ceis

Août 2016

Emploi du Cloud dans les Armées

Première approche des concepts et contraintes

Par Axel Dyèvre, Pierre Goetz,
et Martin de Maupeou

Les notes stratégiques

L'intelligence
de la décision

Les notes stratégiques

Notes d'étude et d'analyse

Les auteurs souhaitent remercier l'ensemble des experts rencontrés au cours de cette étude.

Les idées et opinions exprimées dans ce document n'engagent que les auteurs et ne reflètent pas nécessairement la position de CEIS ou des experts rencontrés.

CEIS est une société d'études et de conseil en stratégie. Sa vocation est d'assister ses clients dans leur développement en France et à l'international et de contribuer à la protection de leurs intérêts. Pour cela, les 80 consultants de CEIS associent systématiquement vision prospective et approche opérationnelle, maîtrise des informations utiles à la décision et accompagnement dans l'action.

CEIS met en œuvre et anime le DGA Lab, le laboratoire d'innovation du ministère de la Défense www.defense.gouv.fr/dga/innovation2/dga-lab

La Direction Générale pour l'Armement a initié en 2013 un centre de réflexion sur l'innovation et un espace de démonstrations de technologies innovantes dans le domaine des systèmes d'informations, le SIA Lab (**www.sia-lab.fr**), créé et animé par CEIS sous la responsabilité du Groupe Sopra Steria, architecte-intégrateur du programme SIA.
Forte du succès de cette initiative, la DGA a étendu en 2016 le périmètre de ce centre à l'ensemble des domaines technologiques d'intérêt pour la défense et a lancé le DGA Lab. Espace de démonstration technologique mais aussi de réflexion collaborative sur les usages des nouvelles technologies, le DGA Lab est ouvert à l'ensemble des acteurs de l'innovation de défense, au premier rang desquels les opérationnels du ministère de la Défense.
Le DGA Lab est mis en œuvre et animé par la DGA avec le concours des sociétés CEIS et SopraSteria.

Dans le cadre de cette activité, les consultants de CEIS publient des Notes Stratégiques portant notamment sur les questions relatives aux impacts de la transformation numérique pour la Défense.

Travaillant étroitement avec les équipes de CEIS et le DGA Lab, le **Bureau Européen de CEIS** à Bruxelles, conseille et assiste les acteurs publics, européens ou nationaux, ainsi que les acteurs privés dans l'élaboration de leur stratégie européenne, notamment sur les problématiques de défense, sécurité, transport, énergie et affaires maritimes. CEIS - Bureau Européen participe également à des projets de recherche européens dans ces domaines. Pour mener à bien l'ensemble de ses missions, l'équipe s'appuie sur un réseau européen de contacts, d'experts et de partenaires.

Contact :
Axel Dyèvre
adyevre@ceis.eu

CEIS
Tour Montparnasse
33 avenue du Maine
75755 Paris Cedex 15
+33 1 45 55 00 20

CEIS - Bureau Européen
Boulevard Charlemagne, 42
B-1000 Bruxelles
+32 2 646 70 43

DGA Lab
40, rue d'Oradour-sur-Glâne
F-75015 Paris
+33 1 84 17 82 77

www.ceis.eu

Retrouvez toutes les Notes Stratégiques sur **www.ceis.eu** et **www.sia-lab.fr**

Sommaire

Synthèse

“Nous créons actuellement en deux jours autant d’information que nous en avions créée depuis la naissance de la civilisation jusqu’en 2003”
Eric Schmidt, PDG de Google (2010)

Ces dix dernières années ont vu une multiplication des terminaux connectés générant toujours plus de données, soit par action humaine, soit - et de plus en plus - de manière automatisée. Dans le même temps, les réseaux de communication ont vu leurs débits augmenter, que ce soit les réseaux locaux sans fil comme le Wifi, les réseaux de télécommunication sans fil comme la 4G ou les réseaux de télécommunication fixe comme la fibre ou le VDSL. En conséquence, les volumes de données échangés sur les réseaux – à commencer par Internet – ont explosé.

Ce mouvement a entrainé un passage d’un mode de fonctionnement classique « en local » – c’est-à-dire reposant sur l’utilisation de ressources principalement stockées sur le terminal de l’utilisateur – à un mode de fonctionnement généralisé « en Cloud », faisant très largement appel à des données et des applications hébergées à distance par le biais d’un réseau Internet ou non.

Le fonctionnement en Cloud est devenu en effet l’un des moyens les plus efficaces pour transmettre, stocker ou accéder à de grandes quantités d’informations de manière quasi instantanée. L’usage du Cloud repose donc en tout premier lieu sur l’accessibilité et la disponibilité des réseaux qui

permettent d'accéder aux données, aux applications et à une puissance de calcul hébergées sur des serveurs externes.

Pour les Armées, la problématique est double. D'un côté, les volumes de données produits ou à utiliser explosent, exactement comme pour le civil. En opérations, les niveaux tactiques ou opératifs ont de plus en plus de besoins d'accès et de transmission de données, phénomène qui va s'accentuer avec l'arrivée en service de véhicules ou de plateformes plus communicantes.

Mais d'un autre côté, les missions s'effectuent la plupart du temps dans des conditions dégradées ou contraintes d'accès aux réseaux. Les unités doivent donc pouvoir travailler aussi bien « connectées » que « déconnectées » ou avec des niveaux de connexion (serveurs de réplication asynchrone par exemple) plus ou moins localisés. Ceci doit permettre d'éviter tant les pertes de capacités opérationnelles que les dysfonctionnements liés à la latence des réseaux.

Pour les Armées, l'enjeu du fonctionnement en Cloud est donc d'assurer la bonne répartition des ressources informatiques entre les différents niveaux afin de garantir la disponibilité, la résilience et l'autonomie possible de chaque niveau. Le tout devant tendre à une utilisation la plus transparente possible pour les utilisateurs, exactement comme c'est le cas dans le secteur civil et dans les applications grand public : quel utilisateur de Gmail s'est-il déjà fait la réflexion que l'applicatif serveur dont il se servait était une application « en Cloud » et dont les données étaient également hébergées « dans le Cloud » ? Quel utilisateur d'iPhone regardant sur son ordinateur les photos prises de son téléphone quelques secondes plus tôt s'est demandé si elles avaient été transférées automatiquement sur son espace iCloud consultable de tous ses périphériques enregistrés ?

Introduction

Au cours de ces dernières années les volumes d'information créés, consultés et échangés ont explosé. Le monde produisait 5 exaoctets d'informationnel en deux jours en 2011 mais deux ans plus tard, en 2013, il lui fallait seulement dix minutes pour produire la même quantité d'information[1]. Cette accélération exponentielle - qui se poursuit - s'explique en grande partie par la multiplication des terminaux connectés et par les performances accrues de débits des réseaux de communication.

La conséquence principale de ces évolutions a été une transition progressive mais complète du mode de fonctionnement de l'informatique aussi bien personnelle que professionnelle. Jusqu'à il y a seulement quelques années, les données et les applications des utilisateurs étaient stockées localement sur leur ordinateur, voire - dans le cas des administrations ou des sociétés - sur des serveurs locaux. Désormais, l'ensemble des terminaux connectés (téléphones, tablettes et ordinateurs) tendent à devenir de simples interfaces permettant d'accéder à du contenu, des services et des applications qui sont en fait stockés à distance – sur des serveurs externes - et qui peuvent être consultés et ou utilisés depuis un terminal en réseau.

Par ce biais, l'utilisateur a accès en permanence aux mêmes informations et ce quelle que soit la connexion utilisée – terrestre ou cellulaire – et le lieu dans lequel il se trouve – au bureau, à la maison, ou en déplacement.

