

Avec la transformation numérique, un enjeu clé est d'assurer le bon fonctionnement permanent de cette infrastructure qui devient indispensable à la vie des organisations.

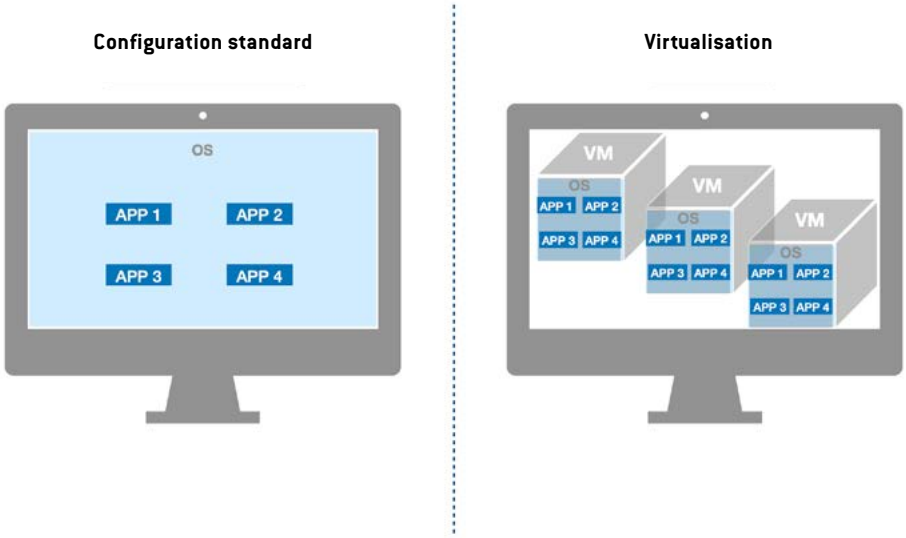
3 **« Le volume des données sera multiplié par 45 entre 2020 et 2035 »**, Journal Du Net, Marjolaine Tasset, URL. zÀ titre indicatif, 1 zettaoctet (1021) équivaut à 1 milliard de teraoctet. En comparaison, le dernier modèle d'iPhone (XR) possède une capacité maximale de 128 Go. Un teraoctet égale à 1 024 gigaoctet.

Au sein de ces infrastructures informatiques, les ordinateurs se composent de plusieurs éléments, que l'on peut structurer en différentes « *couches* » :

- Le matériel ***(hardware)***[4]
- Le système d'exploitation ***(Operating System - OS)***[5]
- Les applications et logiciels ***(softwares)***

Le principe des logiciels de virtualisation est d'optimiser l'exploitation du matériel, en faisant fonctionner dessus plusieurs environnements ségrégués, ayant chacun leur propre OS, leurs propres applications et donc leurs propres accès réseau. On appelle « *machine virtuelle* » (VM - virtual machine) ces « *instances* » créées. Ce procédé permet d'utiliser au mieux les ressources physiques d'un ordinateur (puissance de calcul ou mémoire par exemple).

Comparaison de configurations standard et virtualisée



4 « Définition : hardware », Le Mag IT, URL

5 « Définition : OS », Culture Informatique, URL

Que peut-on virtualiser ?

Selon les besoins des utilisateurs, les éléments suivants sont actuellement virtualisables[6] :

