Maîtriser le *cloud computing* : enjeux géographiques, géopolitiques et géostratégiques

Clotilde Bômont[*], Université Panthéon-Sorbonne, UMR Prodig, Centre de Recherche des Ecoles de Saint-Cyr Coëtquidan

Le *cloud computing* - ou *cloud* -, traduit en français par « informatique en nuage », est l'une des innovations les plus récentes et les plus marquantes proposées pour répondre aux mutations continuelles du domaine numérique. Le *cloud* est un système de stockage, de mutualisation et de traitement des données numériques qui repose sur l'externalisation de la gestion des ressources informatiques ; on parle alors d'infogérance. Il existe principalement trois niveaux d'externalisation ; les modèles :

- IaaS (Infrastructure as Service) qui correspond à la mise à disposition par un prestataire de son infrastructure informatique ;
- PaaS (Plateform as Service) où en plus de l'infrastructure, un prestataire fournit à son client systèmes d'exploitation et logiciels de traitement de bases de données ;
- SaaS (Software as Service) où le prestataire gère l'ensemble du dispositif informatique, jusqu'aux applications.

Dans un contexte de complexification des systèmes d'information et de communication (SIC) et de prolifération des données, les avantages du *cloud* sont nombreux : facilité d'utilisation, facturation à l'usage, ressources en libre-service, élasticité des capacités informatiques, aisance du partage de données (Mell & Grance, 2011)… C'est pourquoi il connaît une popularité croissante et pourrait prochainement devenir un modèle prédominant dans l'organisation et la configuration des SIC. Maîtriser la technologie du *cloud computing* apparaît alors comme un impératif, tant pour allier performances et sécurité que, dans le cas des Etats, pour affirmer leur place dans les relations numériques internationales. Bien qu'il soit un objet technique, le *cloud* pose effectivement des enjeux géopolitiques et géostratégiques qui se rapportent aussi bien à la souveraineté, à la puissance étatique ou encore à la capacité informationnelle des forces armées qui réfléchissent à son intégration dans les opérations militaires.

[*] Doctorante en géographie à l'Université Panthéon-Sorbonne. Elle est rattachée à l'UMR Prodig. Elle est également chercheuse associée au Centre de Recherches des Ecoles Saint-Cyr Coëtquidan et allocataire de la DGRIS (Direction Générale des Relations Internationales et de la Stratégie).

Le travail autour de la maîtrise du *cloud* ne peut donc pas être exclusivement technique et doit s'ouvrir aux apports de disciplines des sciences humaines et sociales. Parce que le déploiement du *cloud* répond à des logiques territoriales et d'acteurs, une analyse géographique et géopolitique met ainsi en exergue nombre d'éléments conditionnant cette maîtrise.

Spatialiser le *cloud*

Aborder le *cloud* selon une perspective spatiale peut surprendre compte tenu de l'abstraction et de l'apparente immatérialité de l'informatique en nuage pour ses utilisateurs. Néanmoins, chercher à le définir en tant qu'espace et à le situer dans l'espace géographique aide à comprendre de son fonctionnement et contribue à sa conceptualisation.

Le cloud, nouvel espace de concentration dans le cyberespace

Dans l'imaginaire collectif, le *cloud* est souvent perçu comme un « ailleurs » numérique, un lieu lointain et abstrait aux contours flous. Cette description est proche de celle que l'on faisait du cyberespace il y a quelques années encore. Le terme de cyberespace désigne dans cette approche l'espace numérique dans son ensemble. Il est apparu en 1984, dans le roman de science-fiction *Neuromancer* de William Gibson (Gibson, 1984). Dystopie cyberpunk, l'œuvre de Gibson a changé la conception que nous avions d'Internet et du monde numérique, en l'envisageant à la fois comme un espace d'abstraction et un dispositif technique (Lohard, 2008). Cette vision qui conjugue espace et technologie est similaire à celle que nous avons aujourd'hui du *cloud*.