DropBox et iCloud sont des exemples grand public de la mise en pratique de ce mode de fonctionnement : ces solutions permettent par exemple à un utilisateur d'avoir accès depuis tous ses terminaux et en permanence à une

[1] http://www.lecese.fr/sites/default/files/pdf/Avis/2015/2015_01_donnees_numeriques.pdf

bibliothèque de plusieurs milliers de photos ou à des giga-octets de documents divers sans avoir besoin de les stocker localement. Ces éléments sont en effet hébergés sur des serveurs externes et seule une petite partie - icône ou version allégées de ces photos; métadonnées et aperçu des documents - est physiquement présente sur les diver appareils de l'utilisateur : téléphone, tablette, ordinateur, etc. Cela permet notamment de faire en sorte qu'une photo prise depuis un appareil « se retrouve » sur - ou plus précisément soit accessible depuis – tous les autres terminaux appartenant à un utilisateur donné et ce de façon simultanée.

Le même mécanisme permet d'avoir recours à des applications ou à de la puissance de calcul « externes » à partir d'un terminal local connecté en réseau. Entreprises et particuliers recourent ainsi de plus en plus à de telles applications qui tendent à devenir des « services ». L'exemple le plus ancien est probablement le mail : les utilisateurs se connectent via une application ou un navigateur web à une application hébergée à distance et accessible par Internet (ou Intranet selon le cas). La plupart du temps, cette utilisation est tellement fluide et aisée que l'utilisateur ne se rend même plus compte qu'il utilise des ressources qui ne sont en fait pas physiquement stockées sur son terminal.

Autre avantage - pour les directions informatiques et financières - la flexibilité, qu'autorise le fonctionnement en Cloud. En effet, les besoins en puissance de calcul ou en capacité de stockage des particuliers mais surtout des entreprises peuvent varier rapidement et dans de grandes proportions. Une solution, très coûteuse, peut consister à dimensionner son infrastructure pour lui permettre de couvrir les besoins maximaux – par exemple en capacité de stockage – tout en sachant que de tels espaces ne seraient dans les faits utilisés pleinement qu'une partie du temps. L'autre option qui tend à se

développer consiste à avoir recours à des serveurs – virtuels[2] ou non – hébergés chez des prestataires externes. Cela permet de faire varier quasiment au jour le jour la taille et la composition d'une infrastructure informatique en « ajoutant » ou « supprimant » des serveurs – c'est-à-dire en achetant de l'espace supplémentaire ou au contraire en réduisant son forfait - en fonction des besoins.

L'ensemble de ces nouveau usages - hébergement de données à distance, applications et infrastructures externalisées - relèvent de ce que l'on appelle le *« Cloud » ou « Cloud Computing », c'est-à-dire « l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet*[3] *[NDA : mais pas exclusivement donc]*[4]*».*

L'infographie des pages suivantes est issue du site www.thoughtsoncloud.com

[2] Un serveur virtuel est une méthode de partage d'un serveur physique (hardware) en plusieurs serveurs virtuels indépendants (software) qui ont chacun les caractéristiques d'un serveur dédié. Chaque serveur peut fonctionner avec un système d'exploitation différent et redémarrer indépendamment. Les différents serveurs virtuels « tournent » en même temps sur une seule machine et optimisent l'utilisation du matériel en réduisant les coûts.
[3] L'expression Cloud Computing vient d'ailleurs de la représentation qui est faite d'Internet dans les diagrammes informatiques en utilisant une icône de nuage.
[4] https://fr.wikipedia.org/wiki/Cloud_computing

Cloud Computing : faire face à l'explosion des données

« [Le Cloud Computing est un] modèle permettant un accès réseau pratique et à la demande à une famille de ressources informatiques partagées par tous qui peuvent être rapidement mobilisées ou libérées en utilisant des efforts minimaux de gestion ou d'interaction avec le fournisseur de service ».

Définition du National Institute of Standards and Technology (NIST)

Le Cloud s'est imposé progressivement

En faisant appel à des technologies et des concepts datant des débuts des réseaux informatiques, le Cloud Computing a fait son chemin au cours des dernières décennies pour atteindre un niveau de maturité technologique permettant d'accorder les moyens - entre informatique localisée sur un terminal et virtualisée sur des serveurs - aux besoins des utilisateurs.

Ces progrès technologiques concernent en particulier la virtualisation, qui consiste à faire tourner plusieurs systèmes d'exploitation sur une même machine physique, et l'augmentation considérable de la capacité et de la vitesse des réseaux.

Dès les années 1980, les data centres concentraient déjà d'importantes ressources informatiques, fournissant des accès et des services à des organisations et stockant leurs données. De même, la mise à disposition d'applications fournies comme un service, que l'on désigne désormais « Software as a service » dans la terminologie du Cloud Computing, est une pratique connue depuis de nombreuses années qu'offrent ceux que l'on

nommait dans les années 1990-2000 les « Application Service Providers » (ASP). Ces applications étaient hébergées et centralisées sur un serveur unique et accessible à travers un réseau.

Dans les années 1990, la tendance, portée par la miniaturisation accrue des composants, était davantage au développement d'ordinateurs dotés de capacités de stockage et de calcul importantes.

Au cours de la dernière décennie, la « transformation numérique » a été le résultat des progrès technologiques, de la multiplication des usages, de l'augmentation des débits, de l'omniprésence des terminaux mobiles et de l'interconnexion des réseaux. Le mode de fonctionnement en « Cloud » s'est ainsi généralisé ces dernières années pour répondre à ces mutations et à la croissance de l'activité, de la mobilité et du volume des données informatiques.

Dans les 10 à 15 dernières années les besoins des utilisateurs ont évolué au fur et à mesure de l'apparition de nouvelles possibilités :

- Accéder à de plus en plus d'information, à la demande et sans être contraint d'en stocker l'intégralité
- Disposer de la même information et des mêmes services sur différents terminaux
- Partager l'information en temps réel avec des collaborateurs mobiles
- Evoluer dans un environnement technologique transparent et ergonomique permettant l'utilisation de terminaux légers et de différents types et systèmes

Le Cloud, réalité d'aujourd'hui pour la Défense

Si le grand public et le secteur civil ont vu le Cloud émerger comme une solution à l'explosion des volumes de données et des usages, les Armées n'ont pas échappé à cette tendance, sans que les utilisateurs, notamment militaires, ne s'en rendent forcément compte. De nombreuses applications dans le domaine de l'administration et de la gestion sont ainsi « passées » dans le Cloud privé du ministère de la Défense. Elles recouvrent plusieurs fonctions dont notamment la formation à distance, la gestion des ressources humaines, la planification des activités, la gestion des frais de déplacements, la simulation de paiement, la gestion des pannes informatiques, la gestion des commandes d'habillement, l'annuaire, etc. Pour le moment, l'usage du Cloud computing se cantonne essentiellement à l'environnement de travail administratif du ministère de la Défense. Il n'est en effet pas encore véritablement exploité pour l'aspect opérationnel des missions.

Il sera néanmoins de plus en plus difficile d'imaginer que les capacités de stockage et de traitement nécessaires à une force en opération puissent être intégralement déployées sur place et qu'elles fonctionnent en totale autarcie. A titre d'illustration, un drone collecte au cours d'une mission l'équivalent de la contenance de 20 ordinateurs portables[5]. En conséquence, le recours à des moyens répartis de traitement et de stockage[6] va probablement s'imposer progressivement comme la seule possibilité pour faire face à des volumes croissants de données générées, stockées, traitées et échangées.