- **Les OS :** ce procédé de virtualisation permet de « *poser* » sur une même machine physique plusieurs machines virtuelles qui vont fonctionner en parallèle comme s'il y avait plusieurs machines. Cela permet d'exploiter au maximum les capacités de la machine physique, tout en limitant l'encombrement, la consommation et le poids.
- **Les postes de travail :** l'utilisateur peut simuler son environnement de travail depuis n'importe quel appareil connecté afin d'y accéder depuis n'importe où. Cela facilite également la maintenance et la mise à niveau des postes de travail puisque les applications sur ces postes virtuels résident sur un serveur central permettant de réaliser simultanément et de façon harmonisée l'ensemble des mises à jour et sauvegardes (et ainsi, respecter les normes de conformité). Un autre avantage peut être de faire fonctionner sur un même poste de travail plusieurs environnements différents cloisonnés, et même plusieurs systèmes d'exploitation différents pour utiliser par exemple des applications spécifiques.
- **Les applications :** grâce à la virtualisation, les applications sont exécutées sous une « *forme encapsulée* »[7] (aussi appelé *"container"*) permettant de faire abstraction du système d'exploitation. De cette façon, un logiciel Windows peut être utilisé sur un OS Linux ou Mac. Quel que soit son OS, l'utilisateur peut ainsi exécuter des applications indépendamment de cette limite sans pour autant virtualiser la totalité du système.
- **Le stockage :** le logiciel de virtualisation identifie l'espace de stockage disponible sur les machines physiques connectées en réseau et crée un « *disque virtuel* », contrôlable depuis une interface centrale. Cet espace de stockage est vu par les ordinateurs qui s'en servent comme un disque unique et c'est le logiciel de virtualisation qui répartit les données sur les espaces physiques disponibles.
- **Les données :** virtualiser les données permet à une application d'accéder à celles-ci « *et de les exploiter sans avoir besoin des détails sur l'emplacement physique ou le format de ces données* »[8]. Cet accès est rendu possible grâce à un logiciel de virtualisation spécifique, qui récupère ces données « *éparpillées* » dans un environnement informatique et les regroupe sous une forme unique en les virtualisant.[9] Ainsi en s'appuyant sur un tableau de bord intégré dans le logiciel de virtualisation, l'utilisateur peut agréger des données de plusieurs sources issues de différents emplacements physiques sans avoir à les copier, les déplacer ou les formater préalablement.
- **Le réseau :** un réseau traditionnel repose sur des ressources matérielles (commutateurs, routeurs, serveurs, câbles et hubs)[10]. Virtualiser un réseau permet de faire abstraction de ses composants matériels, puisqu'un réseau virtuel peut « *combiner plusieurs réseaux physiques […] ou encore diviser un réseau physique en plusieurs réseaux virtuels indépendants et distincts* ». Ici la virtualisation permet une optimisation des fonctions du réseau et présente plusieurs cas d'usages intéressants : préparation des mises à jour ou de nouvelles configurations réseau, conduite de test avant une installation sur le réseau ou encore simplification de la gestion du réseau selon les besoins des différents utilisateurs et la bande passante disponible.

6 « Qu'est-ce que la virtualisation », Citrix, URL

7 « Virtualisation : qu'est-ce que c'est et à quoi ça sert », Le Big Data, URL

8 « Qu'est-ce que la virtualisation », Citrix, URL

9 « Qu'est-ce que la virtualisation ? », Red Hat, URL

10 « Qu'est-ce que la virtualisation ? », Red Hat, URL

Gains opérationnels pour les Armées

Pour les Armées comme pour le secteur civil, investir dans des solutions de virtualisation permet des gains financiers, puisque moins d'ordinateurs physiques (*hardware*) sont nécessaires pour accomplir les mêmes tâches. Des études évaluent à 50% les gains en nombre de postes et serveurs physiques dans un parc informatique utilisant la virtualisation[11]. Le coût des licences logicielles reste lui constant, puisque même « *virtuellement* », elles sont utilisées et il faut y ajouter le coût des solutions de virtualisation.

Mais dans le contexte d'emploi des Armées et avec les contraintes très spécifiques qui sont les leurs, des avantages opérationnels viennent s'ajouter à ces avantages « *génériques* » :

- **Réduction du poids et de l'encombrement**. Les plateformes (véhicules terrestres de commandement, shelters, avions et navires) sont par nature des espaces réduits et la transformation numérique impose aux Armées des capacités informatiques embarquées toujours plus importantes. Le fait de pouvoir réduire l'encombrement et le poids tout en augmentant la puissance disponible constitue un véritable avantage dans la lutte pour la suprématie informationnelle.
- **Réduction énergétique.** La consommation électrique et la dissipation de chaleur constituent des enjeux sur les plateformes militaires : plus les équipements électroniques consomment, plus la puissance dédiée des moteurs est importante et plus la consommation de carburant l'est aussi, avec les contraintes d'autonomie et/ou de logistique que cela suppose. La dissipation de chaleur corollaire à leur fonctionnement engendre également des besoins de ventilation et de refroidissement qui accentue la consommation énergétique. En virtualisant les infrastructures informatiques, la baisse des besoins énergétiques est estimée jusqu'à 80%[12].
- **Réduction du soutien nécessaire.** La réduction des moyens physiques engendre logiquement une réduction des opérations de maintenance matérielle et donc du personnel dédié. Certaines études avancent que le gain d'une machine virtuelle par rapport à une machine physique atteindrait jusqu'à 50% en termes d'investissement et de maintenance[13]. Pour les Armées qui cherchent en permanence à réduire leur empreinte logistique pour réduire leur exposition et améliorer leur manoeuvrabilité, cet avantage présente une réelle plus-value opérationnelle.