Parfois appelé « espace de stockage en ligne » ou « espace de traitement des données »[1], le *cloud computing* est défini par ses fonctions et son rapport aux données numériques. Il pourrait également être présenté comme un espace numérique à part entière au sein du cyberespace. Il en est effectivement partie intégrante et en est totalement dépendant. Il partage donc plusieurs caractéristiques et particularité du cyberespace (espace d'échange et de production de l'information, caractère ubiquitaire, relative intangibilité, réticularité…), véhicule des enjeux communs (fonctionnement systémique, difficulté d'encadrement juridique, transfrontalité…) et soulève des débats identiques (risques sécuritaires, qualification en tant qu'espace géographique…). Si le *cloud* s'inscrit dans le cyberespace, il en modifie aussi l'architecture.

L'importante ramification et l'efficacité des réseaux cybernétiques[2] autorise une grande rapidité dans les échanges numériques. La vitesse de circulation des données sur ces réseaux relativise les distances entre les appareils, entre les individus et entre les appareils et les individus. Leur proximité géographique n'est alors plus un impératif.

[1] Termes récurrents dans les présentations « marketing » du *cloud*.
[2] Internet est le principal réseau cybernétique mondial, mais il en existe d'autres ; on parle alors d'intranets.

En s'appuyant sur l'hyperconnectivité croissante, la technologie du *cloud computing* repose précisément sur cette possibilité d'éloignement. La gestion à distance des dispositifs informatiques a alors deux conséquences. La première est la dissémination de par le monde des utilisateurs d'un même *cloud*. C'est là l'un des principaux attraits du *cloud computing* qui permet d'accéder à des données et de les traiter depuis n'importe quel point du globe, à condition d'être connecté à un réseau. Il participe ainsi à l'extension des SIC et est donc potentiellement transnational.

La seconde conséquence est la concentration en un même lieu des ressources informatiques et numériques. L'externalisation de la gestion des dispositifs matériels et logiciels a entraîné la délocalisation des infrastructures qui ne sont alors plus situées dans les locaux de l'entreprise ou l'organisation clientes ou chez l'utilisateur particulier. Dans le même temps, dans un souci de rentabilité et d'efficience, les infrastructures sont rassemblées par les prestataires au sein de *datacenters*[3]. Le *cloud* provoque également la concentration des applicatifs. Le développement des architectures web au milieu des années 1990 a conduit à la centralisation de outils de traitement sur des serveurs extérieurs et non plus sur les terminaux (Plouin, 2011). Le *cloud computing* accentue cette tendance et poursuit la centralisation des applications qui sont hébergées sur les infrastructures susmentionnées. Le *cloud*, enfin, concentre les données. En rassemblant les infrastructures et les applicatifs, il devient naturellement un lieu virtuel de convergence. De plus en plus utilisé pour ses importantes capacités de stockage, de mutualisation et de traitement, il polarise une part croissante des données numériques mondiales.

Les infrastructures du cloud et leur environnement

Spatialiser le *cloud*, c'est aussi déterminer l'emplacement des *datacenters*, dispositifs *back-end* et infrastructures maîtresses du *cloud*. Ces infrastructures réseau s'ancrent dans un environnement physique dont elles dépendent et, en plus de devenir une composante de l'espace géographique, ont des conséquences sur son aménagement. Elles sont donc soumises à plusieurs contraintes de localisation.

Contingences humaines, matérielles et économiques

Outre la prise en compte évidente de variables topographiques, le choix d'un site pour la construction d'un *datacenter* répond à des considérations sociales, économiques, matérielles et même politiques. L'accès à une main-d'œuvre spécialisée est par exemple indispensable.

[3] Les *datacenters* sont également appelés « fermes de données », « centres de traitement de données », « entrepôt de données », « centres de flux de données » … Ces dénominations sont approximatives quant à la fonction de ces établissements, aussi emploierons-nous principalement l'anglicisme « datacenters », admis en français.