Le « Cloud Computing » est donc l'application généralisée d'un concept datant des origines de l'informatique, rendu possible par les progrès technologiques et les économies financières générées. Il permet d'adapter les

[5] http://www.claws.in/1286/big-data-a-big-bet-applicability-in-the-defence-forces-haridas-m.html#sthash.z6jjZkVN.dpuf

[6] En plus des IaaS, PaaS et SaaS décrits ci-dessus, on parle désormais également de Network as a Service (NaaS), Storage as a Service (STaaS), Workplace as a Service (WaaS), etc

outils numériques aux besoins de mobilité, de puissance et d'accessibilité des utilisateurs. Les évolutions stratégiques opérées par une société informatique comme Apple à dix ans d'intervalle illustrent bien cette transformation :

- En 2001, Apple dote ses ordinateurs d'un nouveau système d'exploitation, OSX, qui doit permettre de faire de l'ordinateur le centre du « Hub numérique » auquel se connectent l'ensemble des périphériques. Ce « Hub numérique » est lui même raccordé au réseau.
- En 2010, c'est le Cloud, soit le réseau, qui devient le cœur du système. Le réseau permet d'accéder aux données, aux applications et aux services numériques. L'ordinateur, le téléphone et les multiples terminaux sont autant de périphériques, ou objets connectés qui communiquent via Internet pour échanger des données, stockées en réseau.

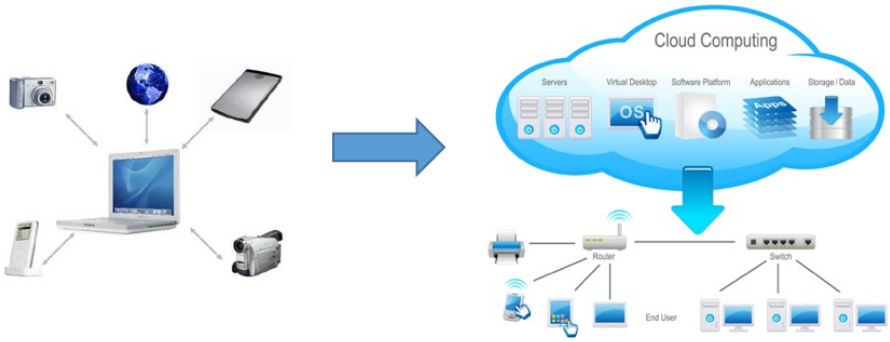
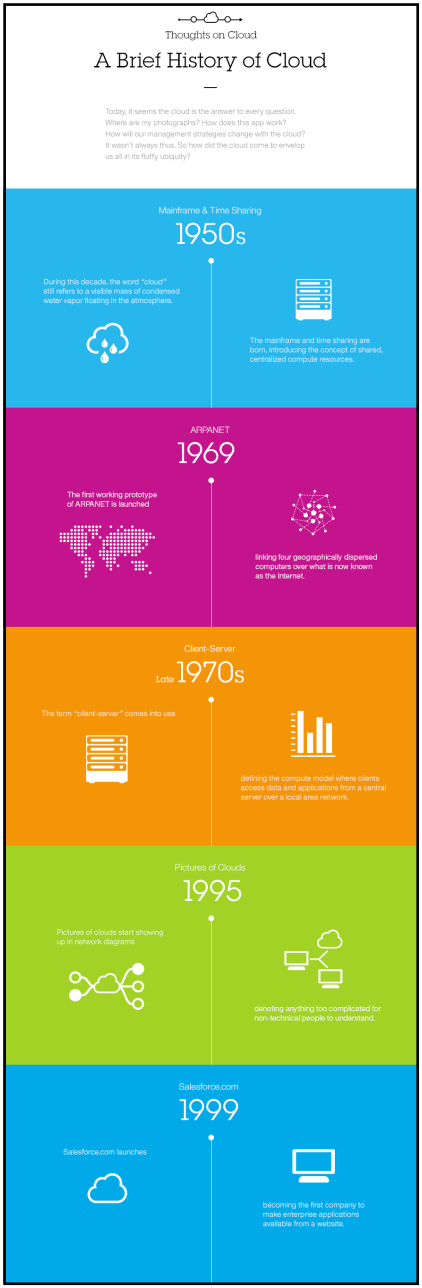
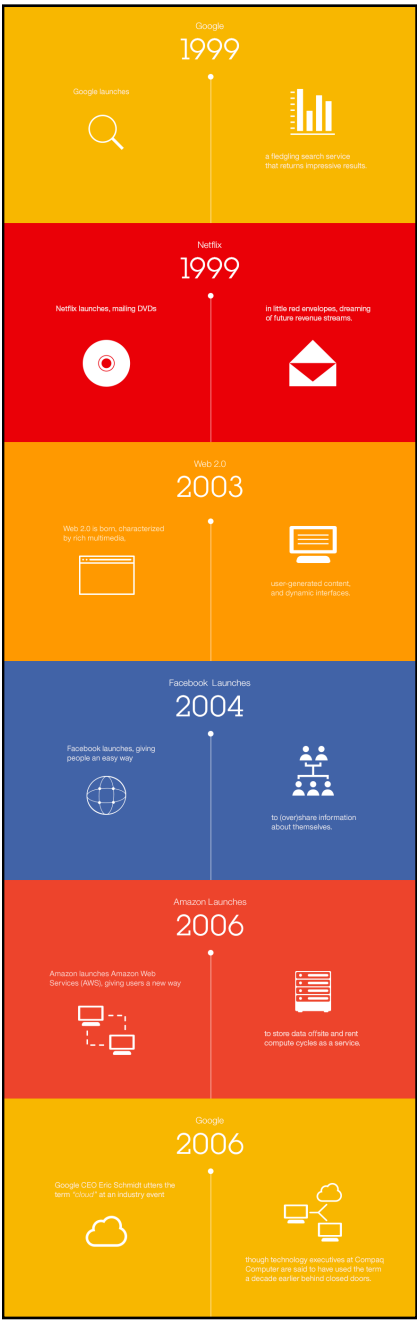


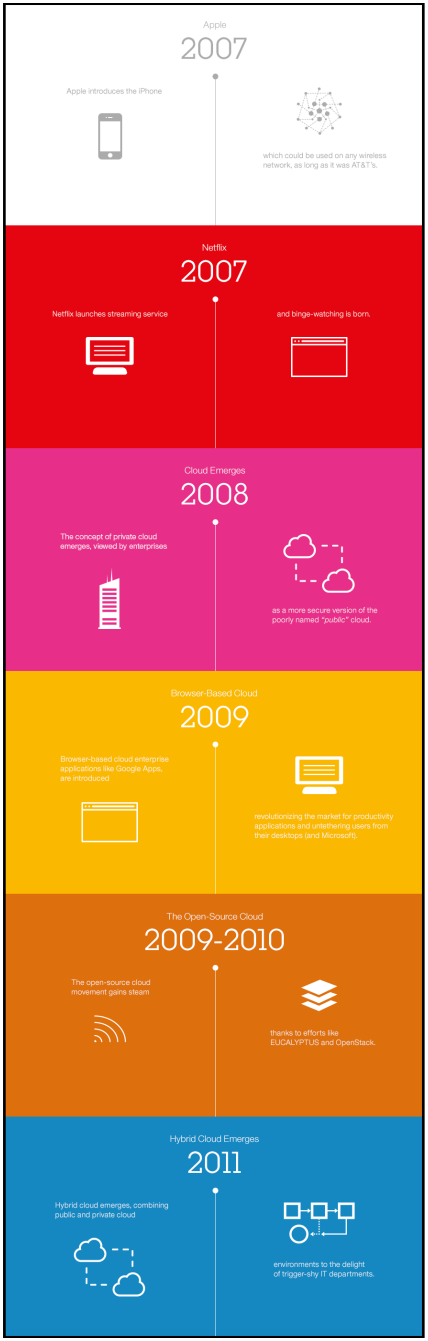
Figure 1 - *Le réseau, au cœur de l'environnement numérique*[7]