11 « La virtualisation des données, une solution économique », CapInfo, Novembre 2019 URL

12 « How VMware Virtualization Right-sizes IT Infrastructure to Reduce Power Consumption », VMware, URL

13 « 4 major benefits of virtualisation », ACCU, URL

Virtualisation à bord des sous-marins de la classe Astute

La dernière génération de sous-marins nucléaires d'attaque de l'Armée britannique (classe Astute) intègre une solution de virtualisation pour leur système de combat intégré, au caractère hautement sensible puisque considéré comme « les yeux, oreilles et système nerveux » des bâtiments. Testée en 2016 pour un tir de torpille, la solution fournie par VMware, Dell et Aish permet de soutenir la prise de décision des membres d'équipage avec un traitement des données collectés par les capteurs et senseurs du sous-marin. Le recours à cette technologie a permis de réduire le volume des équipements physiques avec un centre de données « miniaturisé », donnant plus de flexibilité au centre opérationnel du sous-marin. Outre ce désencombrement des équipements informatiques embarqués à bord, cette solution apporte aussi une amélioration de la performance, au plus près du temps réel, et permet une amélioration de la disponibilité des bateaux, en réduisant les temps de configuration des systèmes et de leurs mises à jour.

Source : https://www.baesystems.com/en/article/artful-submarine-fires-first-torpedo-using-new-common-combat-system

- **Facilitation du déploiement et de la montée en puissance.** La souplesse d'emploi des machines virtuelles, couplée à la dématérialisation de cette configuration, permet de configurer un environnement virtualisé, au gré des missions et des exigences opérationnelles, plus rapidement et facilement qu'avec des solutions classiques. Les VM *« prêtes à l'emploi »* peuvent être transférées en utilisant un transfert réseau ou à partir de supports physiques. Par exemple, configurer les systèmes d'information nécessaires pour un navire requiert plusieurs semaines, voire des mois, pour une configuration standard, puisque cette phase de préparation exige des tests et des mises à jour de l'infrastructure informatique du bâtiment. La virtualisation de ces systèmes d'information permet de réduire le temps consacré à leur déploiement en les configurant en amont, et donc logiquement de dégager davantage de temps aux opérations, en augmentant la disponibilité du navire. Si la notion de jumeaux numérique - sorte de copie conforme de la configuration d'un système - n'est pas nouvelle, la virtualisation permet d'en simplifier grandement la mise en œuvre. Aux États-Unis, un jumeau numérique virtuel *(Digital Twin)* du porte-avions à propulsion nucléaire Abraham Lincoln (CVN-72, en service depuis 1989) a été utilisé fin 2019 pour réaliser des tests et des évaluations sur des systèmes embarqués devant être installés sur le porte-avions[14]. L'analyse du fonctionnement *« en laboratoire virtuel »* de ces systèmes a permis d'identifier des chevauchements de processus, exécutant les mêmes tâches. En corrigeant les problèmes identifiés par ce biais - processus actuellement en cours - il est attendu un gain important de bande passante, souci constant pour toutes les Armées.