L'entretien d'un établissement de ce type requiert des informaticiens, des ingénieurs et des techniciens de réseau, mais aussi des électriciens et des plombiers. Cela empêche l'implantation d'un centre dans un territoire désert. La liaison avec les équipementiers doit également être prise en compte puisque l'acheminement du matériel doit être facile et rapide. Seules les zones bien desservies par des réseaux de transport peuvent donc être envisagées. La possibilité de réutilisation de friches industrielles, les disponibilités foncières (Bakis, 2013) et la fiscalité en vigueur sont d'autres critères d'installation pour un prestataire qui suit prioritairement des logiques économiques. Ainsi, la présence d'une quinzaine de *datacenters* dans les environs de Dublin s'explique en partie par la fiscalité irlandaise, particulièrement favorable (Desmedt, 2012). Certains territoires mettent alors en place des politiques incitatives afin d'attirer des acteurs du numérique et du *cloud*, et des aides substantielles sont parfois allouées aux entreprises.

Hyperconnectivité

Le *cloud* fonctionnant sur l'accès à distance des ressources informatiques, un *datacenter* doit bénéficier d'une excellente connexion à Internet[4]. Il doit être relié à un réseau en fibre optique qui offre un débit important et une possibilité d'accès à plusieurs opérateurs de télécommunication (*ibid.*). Il s'agit d'une contrainte technique incontournable obligeant les hébergeurs à implanter leurs *datacenters* à proximité des dorsales Internet. Les infrastructures du *cloud* sont ainsi généralement situées non loin des métropoles, mieux connectées que le reste du territoire.

De grands énergivores

Un *datacenter* de 10 000m² consomme en moyenne autant d'énergie qu'une ville de 50 000 habitants, et les plus grands centres ont une consommation d'électricité équivalente à celle de 250 000 foyers européens[5] (Bakis, 2013). D'après une étude de Greenpeace parue en 2012, la demande globale en énergie des *datacenters* a augmenté de 56% entre 2005 et 2010 ; cela placerait le *cloud*, s'il avait été un pays, en cinquième position des Etats les plus énergivores (Greenpeace, 2012). Les prestataires doivent donc assurer une alimentation en électricité des infrastructures conséquente, de qualité et continue au risque, le cas échéant, de provoquer une panne totale des dispositifs, voire leur dégradation. Les clients ne pourraient alors plus accéder à leurs données qui risqueraient même d'être définitivement perdues. La proximité d'une source d'approvisionnement en énergie est donc un autre facteur déterminant pour l'installation d'un *datacenter*.

[4] Il peut s'agir d'un réseau intranet dans le cas d'un *cloud* privé, mais ce cas de figure est rare.
[5] A l'échelle mondiale, la taille moyenne d'un *datacenter* est d'un peu moins de 30 000m². Le plus gros *datacenter* au monde si situe à Langfang, en Chine, et couvre une superficie d'environ 2 000km².

Google a par exemple décidé en 2006 d'implanter un centre dans la ville de The Dalles, dans l'Oregon aux Etats-Unis, et d'ainsi profiter des infrastructures hydro-électriques installées sur la rivière Columbia. Le site de The Dalles est par ailleurs très bien desservi par la fibre optique, sous-exploitée suite au krach d'une bulle spéculative qui a touché le secteur des TIC au début des années 2000. Les bords du fleuve Saint-Laurent, au Canada, sont eux aussi devenus le lieu d'implantation des *datacenters* d'OVH et d'Ericsson du fait de la présence d'une centrale hydro-électrique.

Si l'énergie permet de faire fonctionner les infrastructures, elle sert également au refroidissement des machines qui produisent de la chaleur lorsqu'elles sont actives. La température à l'intérieur d'un *datacenter* ne devant pas dépasser 25°C, ce sont près de 40% de l'énergie consommée qui sont destinés à sa climatisation (Song, Zhang & Eriksson, 2015). Cette consommation peut néanmoins être réduite dans les régions froides grâce au *free cooling*, qui consiste à refroidir les locaux en utilisant l'air extérieur ou en recourant à un système par circulation d'eau froide. Le climat peut donc également jouer sur l'emplacement d'un *datacenter*. Le centre de Bahnhof construit dans un ancien bunker nucléaire de la Guerre Froide sous Stockholm et ceux de Google en Finlande, à proximité des eaux froides de la mer Baltique, en sont de bonnes illustrations.