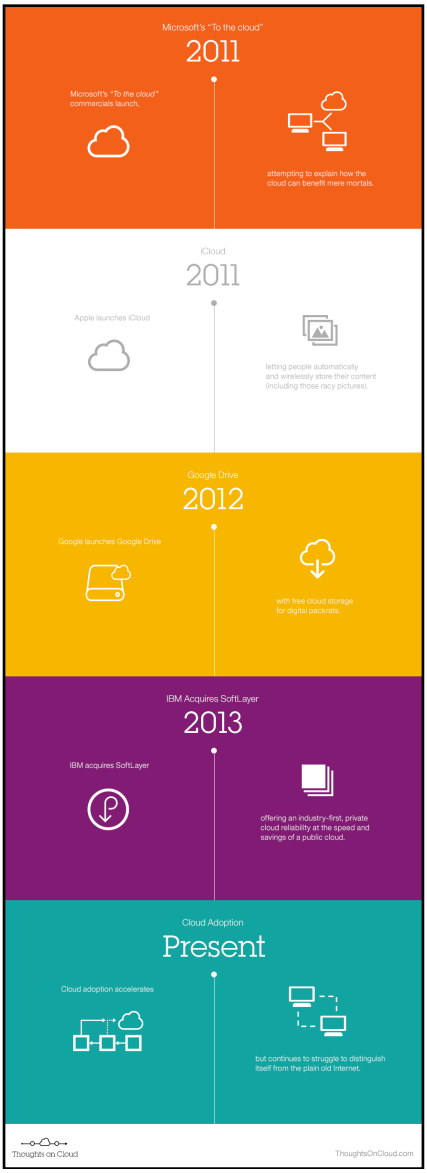
Le Cloud Computing propose ainsi une architecture qui opère un compromis entre serveurs, offrant une capacité de stockage et de calcul considérable à distance accessible via le réseau, et terminaux permettant de disposer de capacités de traitement et de stockage adaptées à l'usage « local ».

[7] Sources : Apple et http://toulouse.groupe-sii.com/fr/TOU_infra_reseau_et_systeme


Thoughts on Cloud
A Brief History of Cloud
Today, it seems the cloud is the answer to every question.
Where are my photographs? How does this app work?
How will our management strategies change with the cloud?
It wasn't always thus. So how did the cloud come to envelop
us all in its fluffy ubiquity?
Mainframe & Time Sharing
1950s
During this decade, the word "cloud"
still refers to a visible mass of condensed
water vapor floating in the atmosphere.
The mainframe and time sharing are
born, introducing the concept of shared,
centralized compute resources.
ARPANET
1969
The first working prototype
of ARPANET is launched
linking four geographically dispersed
computers over what is now known
as the Internet.
Client-Server
Late 1970s
The term "client-server" comes into use
defining the compute model where clients
access data and applications from a central
server over a local area network.
Pictures of Clouds
1995
Pictures of clouds start showing
up in network diagrams
denoting anything too complicated for
non-technical people to understand.
Salesforce.com
1999
Salesforce.com launches
becoming the first company to
make enterprise applications
available from a website.


Google
1999
Google launches
a fledgling search service
that returns impressive results.
Netflix
1999
Netflix launches, mailing DVDs
in little red envelopes, dreaming
of future revenue streams.
Web 2.0
2003
Web 2.0 is born, characterized
by rich multimedia,
user-generated content,
and dynamic interfaces.
Facebook Launches
2004
Facebook launches, giving
people an easy way
to overshare information
about themselves.
Amazon Launches
2006
Amazon launches Amazon Web
Services (AWS), giving users a new way
to store data offsite and rent
compute cycles as a service.
Google
2006
Google CEO Eric Schmidt utters the
term "cloud" at an industry event
though technology executives at Compaq
Computer are said to have used the term
a decade earlier behind closed doors.


Apple
2007
Apple introduces the iPhone
which could be used on any wireless network, as long as it was AT&T's.
Netflix
2007
Netflix launches streaming service
and binge-watching is born.
Cloud Emerges
2008
The concept of private cloud emerges, viewed by enterprises
as a more secure version of the poorly named "public" cloud.
Browser-Based Cloud
2009
Browser-based cloud enterprise applications like Google Apps, are introduced
revolutionizing the market for productivity applications and untethering users from their desktops (and Microsoft).
The Open-Source Cloud
2009-2010
The open-source cloud movement gains steam
thanks to efforts like EUCALYPTUS and OpenStack.
Hybrid Cloud Emerges
2011
Hybrid cloud emerges, combining public and private cloud
environments to the delight of trigger-shy IT departments.


Microsoft's "To the cloud"
2011
Microsoft's "To the cloud" commercials launch,
attempting to explain how the cloud can benefit mere mortals.
iCloud
2011
Apple launches iCloud
letting people automatically and wirelessly store their content (including those racy pictures).
Google Drive
2012
Google launches Google Drive
with free cloud storage for digital packrats.
IBM Acquires SoftLayer
2013
IBM acquires SoftLayer
offering an industry-first, private cloud reliability at the speed and savings of a public cloud.
Cloud Adoption
Present
Cloud adoption accelerates
but continues to struggle to distinguish itself from the plain old Internet.
Thoughts on Cloud
ThoughtsOnCloud.com

Modèles de services Cloud

Il existe plusieurs types d'utilisation du Cloud et plusieurs modèles de déploiement qui répondent à différents besoins, selon différents modèles de coût :

Le « Cloud public » : des ressources (données ou applications) sont hébergées chez un fournisseur et disponibles à tous à la demande via Internet. Le Cloud public ne veut pas dire pour autant que ces ressources sont ouvertes, mais uniquement qu'elles sont hébergées sur des serveurs partagés avec d'autres utilisateurs. Amazon EC2, Windows Azure et Google Apps Engine comptent parmi les principaux Clouds publics. L'exemple du service « Dropbox » illustre ce concept : les particuliers peuvent y souscrire et leurs données sont hébergées sur des serveurs pouvant être physiquement localisés n'importe où dans le monde (et qui sont dupliqués en cas de défaillance). Néanmoins, même si des millions d'utilisateurs utilisent les mêmes centres de données et, à l'intérieur, partagent également les mêmes serveurs, leurs données ne sont accessibles que par eux même sauf s'ils souhaitent les partager avec des personnes précises. Il en est de même avec les usages « professionnels » de ces services de Cloud public.

Le « Cloud privé » : le principe général est le même que dans le premier cas mais les serveurs utilisés sont à l'usage exclusif d'une seule organisation. L'infrastructure peut être hébergée par l'organisation elle-même et mise à disposition sur son réseau ou via internet par VPN ou tunnel, mais il peut aussi s'agir d'une infrastructure de Cloud hébergée par un tiers qui reste dédiée et uniquement accessible par l'organisation. Le Cloud privé présente des avantages en termes de contrôle, de protection et de confidentialité des

données et applications hébergées. Bien plus onéreuse que la version « publique », cette solution est en général principalement mise en œuvre par des organisations de très grande taille.