14 « NAVWAR completes first digital model of systems on USS Abraham Lincoln », Naval Information Warfare Systems Command, 23/10/2019, URL

Virtualisation d'un C2

Le **United States Central Command (US CENTCOM), État Major Central américain** a développé a développé un système de contrôle, de commandement et communication (C3) facilitant les opérations en mode coalition. Déployé via un réseau de satellites et entièrement virtualisé, il permet à chaque nation alliée des États-Unis de se connecter à un environnement numérique commun rassemblant des informations collectées par différentes sources (unités au sol, drones de reconnaissance, véhicules blindés, QG avancé). Les avantages sont nombreux :

- Déploiement rapide du système (10-15 minutes) ;
- Plus grande coordination et interopérabilité des forces alliées, chacune recevant la même information au même moment (flux continu et en temps quasi-réel) ;
- Haut niveau de sécurité (micro-segmentation du réseau - NSX) empêchant la propagation d'attaques sur l'ensemble du réseau et offrant un délai plus long pour les contrer ;
- Déconnexion rapide une fois la mission terminée (2-5 minutes).

Le système a notamment été testé lors de l'exercice Bold Quest (Savannah, Géorgie, États-Unis) qui a rassemblé 1800 soldats de 16 pays alliés.

- **Souplesse d'emploi et agilité accrues**. Dans le cas des systèmes de « *Command & Control* » (C2), par exemple, la virtualisation permet de déployer, sauvegarder et restaurer facilement des machines virtuelles. C'est le principe d'encapsulation[15] qui permet techniquement de simplifier des actions sur les machines virtuelles (copies, sauvegardes ou création), et notamment d'effectuer un déplacement complet de systèmes informatiques d'un serveur physique à un autre sans engendrer d'interruption de services. Ainsi le parc de machines virtuelles d'un C2 peut rapidement être ajusté, voire reconfiguré, au gré des besoins opérationnels en se reposant sur la possibilité offerte par un Cloud tactique, déployé au plus près du théâtre d'opérations. À titre d'illustration, lors de l'exercice Trident Jupiter (fin 2019), l'OTAN a évalué les performances de ses systèmes informatiques, et notamment son *RemoteApp Provisioning Service*, un système permettant aux utilisateurs d'utiliser des applications informatiques OTAN non installées sur leurs postes de travail. Un autre élément clé de l'exercice a été le déploiement en 18 heures du réseau de communication et d'information (*CIS*) par un bataillon OTAN basé en Bulgarie. Grâce au système C3 tactique virtualisé « *DragonFly HQ08* », adapté à un réseau dynamique et utilisant la microsegmentation pour garantir sa cybersécurité, le bataillon bulgare a pu fournir un réseau de communication aux utilisateurs localisés à Stavanger en Norvège.[16]

- **Virtualisation de systèmes historiques (legacy).** Les Armées disposent d'une variété de systèmes et équipements existants (*legacy systems*[17]), leur intégration dans un environnement numérique moderne représente un vrai défi. En outre, n'ayant pas été conçus pour fonctionner dans des environnements aussi connectés que les systèmes actuels, ils peuvent être vulnérables sur le plan de la cybersécurité. La possibilité de « *porter* » ces systèmes anciens[18] sur des machines virtuelles fonctionnant sur des environnements modernes permet de prolonger leur vie opérationnelle plutôt que de se lancer dans des refontes complètes.

15 VMware vSphere 4. Mise en place d'une infrastructure virtuelle, URL

16 « NCIA puts IT systems to the test in exercise Trident Jupiter », NCIA, URL

17 Le terme legacy systems désigne un système utilisé par une organisation qui est dépassé d'une manière ou d'un autre par l'état de l'art ou le marché actuel.

18 « VMware vSphere 4. Mise en place d'une infrastructure virtuelle », URL

Kessel Run[19], une approche de l'innovation radicalement différente de l'Armée de l'Air américaine

Sorte de « *fabrique à logiciels* », le projet Kessel Run de l'USAF propose une approche radicalement différente de l'innovation via sur une méthodologie agile. Kessel Run a permis de résoudre de nombreux défis rencontrés précédemment dans le développement des logiciels utilisés par l'US Air Force.

Le projet se distingue par :

- Un projet s'appuyant sur une plateforme de développement agile d'applications métiers par des utilisateurs finaux (Pivotal Lab)
- Un développement conduit donc par les militaires eux-mêmes, au plus près aux besoins opérationnels
- Une conception en cycles courts itératifs d'applications opérationnelles et un déploiement rapide grâce à la virtualisation
- Des déploiements automatisés pour les mises à jour des applications développées.