Eco-responsabilité dans le cloud

Du fait de son importante consommation énergétique, l'utilisation du *cloud* n'est pas sans conséquences environnementales. Les *datacenters* sont responsables de 27% des émissions carbones générées par le numérique (ADEME[6], 2017). De plus, la concentration des infrastructures entraîne une augmentation localisée de la demande en énergie, ce qui complique l'utilisation d'énergies propres. Les énergies fossiles sont particulièrement sollicitées dans les pays en développement à croissance économique rapide où le secteur des NTIC est en plein essor.

Toutefois, le concept d'informatique durable – ou *green-IT* -, apparu dans les années 1990, est de plus en plus récurrent. Il est aujourd'hui question d'un *cloud* « éco-responsable » (Flipo & al., 2009 ; Ullmann & al., 2008) qui se base sur l'efficacité énergétique des *datacenters*, mesurée par le PUE (Power Usage Effectiveness)[7], et sur l'usage d'énergies renouvelables. Si la « propreté » d'un *cloud* est parfois un argument de vente, ce sont en premier lieu pour des raisons économiques que les hébergeurs s'y intéressent.

[6] ADEME : agence de l'environnement et de la maîtrise de l'énergie.

[7] Le PUE (Power Usage Effectiveness) est un indicateur qui montre le ratio entre l'énergie totale consommée par l'établissement et celle consommée par les systèmes informatiques. Il manque cependant de fiabilité (il est possible de faire mentir l'indice en augmentant la consommation des systèmes informatiques) et est incomplet (il ne prend pas en compte, par exemple, la réutilisation des calories produites). Le DCEM (Data Center Energy Management) a été proposé par le CRIP (Club des Responsables d'Informatique et de Production) en 2014 pour remplacer le PUE (Fléchaux, 2014).

Le poids des multinationales du numérique dans les relations internationales est tel que leur volonté de réduire leur consommation et leur souci de recourir à des énergies propres et/ou renouvelables pourraient influencer les gouvernements et orienter leur politique énergétique.
Le critère environnemental est encore bas dans la liste des facteurs de localisation des *datacenters*, mais l'imminente pénurie d'énergies fossiles et leur coût pourraient, dans un avenir tout proche, en faire un aspect à ne pas négliger.

Le tableau suivant dresse une typologie récapitulative des critères de localisation d'un *datacenter*.

Critères d'implantation d'un datacenter

BESOINS		**FACTEURS DETERMINANTS**	**SOLUTIONS**
Energie	Fonctionnement	Approvisionnement énergétique	Proximité de sources d'approvisionnement (hydraulique, éolienne, nucléaire…)
	Refroidissement	Approvisionnement énergétique, *free cooling*	Proximité de sources d'approvisionnement, zones ou pays froids
Connectivité		Points de raccordement à la dorsale, présence de nombreux opérateurs	Métropoles
Contingences économiques		Attractivité économique du pays	Fiscalité favorable, aides gouvernementales, coût de l'énergie, énergies propres…
Contingences humaines et matérielles		Main d'œuvre qualifiée, réseau de transports performant, disponibilité foncière…	Périphérie des centres urbains

Bômont Clotilde, mai 2017

Opacité et complexité de la circulation des données dans le cloud

Le *cloud* peut être pensé tel un réseau dont les axes seraient constitués par les flux de données échangées entre utilisateurs et dispositifs. Spatialiser un *cloud*, c'est donc aussi modéliser l'itinéraire des données présentes sur ce *cloud*. Cependant, cela s'avère souvent compliqué. La logique de circulation des données dépend du réseau sur lequel un *cloud* est construit. Dans le cas d'Internet où les ramifications sont très nombreuses, le découpage de l'information en paquets IP[8] et leur routage vers les embranchements les moins chargés du réseau mondial rendent les itinéraires des données aléatoires et donc imprévisibles.