Le « Cloud hybride » : cette troisième possibilité vise à combiner des infrastructures de Clouds privées et publiques. Une partie de l'infrastructure est alors physiquement hébergée dans les locaux de l'organisation, l'autre partie se trouvant chez un ou plusieurs prestataires extérieurs. Les données et applications sont ensuite réparties généralement en fonction de leur sensibilité ou de la criticité de leur disponibilité. Un rapport[8] publié par la société d'études Gartner en juin 2016 estime que, d'ici 2020, l'utilisation du Cloud hybride sera la norme car il combine les avantages en termes de coûts et d'évolutivité des Clouds publics d'une part, et la sécurité d'un Cloud privé pour des opérations sensibles d'autre part.

Modèles de déploiement du Cloud

Au-delà de cette approche par type de service fourni, il est également possible de catégoriser le Cloud selon les types de déploiement et les niveaux d'intervention fournis.

Cela peut ainsi concerner l'infrastructure (**IaaS ou infrastructure as a service** : stockage des données, puissance de calcul), la plate-forme d'exécution (PaaS : platform as a service ; exécution et intégration des applications) mais aussi les services (SaaS : software as a service : bureautique, applications métiers).

[8] http://www.gartner.com/newsroom/id/3354117

Couches	Cloud	Fonction	Illustration
Donnée		Stocker et accéder à la demande à un large volume de données	Dossier partagé
Application	SaaS	Utiliser des applications	Service de messagerie mail
Infrastructure	IaaS	Accéder à des capacités de traitement, de stockage ou de communication	Serveur
Plateforme	PaaS	Pouvoir déployer et exécuter sur l'infrastructures ses propres applications	Plateforme de développement

Un concept adapté aux besoins opérationnels des Armées

Les missions des Armées requièrent de plus en plus un accès, une circulation et une exploitation rapides de l'information dans des contextes d'opérations aux multiples contraintes d'environnement et de sécurité. C'est ce que soulignait dès 2013 le Livre Blanc sur la Défense et la Sécurité Nationale (LBDSN), en définissant la maitrise de l'information comme un facteur clef d'autonomie d'évaluation de situation, de décision et d'action de la France[9].

Dans cette perspective, le ministère de la Défense ambitionne de développer un modèle de force global à même de remplir ses missions en rapprochant toujours plus les unités, les équipements et les systèmes d'armes, au moyen de systèmes d'information opérationnels et de communications (SIOC) performants.

Une transformation entamée

Sur le théâtre d'opération, les plateformes de combat et les soldats tendent ainsi à être dotés de capacités d'émission de l'information et de conduite collaborative du combat, qui contribuent au raccourcissement de la boucle décisionnelle et à l'accélération du rythme du combat. C'est par exemple l'objectif du programme SCORPION qui inclura un système d'information du combat (SICS) unique mettant en réseau tous les systèmes produisant un effet tactique sur le terrain.

[9] Voir Note Stratégique : https://www.sia-lab.fr/sites/sia/files/images/note_strategique_sia_maitrise_information.pdf

Le programme SIA, en unifiant progressivement les systèmes d'information des Armées (Terre, Marine, Air) du niveau stratégique (CPCO, DRM) jusqu'au niveau opératif des brigades, des bâtiments et des bases aériennes, participe du même objectif.

Cette transformation progressive des capacités et de l'environnement du combattant multiplie les sources et les volumes d'information. Elle fait de chaque plateforme - satellites, drones, véhicules, radars, soldats etc. - autant d'objets connectés à même de capter, diffuser et échanger de l'information.

Les Armées font ainsi face aux même défis que ceux observés dans le monde civil à savoir :

1. **L'augmentation des volumes d'information** générés et échangés qui sont autant de ressources utiles à la conduite des opérations qu'il importe de traiter, exploiter, valoriser et partager entre les différents niveaux de commandement et d'action tout en préservant l'autonomie du chef.
2. **La mise en réseau des hommes, des équipements et des infrastructures** qui sont autant d'éléments connectés à même de recevoir et transmettre de l'information tout en faisant peser le risque d'une dépendance à l'égard de la technologie.
3. **La mobilité et la réactivité des Armées** dont la projection sur des théâtres éloignés dans des intervalles de temps toujours plus réduits rend nécessaire le raccourcissement de la boucle informationnelle tout en imposant des environnements et contextes d'opération dégradés.

Se pose dès lors la question des défis techniques liés à l'accroissement du volume et de la diversité des données à exploiter : images satellitaires, interceptions radar, communications militaires, données logistiques, etc. Comment stocker, traiter et échanger de façon efficace, ces masses considérables de données et accéder aux applications permettant de les exploiter sur le terrain ?

Les mêmes besoins engendrant souvent la mise en œuvre de solutions comparables, l'externalisation et la virtualisation des systèmes d'information – déjà bien engagées dans le monde civil - seront très probablement également dans les années à venir au cœur du déploiement opérationnel des Armées.

L'US Army[10] s'y est déjà attelée et a privilégié une approche de « Cloud privé » avec le programme APC2[11] articulé autour de quatre objectifs principaux :

- Réalisation d'économies d'échelle et optimisation des coûts par la mutualisation des capacités d'hébergement et de traitement des données.
- Sécurisation accrue des données et des services.
- Amélioration de la qualité de service et de la puissance de traitement disponible.
- Simplification de l'accès aux données à partir de terminaux mobiles.

Le contrat prévoit également la livraison de data centres mobiles afin de délivrer les services au plus près des théâtres d'opération. Plus généralement, l'Armée américaine utilise simultanément ressources localisées et distantes, internes et externes dans nombre de ses systèmes[12]. Un document intitulé « Army Cloud Computing Strategy » a d'ailleurs été publié à ce sujet[13].

[10] http://www.penseemiliterre.fr/le-cloud-computing-dans-les-applications-militaires-la-defense-francaise-peut-mieux-faire_2015825.html
[11] http://www.informationweek.com/cloud/army-awards-$250-million-cloud-contract/d/d-id/1102108
[12] https://www.army.mil/article/169635/reaching_for_the_cloud
[13] http://ciog6.army.mil/Portals/1/Army_Cloud_Computing_Strategy%20Final_v1_0.pdf

Une réflexion en cours dans les Armées

En France, l'amélioration des capacités d'échange de l'information et de communication que permet le Cloud Computing pourrait également se traduire par des gains opérationnels et notamment :

- La réduction de la boucle OODA[14] grâce à un accès et un partage simplifié de l'information entre les différents niveaux de décision.
- L'interopérabilité croissante entre les hommes, les équipements et les systèmes d'armes, tous en mesure d'accéder à la demande à une information commune et synchronisée.
- La réduction du risque de perte de données dans la mesure où la destruction d'un appareil ne signifierait plus forcément la disparition des données.

Ces gains opérationnels pourraient être déclinés dans de nombreux domaines comme la surveillance et le renseignement mais également la logistique.

La réflexion actuelle autour de la mise en place d'un « Cloud tactique » ou « Cloud de théâtre » témoigne de la volonté d'appliquer ce mode de fonctionnement pour répondre aux besoins opérationnels des Armées pour la conduite des opérations.

De même que dans le civil le modèle du Cloud hybride mêle Cloud privé et Cloud public, il pourrait s'agir pour les Armées de pouvoir disposer d'une part d'un Cloud, déployé localement au sein des unités (qui serait en quelque sorte le Cloud privé) et mettant à disposition de celles-ci les informations nécessaires à la conduite des opérations sur le terrain. Elles disposeraient d'autre part d'un Cloud central (qui jouerait le rôle de Cloud public - en étant

[14] Observer, s'orienter, décider et agir

bien sûr réservé au seul usage du ministère), sorte de méta-Cloud de la Défense permettant de faire remonter l'information au niveau stratégique et de se connecter à l'ensemble des Clouds locaux.