Ainsi, les équipes de Kessel Run ont réussi à livrer une plateforme homologuée de développement pour un *Secret Internet Protocol Router* en moins de 130 jours à une base située au Qatar - là où le précédent programme avait duré 10 ans et coûté près de $ 340 millions, sans pour autant « *avoir fourni de capacité significative* ».

Sources: https://mwi.usma.edu/software-wins-modern-wars-air-force-learned-kessel-run/ & https://media.defense.gov/2019/Mar/07/2002097482/-1/-1/0/SWAP_STUDY_VIGNETTES.PDF

19 "Why Kessel Run is such a big deal", The Business of Federal Technology, URL

Renforcer la cybersécurité des systèmes

L'impératif de connectivité, voire d'hyperconnectivité, est au cœur des problématiques de sécurité des systèmes et équipements informatiques qui doivent communiquer et être interconnectés afin d'optimiser leur efficacité. Or connecter crée *de facto* des vulnérabilités : un serveur totalement isolé, dédié à une seule application, sera logiquement mieux protégé puisque présentant une seule porte d'entrée.

À l'heure du combat collaboratif et donc connecté, la virtualisation permet de renforcer la cybersécurité des systèmes d'information :

- **Fonctionnement en « *silo* »** : La virtualisation permet de créer autant de machines virtuelles que de besoins à satisfaire, et de faire fonctionner des OS ou applications de façon isolée et indépendante, sans avoir à multiplier le nombre de machines. Chaque machine virtuelle disposant de ses propres configurations, applications et d'une configuration réseau adaptée, les risques cyber sont ainsi limités.
- **Sécurité assurée par l'isolation** : L'isolation des machines virtuelles garantit leur sécurité et celle des autres puisque les éventuelles vulnérabilités d'une VM n'affectent pas les autres, alors qu'elles fonctionnent avec les mêmes composants matériels. Les VM peuvent aussi servir d'espace sécurisé pour tester les mises à jour logicielles avant de les déployer sur l'ensemble des postes de travail. La sécurité du dispositif de virtualisation est elle-même assurée par l'hyperviseur, qui permet une gestion centralisée.
- **Ségrégation des environnements de travail** : La virtualisation permet de faire cohabiter des environnements de travail différents sur le même matériel informatique en complète ségrégation. Cette possibilité présente des avantages pour les opérations en coalition, puisqu'elle permet par exemple à un opérateur français déployé dans le cadre d'une mission OTAN d'utiliser sur le même ordinateur son système informatique habituel et celui de l'Alliance. Chaque système est alors hébergé par une machine virtuelle différente et isolée.
- **Création d'environnements sécurisés pour les forces amies.** Dans un contexte de coalition, la virtualisation permet d'envisager de manière plus simple et sécurisée la participation des forces amies à un système d'information, en leur mettant à disposition des VM sécurisées et prêtes à l'emploi, qu'elles pourront facilement « *poser* » sur leur infrastructure.
- **Création facilitée de « *pots de miel* »**. Virtualiser un système d'information facilite également le passage à une posture plus offensive de cybersécurité. La technique du « *pot de miel* » (*honeypot*[20]) permet de créer un faux réseau pour tromper l'adversaire, observer ses méthodes et ses cibles, sans compromettre le reste des réseaux et équipements. De cette manière, les moyens de l'adversaire sont mobilisés sur une cible factice qui peut permettre aussi de l'intoxiquer en le laissant accéder à des informations faussées. La virtualisation permet de faciliter la mise en oeuvre de ces « *pots de miel* », en minimisant les besoins tout en maximisant leur réalisme.

20 « La virtualisation pour quoi faire ? », Françoise Berthoud & Maurice Libes, URL

Enjeux de la transformation numérique

Si la virtualisation peut apporter des réponses aux problèmes soulevés par la transformation digitale des forces armées, certains points doivent être pris en compte pour réussir un déploiement sécurisé et efficace de cette solution logicielle.