Les flux de données se caractérisent également par leur provenance et leur destination. Toutefois, là encore, il n'est pas évident de déterminer les points d'émission et de convergence des données dans un *cloud*. Si l'adresse IP du terminal d'un utilisateur permet de le localiser plus ou moins précisément sur le globe, beaucoup d'appareils ont une IP dynamique, c'est-à-dire changeante. Cela empêche une modélisation définitive. Le *cloud* étant voulu ubiquitaire, il faut également compter avec la mobilité des utilisateurs. Il est aussi vanté comme un outil de mutualisation et de partage de ressources, ce qui signifie que les données ne reviennent pas systématiquement vers leur émetteur et qu'elles peuvent être envoyées vers plusieurs appareils. Par ailleurs, le principe de proximité n'ayant plus cours, le lieu d'émission ou de réception des données ne permet pas nécessairement d'identifier l'infrastructure vers laquelle elles convergent. La standardisation des dispositifs informatiques au sein des *datacenters* permet en outre le transfert des données d'un centre à l'autre. Ces transferts répondent généralement à des contraintes techniques (équilibrage des requêtes en fonction des capacités), à des facteurs économiques (prix des dispositifs) et, nous le verrons, à des impératifs légaux. La complexe circulation des données présentes dans un *cloud* ne s'explique donc pas uniquement par des facteurs géographiques. Leur itinéraire soulève néanmoins des enjeux géopolitiques et certains acteurs cherchent à l'encadrer.

Contrôler le *cloud* : un facteur de puissance transnational

L'approche géographique révèle certains mécanismes du *cloud* (concentration, infogérance, opacité des lieux d'hébergement des données…) qui, envisagés selon une perspective géopolitique, expliquent les motivations de certains acteurs qui cherchent à maîtriser cet outil numérique.

[8] En s'appuyant sur les travaux de Leonard Kleinrock, l'ingénieur français Louis Pouzin développe les datagrammes. Un datagramme est un paquet de données dans un réseau informatique. Dans un système de commutation par paquets, les messages sont constitués de plusieurs datagrammes distincts, acheminés séparément et réagencés ensuite au niveau du destinataire. Aujourd'hui, à chaque datagramme est attribuée une adresse IP permettant de l'orienter vers son appareil de destination.

Accessibilité des données dans le cloud

Après les débuts d'Internet marqués par des stratégies de contrôle des infrastructures cyber (câbles, instances de normalisation…) puis de gestion des plateformes de consultation et d'échange, la maîtrise des données constitue aujourd'hui un enjeu majeur (Chartron et Broudoux, 2015, p.2). Les données numériques sont des descriptions codées d'informations relatives à un contexte (Kitchin, 2014). Leur accessibilité est donc disputée. Celle-ci renvoie aux acteurs impliqués dans le déploiement du *cloud* et à ceux qui en ont *in fine* le contrôle.

Infogérance et contrôle des données

En recourant à l'infogérance, un client[9] accepte de confier ses données à un prestataire. Leur accès est alors régulé par des contrats de confidentialité[10]. Cependant, plus la gestion des ressources est externalisée, plus un *cloud* peut compter d'intermédiaires spécialisés ; or, les accords passés entre un prestataire et son client n'entraînent pas nécessairement d'obligation entre le prestataire et un éventuel sous-traitant (Bensamoun & Zolynski, 2015). Un utilisateur peut donc perdre son droit de regard sur le devenir de ses données.

Si la décentralisation souhaitée initialement dans l'élaboration du réseau Internet permet sa résilience, elle prévient également toute prise de contrôle. Le fonctionnement centralisé du *cloud* et la concentration des ressources qu'il occasionne amènent à s'interroger sur l'emprise des fournisseurs sur les dispositifs externalisés et donc sur les données dont ils organisent le stockage et le traitement, mais aussi l'édition et le retrait. L'opacité des logiques sous-jacentes à la localisation des données contribue également à la marginalisation de l'usager quant au devenir de ses données (De Filippi & McCarthy, 2012).

Acteurs du cloud

Francis Hintermann, directeur d'Accenture Research, propose de distinguer les acteurs intervenant dans la chaîne d'approvisionnement d'un *cloud* selon cinq catégories : les éditeurs de logiciels et progiciels (Microsoft, SAP, Oracle…), les entreprises de service numérique ou ESN (IBM, HP, les français Atos et Capgemini…), les équipementiers et constructeurs de matériel (Cisco, Intel, Apple…), les opérateurs de télécommunication (AT&T, Orange…) et les « acteurs du Web » (Amazon, Google…) (Hintermann, 2010).