L'Armée dispose déjà d'une forme de ce « Cloud central/public » : la DIRISI (Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la Défense) met en œuvre le « Cloud Défense » qui repose sur cinq data centres principaux localisés en métropole et dont les capacités permettent de garantir aux Armées la disponibilité, la souveraineté et la sécurité des données hébergées (RH, logistique, financier, ...). Ce « Cloud Défense » devrait être achevé en 2017[15].

Cette esquisse d'environnement Cloud militaire correspond en quelque sorte à un mode d'hybridation entre des capacités locales et des capacités centrales de stockage et d'échange d'information.

En hybridant des ressources locales et distantes, l'ambition est de pouvoir répartir les applications et les données entre les différents niveaux (tactique, opératif et stratégique) en fonction du besoin tout en prenant en compte les risques liés :

- A la sécurité et à la confidentialité des données.
- A la disponibilité de l'information, dans des contextes de faibles débits voire de perte possible du réseau.

L'adoption progressive d'un mode de fonctionnement en « Cloud » par les Armées vise à terme à impliquer les unités déployées au plus bas niveau sur le théâtre d'opération.

[15] Revue Transmetteurs n°9 (juin 2015) https://tools.etrs.terre.defense.gouv.fr/etrs/enligne/transmetteurs/transmetteurs_9/files/docs/all.pdf

A travers le concept de « Cloud tactique », ce sont les systèmes d'information opérationnels et de communication, encore souvent fragmentés en fonction des Armées et des niveaux de commandement, qui bénéficieront et contribueront à la mise en réseau de tous les acteurs et à la valorisation de l'information au service de la conduite des opérations.

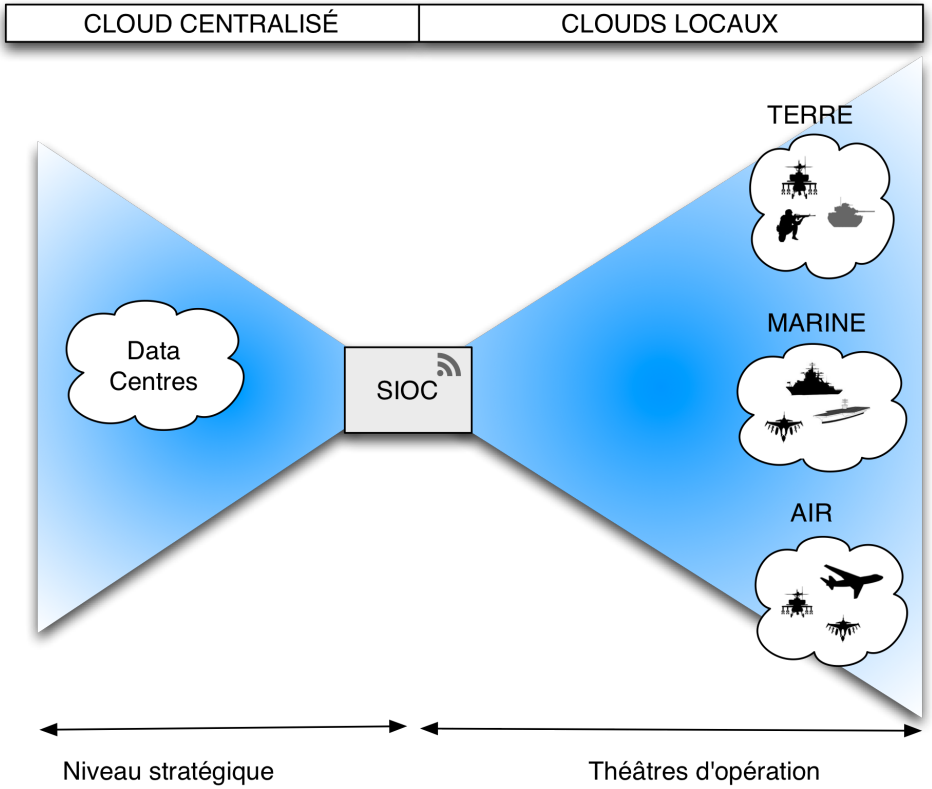


Figure 2 *- Cloud tactique*

Le Cloud computing à l'épreuve des contraintes militaires

Au vu des besoins croissants d'accès rapide à de grandes quantités d'informations, la question n'est plus seulement de savoir si les Armées vont devoir se pencher sur la question de mettre en place des Clouds tactiques hybridant des ressources localisées et distantes, elle est aussi de déterminer de quelle manière ils pourront être déployés en pratique compte tenu des contraintes opérationnelles particulières qui présideront à leur mise en œuvre dans un contexte militaire.

En plus des armées conventionnelles – et notamment l'US Army – qui réfléchissent à la mise en œuvre de solutions basées sur le Cloud, il est intéressant de noter que certains adversaires non conventionnels emploient déjà ce type de solutions, notamment pour leurs communications.

Le Cloud est déjà mis à profit par l'adversaire

L'exemple de Daesh, qui fait un usage massif de l'application Telegram — fonctionnant en service Cloud[16] — tant pour assurer sa propagande que pour transmettre des ordres, vient aussitôt à l'esprit[17].

Comme l'indique le site Internet de l'application, cette dernière permet de se connecter à distance, de coordonner des groupes allant jusqu'à 5 000

[16] *Telegram is a cloud service. We store messages, photos, videos and documents from your cloud chats on our servers, so that you can access your data from any of your devices anytime and use our instant server search to quickly access your messages from waaay back. All data is stored heavily encrypted and the encryption keys in each case are stored in several other DCs in different jurisdictions. This way local engineers or physical intruders cannot get access to user data*. https://telegram.org/privacy

[17] http://www.frandroid.com/culture-tech/324124_telegram-vecteurs-de-propagande-prefere-de-daesh

personnes, de synchroniser les conversations entre différents outils, d'envoyer des documents de tous types de formats, de crypter les messages et même de faire en sorte de les détruire de manière programmée. Ces contenus, textes, audio, photos et videos, sont stockés sur des serveurs hébergés par le fournisseur du service. Le protocole est basé sur le chiffrement AES-256 qui est considéré comme l'un des plus sécurisés et qui n'a officiellement jamais été compromis.

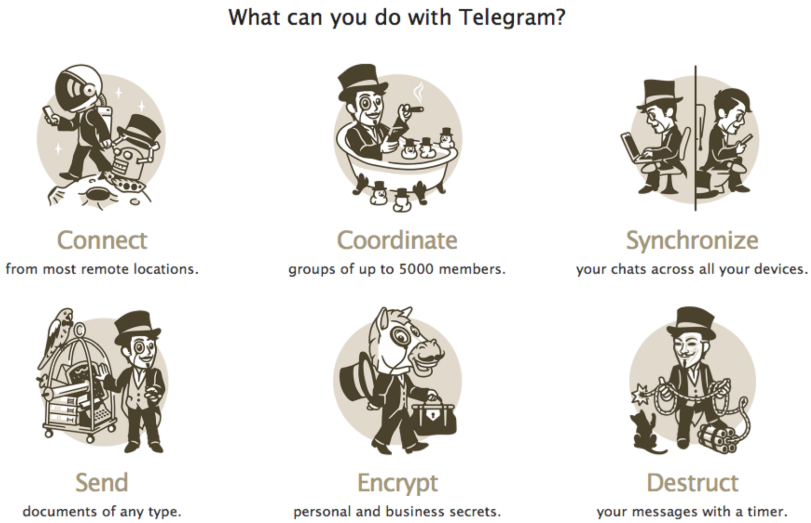


Figure 3 *- Telegram - Source : https://telegram.org*

Autant de fonctionnalités qui permettent à un adversaire non-étatique de disposer de moyens conséquents et sécurisés pour assurer la transmission et l'accès à des données en temps réel en ayant recours aux réseaux Internet civils « classiques ».