Évolutivité et maintenance

La disponibilité des compétences techniques IT et cyber représentant un enjeu majeur pour les Armées, le choix des architectures et des solutions mises en oeuvre constitue un enjeu important entre coûts de licence et coûts d'intégration et sont donc des points clé à prendre en compte. En effet, comme tout logiciel, les solutions de virtualisation doivent être déployées, maintenues et mises à jour régulièrement afin de prendre en compte l'évolution des environnements, corriger les anomalies de fonctionnement et les failles de sécurité et enfin développer de nouvelles fonctions.

Certes, des solutions de virtualisation en open source existent, comme Oracle VM Virtual Box ou encore OpenVZ[21]. Ces solutions sont souvent gratuites et permettent un accès facilité au code source. Toutefois, comme pour tous les logiciels open source, la maintenance n'est pas contractuelle et n'est donc pas toujours assurée avec la même diligence que pour les solutions propriétaires, car elle repose souvent sur une forme de « *bénévolat* » de la communauté qui les soutient. La faiblesse du support oblige souvent les organisations utilisatrices à assumer elles-mêmes les problèmes d'intégration logicielle ou à faire appel à des prestataires, augmentant ainsi les coûts. L'absence de feuilles de route techniques peut également représenter un inconvénient pour la planification des organisations. À titre d'illustration, dans le domaine de la virtualisation, la seule société VMware - leader mondial des solutions de virtualisation - investit annuellement près de 2 milliards de dollars pour ses activités de R&D[22].

L'utilisation d'une solution de virtualisation, qu'elle soit propriétaire ou open source, est par nature engageante, car l'infrastructure se développe autour de solutions spécifiques. Cet aspect est à prendre en considération pour ne pas se trouver face à un problème de durabilité des architectures, en cas d'arrêt du développement de la solution - risque plus imprévisible souvent pour les solutions open source ; mais aussi dans l'hypothèse d'un changement de politique tarifaire ; ou encore dans l'hypothèse d'une nouvelle rupture technologique.

21 « Le point sur la virtualisation Open Source », Wooster, Juin 2014, URL

22 « NITECH. NATO Innovation and Technology », NCI Agency, Juin 2020, URL

Maîtrise des données

Plusieurs types de solutions de virtualisation existent sur le marché, que ce soit en open source ou propriétaires. Parmi celles-ci, les solutions de virtualisation dites « *on-premise* » semblent les mieux adaptées à des usages militaires. Ce procédé permet aux acteurs de la Défense de disposer d'une licence du logiciel et de l'utiliser en toute indépendance, en conservant la responsabilité de la gestion de l'infrastructure informatique mobilisée - un effort non négligeable en termes de ressources et compétences humaines par rapport à des solutions en Cloud. En revanche, cette solution « *on premise* » permet aux Armées de garder le contrôle de la mise en oeuvre de ces solutions et surtout de garder leurs données sur leurs réseaux internes.

Standards et certifications

Les évolutions technologiques rapides posent des problèmes de standardisation et de certification, pour répondre aux exigences de résilience et de sécurité du secteur de la Défense. En effet, ces processus de standardisation et de certification demeurent longs, avec des procédures conséquentes, en décalage avec le rythme accéléré de l'innovation technologique. Par exemple, une solution ou un service de virtualisation peut être engagé dans un processus de certification et connaître durant ce laps de temps une mise à jour ou un changement de version - rendant son processus de certification obsolète. Toutefois, certaines solutions de virtualisation, comme VMware[23] et Red Hat[24] par exemple, sont conformes à des standards internationaux - comme les Critères Communs[25] - ou nationaux, comme les standards américains « *Federal Information Processing Standard (FIPS)* ». En outre, les solutions de virtualisation intègrent généralement des dispositions de sécurisation garantissant leur résilience - tels que des hyperviseurs qui prennent en charge la gestion des machines virtuelles. En leur assignant des tâches spécifiques, ils permettent d'appliquer le principe d'isolation entre les différentes machines virtuelles déployées.