[9] Les utilisateurs du *cloud computing* peuvent être des particuliers, des entreprises ou des organisations diverses. Dans le cadre d'un usage privé, les données envoyées sur le *cloud* le sont par décision du sujet auxquelles elles se rapportent. En revanche, dans le cas d'une entreprise ou d'une organisation, les données sont celles de leurs clients qui ne sont pas toujours informés de ce transfert.

[10] La rigueur apportée à la confidentialité des données est variable selon les services et les fournisseurs ; un utilisateur doit donc y être vigilant, par exemple lorsqu'il souscrit à des conditions d'utilisation sur un réseau social.

Malgré des domaines de prédilection très différents, plusieurs de ces acteurs parviennent à proposer une offre de *cloud* ; ils sont donc souvent en concurrence les uns avec les autres.

Les études de marché distinguent traditionnellement les fournisseurs de service IaaS et PaaS des fournisseurs de service SaaS. Selon Synergy Research Group[11], le *cloud* d'infrastructure (IaaS et PaaS) est largement dominé par Amazon[12] qui détient à lui seul 33% des parts de marché au premier trimestre 2017. Ses plus gros concurrents sont Microsoft, IBM et Google, suivis par Alibaba et Oracle. Toutefois, l'ensemble de leurs revenus cumulés en 2017 n'équivaut pas celui d'Amazon (Synergy Research group, 2017a). Le taux de croissance annuel des activités *cloud* de Microsoft, Google et Alibaba de plus de 80% est néanmoins bien supérieur à celui du leader qui n'est « que » de 43% au troisième trimestre 2017 (Synergy Research Group, 2017b). Les entreprises Salesforce et Rackspace figurent aussi au classement des plus gros prestataires du *cloud computing*. Leur part de marché et leur croissance sont bien en-deçà de celles des meneurs, mais ils occupent une place de choix dans les marchés de niche. Parmi les entreprises de SaaS, Microsoft arrive en tête du classement, suivi par Salesforce et Box en seconde et troisième positions, puis par Amazon et Google en quatrième et cinquième positions (Okta, 2017).

Attractivité des Etats-Unis et oligopoles

A l'exception du chinois Alibaba, toutes les entreprises mentionnées ci-dessus sont américaines. IaaS, PaaS et SaaS confondus, les Etats-Unis dominent donc le *cloud*. Leur position de première cyberpuissance mondiale (Nye, 2010) n'y est pas étrangère. En tant que berceau du projet ARPANET[13], le territoire américain est devenu une plaque tournante pour Internet. Les infrastructures à la base du réseau ont été construites sur le sol étatsunien et y sont encore majoritairement situées. La présence de ces infrastructures explique que le territoire américain capte une grande part de flux numériques mondiaux (Morel, 2017).

Les nombreux clients des multinationales américaines leur fournissent de grandes quantités de données dont la réutilisation (publicité, profilage, *big data*…) génère d'importants revenus. S'ensuit un cercle vertueux : plus ces entreprises ont de données, plus elles sont puissantes, et plus elles sont puissantes, plus elles peuvent développer des services attractifs ; elles attirent ainsi les utilisateurs et donc de nouvelles données. La concentration des données dans le *cloud* se fait donc au profit des acteurs américains.

[11] Le groupe Synergy Research est un cabinet d'étude américain spécialisé dans les télécoms. Il est l'un des seuls à produire des analyses trimestrielles sur le *cloud computing* et est de ce fait une source fréquemment citée dans ce domaine (aux côtés de Gartner).

[12] Au travers d'AWS : Amazon Web Service.

[13] Considéré comme l'ancêtre d'Internet, le projet ARPANET est le premier réseau informatique à utiliser la transmission par paquets sur de longues distances. Il est né en réponse à un intérêt scientifique pour améliorer la communication, notamment entre centres de recherche.

Leurs performances techniques, capacitaires et d'innovation expliquent qu'ils sous-traitent en plus certains pans d'activité d'autres prestataires (DropBox ou Netflix ont par exemple recours aux services proposés par Amazon). Ils sont donc difficilement contournables et interviennent presqu'inéluctablement dans la chaîne d'approvisionnement d'un *cloud*.