En d'autres termes, face à des acteurs qui communiquent de façon instantanée à l'aide d'outils grand public, il est indispensable de trouver le

moyen de faire jeu au moins égal avec des moyens compatibles avec les contraintes d'emploi des Armées.

Vers un concept du Cloud pour les Armées

Le Cloud computing est l'un des moyens les plus efficaces pour transmettre et partager de grandes quantités d'informations de manière quasi instantanée en gérant simultanément le temps réel ainsi que l'accès à des bases de données « historiques » particulièrement volumineuses.

Bien entendu, les capacités d'interconnexions des réseaux des Armées ainsi que la disponibilité d'un débit acceptable en continu constituent deux des principales conditions primordiales au fonctionnement en Cloud.

Dans ce contexte, chaque plateforme devient un « nœud » du réseau et peut ainsi potentiellement communiquer avec l'ensemble des autres « nœuds », qui sont à la fois émetteurs et récepteurs d'information. En bout de chaîne, les données recueillies par des capteurs doivent pouvoir être transmises et interprétées par tous les nœuds du réseau ayant le besoin et le droit d'en connaître, ce qui implique une gestion fine et différenciée des droits des utilisateurs.

Ce fonctionnement en réseau devient une réalité de plus en plus prégnante avec la numérisation accrue des véhicules et des équipements militaires. L'exemple du programme Scorpion qui vise à renouveler les blindés de l'Armée de Terre est particulièrement illustratif. Ainsi, selon Jean-Pascal Laporte, directeur de ce programme chez Thalès, *« [le véhicule multi-rôle Griffon et le véhicule de reconnaissance et de combat Griffon] sont de véritables engins connectés, qui échangent d'énormes flux de données »*[18].

[18] http://www.challenges.fr/challenges-soir/20160613.CHA0500/a-eurosatory-les-armees-se-convertissent-au-digital.html

L'avantage du fonctionnement en Cloud est de pouvoir optimiser la gestion de ces capacités en faisant en sorte de ne faire remonter ou redescendre que les informations essentielles à chaque niveau de décision. Par ailleurs, cela permet également au niveau tactique de recourir en cas de besoin à des données non stockées en local sur le théâtre des opérations.

Bien entendu, ces avantages ne doivent pas masquer les dangers potentiels induits par ce mode de fonctionnement – et notamment l'interruption possible de service ou l'interception potentielle de données – qui représentent un risque jugé la plupart du temps acceptable dans un cadre civil mais qui pourraient avoir des conséquences bien plus graves dans un contexte militaire.

Prendre en compte les contraintes spécifiques

Une approche peut consister à appréhender ces contraintes spécifiques des Armées en partant des fameux « critères de classification de l'information » ou critères « DCIP/T »[19].

Ces critères - notamment utilisés pour conduire des analyses de risques pesant sur les systèmes d'information - sont les suivants :

- **Disponibilité :** soit la faculté d'un système à fonctionner dans des conditions prédéterminées.
- **Confidentialité :** il s'agit ici de faire en sorte que les informations ne soient pas divulguées à des personnes non autorisées.
- **Intégrité :** c'est-à-dire la nécessaire préservation du message dans sa forme originelle, empêchant notamment les retraits ou ajouts d'informations non autorisés.

[19] https://fr.wikipedia.org/wiki/Sécurité_des_systèmes_d%27information

- **Traçabilité (ou Preuve) :** soit capacité de garder des traces des accès, des actions et des échanges réalisés de manière à être en mesure d'effectuer des opérations de contrôle.

Disponibilité

Cette question se pose dans un cadre civil, puisqu'il faut disposer en permanence d'une connexion réseau satisfaisante pour avoir accès aux informations stockées dans le Cloud. Or, pour diverses raisons – problèmes de connexion notamment - les réseaux tant publics que privés ne sont pas toujours accessibles.

La question de la disponibilité se pose avec une acuité particulière dans un contexte militaire. Plus précisément, le fonctionnement en Cloud suppose que les véhicules et autres objets communicants (comme les ordinateurs) et connectés (comme les capteurs) puissent correspondre en permanence avec les serveurs.

Or, sur des théâtres d'opération très étendus, comme cela a été le cas par exemple au Mali, il n'est pas forcément évident de maintenir un contact réseau avec des troupes réparties sur plus de 700 km.
Sur de telles distances, la rotondité de la terre empêche notamment la circulation des ondes et rend inopérant un certain nombre de systèmes. En d'autres termes, cela signifie qu'il faudra imaginer des solutions capables de prendre en compte cette contrainte.

Les récents progrès observés dans le domaine des technologies de communication pourraient dans une certaine mesure permettre d'y faire face. La radio logicielle Contact, développée par Thalès et qui est censée être 100 fois plus puissante que la génération précédente, est un exemple parmi d'autres. Des solutions pourraient également être trouvées par le déploiement de bulles 4G.

Cependant, aucune solution ne pouvant garantir de façon certaine une connexion réseau permanente, il sera également indispensable pour les Armées de réfléchir aux informations dont les troupes ne peuvent absolument pas se passer pour être opérationnelles – les cartes par exemples – et qui devront forcément être stockées en local. Cet inventaire devra être fait à tous les niveaux, aucun maillon de la chaîne ne devant être tributaire du bon fonctionnement du réseau pour pouvoir être opérationnel.

De même les forces devront être en mesure de fonctionner « en mode dégradé » - c'est-à-dire sans avoir recours aux données du Cloud, si pour une raison ou pour une autre – problème technique ou action ennemie – l'accès y était limité voire inexistant.

Ainsi, si l'on se dirige à grands pas vers le « combat collaboratif » qui permettra théoriquement par exemple de connaître le niveau de munition d'un véhicule allié – il ne faudra pas nécessairement partir du principe que ce mode de fonctionnement sera toujours possible.

Les difficultés de communication liées aux contraintes du théâtre d'opération, des problèmes techniques ou encore une attaque portant sur les infrastructures physiques ou les logiciels de partage de l'information sont autant d'aléas qui doivent conduire à s'interroger sur les réflexes à adopter en cas de retour à un mode de fonctionnement plus rustique.

En d'autres termes, les forces connectées – qui auront potentiellement accès à toutes les informations pertinentes issues de différentes sources et capteurs (images prises par des drones, informations en provenance d'autres unités, données sur l'état des véhicules / les munitions disponibles) - devront en cas de nécessité être capable d'opérer « hors ligne » et d'agir comme des forces « déconnectées ».

Au-delà de l'identification des informations essentielles devant être conservées en local aux différents niveaux de commandement – et donc qui ne devront pas être exclusivement stockées sur le Cloud – il faudra également se poser la question de la formation du personnel qui devra à la fois être capable de gérer les flux de données quand ils seront disponibles et de « faire sans » dès lors que pour une raison ou pour une autre le réseau ne sera plus opérationnel.

Si la question de la gestion de flux de données croissants peut en grande partie être résolue par la mise en place de logiciels intelligents capables de synthétiser la masse de données brutes en quelques indicateurs clés rapidement compréhensibles et exploitables, celle du « fonctionnement hors ligne » passera nécessairement par la préservation de compétences (navigation, évaluation de situation) et de savoir-faire (prise de décision en autonomie, initiative) pour les niveaux les plus proches du terrain.