23 VMware FIPS 140-2 Validated Cryptographic Modules URL

24 Red Hat Completes FIPS 140-2 Re-certification for Red Hat Enterprise Linux 7 URL

25 Les Critères Communs (ou **Common Criteria**, CC) consistent un ensemble de normes permettant d'évaluer la sécurité des systèmes et les logiciels. URL

NEXIUM DEFENCE CLOUD

THALES

La supériorité informationnelle est aujourd'hui une arme décisive dans le monde militaire. NEXIUM Defence Cloud (NDC) est une solution certifiée pour les Forces Armées qui permet de combiner la maitrise de l'information avec l'usage d'un système compact. Cette solution repose sur une infrastructure de cloud privé, agile et hautement sécurisé, disponible du Quartier Général jusqu'aux postes de commandement et aux unités mobiles sur le théâtre, au plus proche du soldat. Cette offre répond aux spécifications les plus exigeantes de la défense, notamment en termes de sécurité et de durcissement du matériel, et est conforme aux derniers standards militaires comme le Federated Mission Network (FMN) de l'OTAN.

Les principaux avantages de NEXIUM Defence Cloud sont :

- L'accélération du combat collaboratif, (situation awareness, etc.), des boucles OODA et sensor-to-shooter, et de la consolidation du renseignement et du partage de l'information multi milieux,
- L'information sécurisée partagée avec une architecture Zero Trust, le cryptage de niveau militaire, le support des différents niveaux de classification et l'accès basé sur le besoin d'en connaître,
- Des déploiements maitrisés, des reconfigurations agiles avec un Système de Communication et d'Information (SIC) entièrement orchestré,
- La résilience en cas de déconnexion, ou de connexion intermittente et à débit limité, ainsi qu'en cas de guerre électronique et de cyberattaques
- Des formats matériels durcis pour résister aux conditions extrêmes (taille, poids, énergie, refroidissement, vibrations, etc.) et s'adapter à une logistique réduite avec des formats standardisés,
- Agilité et évolutivité avec les outils cloud-natifs (chaîne DevSecOps, virtualisation, containeurs, etc.),
- Le support d'applications cloud reposant sur des fonctions avancées (ex : IA, Big Data)

L'infrastructure Nexium Defence Cloud maximise l'usage des ressources IT limitées en environnement contraint, avec la virtualisation et les containeurs, pour offrir agilité et flexibilité opérationnelles. Ainsi, toutes les ressources de calcul, de stockage et de réseau sont gérées de façon transparente, et ne nécessitent pas de connaissances spécifiques pour l'opérateur sur le théâtre. Les capacités des réseaux hétérogènes sont optimisées afin de toujours bénéficier du plus haut niveau de disponibilité.

NEXIUM Defence Cloud facilite la transition vers le Cloud en centralisant tous les services digitaux, existants et nouveaux, dans un unique portail et il réduit le coût total de possession (TCO). Les technologies cloud de Vmware sont déterminantes dans cette solution.

NEXIUM Defence Cloud peut être opéré dans tous les milieux et dans toutes les coalitions. Quel que soit l'enjeu.

Conclusion : perspectives futures

Virtualiser de nouveaux équipements. Si la technologie de virtualisation est considérée comme mature pour des composants d'infrastructure informatique (serveurs, postes de travail, réseaux, données, applications), avec des cas d'usages au sein de différentes Armées, d'autres systèmes informatiques restent encore à virtualiser. C'est le cas des terminaux fonctionnant sous une architecture dite *Advanced Risk Machine* (ARM). L'architecture d'un système établit comment il est organisé pour accomplir sa fonction[26]. Les architectures ARM sont utilisées pour des processeurs plus petits[27], intégrés dans la plupart des tablettes numériques et des smartphones, mais également dans des objets connectés comprenant des capteurs embarqués (véhicules, montres intelligentes, robotique, systèmes d'armes, etc.). À ce jour, la virtualisation de ce type d'équipements est encore au stade expérimental compte tenu de la miniaturisation des composants électroniques et de leur puissance limitée, rendant encore techniquement difficile le fonctionnement optimal d'un logiciel additionnel.

Faciliter l'usage du Cloud dans les Armées. L'usage de Clouds tactiques contribue *« à la mise en réseau de tous les acteurs et à la valorisation de l'information au service de la conduite des opérations »*[28]. L'usage de la virtualisation permet de démultiplier le potentiel du Cloud puisqu'elle permet aux ordinateurs connectés à ce Cloud de mettre à disposition ou de piocher auprès d'autres serveurs et terminaux des ressources supplémentaires (logiciels, données, stockage, puissance de calcul par exemple). Elle permet de rationaliser encore davantage les capacités d'exploitation de chaque machine (*hardware*) composant le parc informatique et offre une gestion plus souple de l'ensemble du système informatique grâce à l'automatisation de certains processus (*software*).

Anticiper l'arrivée de la 5G. À l'heure actuelle, l'une des principales limitations à l'usage du Cloud dans les Armées est la bande passante limitée des réseaux militaires. Depuis plusieurs années, les Armées étudient et testent des *« bulles tactiques LTE »*, utilisant la 4G privée pour avoir accès au très haut débit mobile en opération. De cette manière, elles peuvent disposer d'une bande passante plus élevée qu'avec des réseaux radio classiques pour partager tout type d'information multimédia (voix, photos, vidéo, informations géoréférencées, etc.). Selon le ministère français des Armées, *« l'utilisation de bulles tactiques 5G, succédant à des bulles 4G/LTE, permettrait l'usage de services et de technologies cloud sur le terrain. »*[29]. La 5G[30] vise à fournir 10 à 100 fois plus de débit que les actuels réseaux 4G[31], ce qui accélérerait fortement l'interconnexion entre les différents éléments. À la différence des réseaux 4G, les réseaux 5G seront décentralisés. Des fonctions essentielles comme le routage ou la mise en communication ne seront plus uniquement gérées au niveau du cœur de réseau, mais pourront être déportées en périphérie, au niveau des stations de base. La virtualisation sera au coeur de la 5G, grâce à des architectures de type *Network Function Virtualization* et *Software-Defined Network*, qui reposeront sur la séparation des fonctions d'acheminement (transmission de l'information d'une source vers une cible) et de contrôle (calcul des routes, mise en œuvre des politiques de priorisation et de rejet des différents trafics) du réseau. Cela permettra une orchestration du réseau plus flexible et en éliminant les briques physiques (*hardware*),

26 « Architecture logicielle et conception avancée », DigiSchool Ingénieurs, URL

27 « Qu'est-ce qu'un processeur ARM ? », 01 Net, URL

28 Ibid

29 « Enjeux de la 5G au ministère des Armées », Observatoire des nouveaux usages du numériques, Novembre 2019, URL

30 5G signifie 5ème génération

31 « Présentation des réseaux 5G - Caractéristiques et usages », Thales Group, URL

la virtualisation contribuera aussi à diminuer les investissements et les coûts opérationnels. Un logiciel central gérera et coordonnera des tâches auparavant opérées par des infrastructures physiques, limitant ainsi les coûts de fonctionnement. En outre, en améliorant la fiabilité, la performance, le débit et réduisant la latence, la 5G pourra contribuer à faciliter la virtualisation des réseaux, permettant aux forces sur les théâtres d'opérations de déployer par exemple des systèmes de C2 virtualisés rapidement et à distance.

Publications récentes

À télécharger sur **www.ceis.eu**

A2/AD, déni d'accès et interdiction de zone – Réalité opérationnelle et limites du concept

Intelligence artificielle, Applications et enjeux pour les Armées

Blockchain, Enjeux, usages et contraintes pour la Défense

Renseignement, facteur humain et biais cognitif

Réalité immersive, Usages des réalités virtuelle et augmentée pour la Défense

TRANSFORMATION NUMÉRIQUE DES ARMÉES

Une (r)évolution permanente

Par Axel Dyèvre, Florence Ferrando, Séverin Schnepp.

Préface par le **Général (2S) Jean-Paul Paloméros, Conseiller** Senior chez CEIS-Avisa Partners, Ancien Commandant Suprême de l'OTAN, Ancien Chef d'État Major de l'Armée de l'Air.

ceis

avisa partners

CEIS, membre du groupe Avisa Partners, est une société de conseil spécialisé dans les secteurs de souveraineté et leur transformation numérique.

CEIS Paris
Tour Montparnasse - 33 avenue du Maine
BP 36 - 75 755 Paris Cedex 15
France

CEIS Bruxelles
Boulevard du Régent, 35
1000 Bruxelles
Belgique

www.ceis.eu
www.avisa-partners.com