L'une des conditions de la disponibilité des données est d'avoir l'assurance qu'elles transitent par des moyens sécurisés. En effet, le fonctionnement en Cloud repose sur la mise en place de serveurs – centralisés ou en local – qui communiqueront entre eux.

L'une des menaces les plus évidentes pesant sur les serveurs est l'attaque par déni de service qui vise à ralentir voire à empêcher totalement l'accès à un serveur ciblé pendant un certain laps temps en lui faisant parvenir un flux de requêtes instantanées dépassant ses capacités de traitement. Il ne faut cependant pas oublier l'existence d'autres risques : les réseaux de transmission peuvent en effet également être la cible d'attaques ou de brouillages.

Confidentialité

Si la garantie de la confidentialité des échanges devient de plus en plus un argument de vente de certaines sociétés grand public (Apple avec iMessage, WhatsApp, Facebook Messenger ou Viber par exemple) – sans qu'il soit d'ailleurs toujours véritablement possible d'en vérifier le caractère effectif – il s'agit d'un impératif non négociable pour les forces armées.

Or, le fonctionnement en Cloud générant par nature de très nombreux échanges d'informations entre différents niveaux de décision, la protection de ces données devient un enjeu majeur dans un contexte militaire.

En effet, si collecter et mettre en réseau toutes les données d'un théâtre d'opération est particulièrement utile pour assurer une gestion optimale des troupes, l'interception partielle ou totale de ces données par un tiers pourrait s'avérer particulièrement dommageable.

On imagine ainsi assez facilement de quelle manière un adversaire pourrait exploiter des informations sur la disposition exacte de véhicules blindés sur un théâtre et leurs niveaux de munitions à un instant donné.

Cela posera donc forcément la question du cryptage à utiliser et nécessitera de réfléchir à deux points en particulier :

- **Niveau du cryptage :** Au-delà de l'intégrité des « tuyaux » il faudra également crypter le contenu d'échanges dont l'interception pourrait avoir des conséquences dramatiques
- **Mise en œuvre du cryptage :** Il faudra s'assurer que les solutions retenues n'alourdissent pas outre mesure le message dans un contexte de réseaux contraints et demeurent suffisamment simple d'usage de manière à ne pas ralentir les échanges, ce qui reviendrait à faire disparaître les avantages initiaux du recours au fonctionnement en Cloud

En d'autres termes, il faudra parvenir à assurer une sécurisation maximale des données tout en n'entravant pas leur circulation fluide et leur partage instantané entre différents niveaux de commandement.

Intégrité

Les instructions transmises et les points de situations émanant des théâtres d'opération doivent bien entendu être maintenus dans leur forme originelle de manière à pouvoir assurer la bonne conduite des opérations.

Il s'agira donc de s'assurer tout d'abord que la conversion des données visant à faciliter leur transfert se fasse de manière à en préserver l'intégrité – sans toutefois retarder outre mesure les délais de transmission.

Il faudra par ailleurs aussi sécuriser les systèmes de manière à pouvoir éviter ou tout du moins à immédiatement détecter les attaques opérées par le biais d'armes informatiques sophistiquées comme par exemple les virus ou les chevaux de Troie.

De même le risque de compromission des données – de façon involontaire par un dysfonctionnement du système ou volontaire suite à une action ennemie – devra être pris en compte. Il va sans dire que l'effet de l'introduction de faux ordres dans le réseau par l'ennemi serait bien entendu potentiellement dévastateur.

Traçabilité / Preuve

Un autre aspect à prendre en compte est la traçabilité des transmissions de données. En d'autres termes, il faut s'assurer de la possibilité d'enregistrer les différentes opérations effectuées à tous les niveaux et à tout instant de manière à pouvoir procéder à des vérifications en cas de besoin.

C'est une condition indispensable à la conduite de RETEX après une opération ou pour s'assurer en temps et en heure que l'information a bien été transmise au niveau adéquat.

La préservation du contrôle de la gouvernance du système devra être étudiée en détail. Cela couvre différents aspects et notamment la nécessité de ne pas se retrouver prisonnier d'un choix technologique propriétaire. La dépendance vis-à-vis d'éventuels fournisseurs de solutions, voire des prestataires de services de maintenance par exemple, est une question dont l'économie ne pourra être faite.

Conclusion

L'usage du Cloud, on le voit bien, ne relève plus d'un futur possible pour les Armées mais d'une réalité présente. Comme bien souvent avec la transformation numérique, l'apparition des technologies précède le concept d'emploi : le rythme des évolutions est en effet tel et les bouleversements si soudains qu'il est difficile de les précéder en permanence.

L'augmentation des volumes de données mais aussi la multiplication des usages possibles imposent, pour garder une suprématie informationnelle et opérationnelle, de disposer au plus près du terrain de capacités de calcul et de stockage de plus en plus importantes. Le recours à des outils utilisant l'Intelligence Artificielle pour des usages aussi divers que le MCO, la conduite des opérations et la simulation par exemple, nécessite l'usage de masses de données (Big Data) qui ne peuvent être toutes délocalisées sur le terrain. Inversement, les forces en opération génèrent - et vont générer - de plus en plus d'information dont la remontée au plus tôt vers les échelons centraux sera également nécessaire. Le fonctionnement en Cloud semble à cet égard particulièrement adapté.

Néanmoins, les conditions d'emploi contraintes des Armées en opérations posent des problématiques particulières que peu d'acteurs du secteur civil sont amenés à rencontrer.

Aux critères DCIT/P s'ajoute l'usage de réseaux contraints et hétérogènes qui va poser des problèmes de débit comme de latence et d'encombrement. Autre aspect à ne pas négliger, la multiplication des terminaux comme celle

des centres de données répartis sur les différents échelons, pose la question énergétique : tous ces appareils consomment et doivent être souvent refroidis, sachant que la génération d'énergie en opération est un souci constant.

Si l'utilité de l'usage du Cloud pour la Défense semble donc acquise, il importe de se poser maintenant la question des contraintes capacitaires devant être prises en compte dans l'architecture des solutions à imaginer.

ceis

Société Anonyme au capital de 150 510 €
SIREN : 414 881 821 – APE : 7022 Z
Tour Montparnasse - 33, avenue du Maine - BP 36
75 755 Paris Cedex 15
Tél. +33 1 45 55 00 20 / Fax +33 1 45 55 00 60 / **contact@ceis.eu**

Publications récentes

A télécharger sur www.sia-lab.fr ou www.ceis.eu

Internet des Objets (IoT) - Nouvelle donne pour la Défense ? - Juin 2017

Enjeux stratégiques du Big Data pour la Défense - Juin 2017

Emploi du Cloud dans les Armées - Juin 2016

Impression 3D - Technologie de rupture au service des Armées – Juin 2016

Rattrapages technologiques et technologies de l'information - Déc.2015

Impact de la numérisation sur l'exercice du commandement – Déc. 2015

Les objets connectés et la Défense – Déc. 2015

Numérisation de l'outil de Défense - Juin 2015

Rythme des opérations et nouvelles technologies - Juin 2015

Le SIA Lab – Retour sur 2 ans d'activité – Juin 2015 (English version available)

Conditions d'utilisation des logiciels de l'OTAN par les Nations Alliées – Juin 2014 (English version available)

Mission des Armées et systèmes d'information - Déc. 2013

Le Système d'Information des Armées (SIA) - Déc. 2013

ceis