Juridiction et accès aux données

Certains Etats ont introduit des lois permettant d'outrepasser le droit au respect de la vie privée dans le cas où la sécurité nationale ou l'ordre public seraient menacés (France, Russie, Royaume-Uni, Etats-Unis…). Dans ces circonstances exceptionnelles, les prestataires de services *cloud* sont contraints de fournir des données confidentielles aux gouvernements dont ils dépendent. L'usage veut que les données soient soumises à la loi en vigueur sur le territoire où elles se trouvent (De Filippi & McCarthy, 2012). Un Etat peut ainsi accéder aux données hébergées par des infrastructures situées sur son sol. Les données présentes sur le *cloud* n'échappent pas à la centralité technologique[14] des Etats-Unis et la plupart transitent au moins temporairement par le sol américain ; elles relèvent alors de la juridiction étatsunienne.

La localisation géographique des infrastructures n'est cependant pas la seule variable pertinente pour déterminer la législation en vigueur. En effet, est également réputée relever de la législation américaine toute entreprise basée aux Etats-Unis ou y ayant une filiale (Maxwell & Wolf, 2012). Les principaux fournisseurs de services *cloud* répondent donc au droit américain. Ce dernier prévoit diverses mesures facilitant la consultation de données personnelles par les agences de renseignements étatsuniennes. Le *Patriot Act* est la plus emblématique et la plus souvent pointée du doigt. Voté en 2001 à la suite des attentats du 11 septembre, il contraint les entreprises à remettre aux autorités, sur simple demande, toutes données qu'elles jugent utiles. Soumises au secret, les entreprises n'ont pas le droit de signaler à leurs clients cette atteinte à la confidentialité. Peu importe où il opère dans le monde, dès lors qu'il répond au droit américain, un fournisseur de *cloud* est obligé de se conformer à ces requêtes (Van Hoboken & al., 2012). Le *Patriot Act* n'est toutefois qu'une extension de procédures préexistantes et s'inscrit dans une législation qui comprend beaucoup d'autres normes de cette nature (*ibid.*).

Le respect de la confidentialité des données ne dépend donc pas uniquement de la convention passée entre prestataire et utilisateur, mais il est aussi déterminé par le maillon de la chaîne le plus exposé à une juridiction indiscrète. L'itinéraire parcouru par les données a donc des conséquences sur leur accessibilité.

[14] Selon Laurent Bloch, la centralité d'un pays, évaluée sur une échelle de 0 à 1, correspond « à « la probabilité que l'itinéraire d'un paquet de données entre deux points quelconques de l'Internet passe par ce pays » (Bloch, 2015).

Un enjeu de souveraineté et de puissance

Les frontières des juridictions étatiques sont difficiles à définir dans le monde numérique, et particulièrement dans le *cloud*. Or, l'accès aux données pose des enjeux de souveraineté et devient aujourd'hui un facteur de puissance.

Quand maillage administratif et maillage numérique ne coïncident pas

En entraînant la délocalisation des dispositifs informatiques, l'infogérance contribue au déploiement transnational des SI. Le maillage numérique ainsi créé se différencie parfois du maillage administratif. Dans ce cas, parce qu'elles sont situées sur le territoire d'un autre Etat ou parce qu'elles sont gérées par des fournisseurs étrangers, les données d'un utilisateur peuvent dépendre d'une souveraineté différente que l'utilisateur lui-même. Elles sont alors soumises à une législation étrangère et sont potentiellement accessibles par un gouvernement étranger.

L'accès d'un gouvernement à des données qui ne sont pas directement relatives à ses citoyens est problématique : outre l'atteinte à la vie privée des individus, cela autorise l'application d'une juridiction hors du territoire national ou sur des ressources qui ne lui appartiennent pas. Cela constitue une atteinte à la souveraineté de l'Etat dont le *ratione loci* et l'autorité ne sont pas respectés. A l'inverse, l'extension des compétences d'un gouvernement au-delà de ses frontières étatiques lui confère une autorité extraterritoriale. C'est le cas des Etats-Unis qui bénéficient du fonctionnement systémique et réticulaire du *cloud*.

Puissance data-numérique

Les données sont aujourd'hui utilisées dans tous les secteurs d'activité et sont indispensables au développement de nouvelles technologies clefs dans les futures relations internationales. L'intelligence artificielle, par exemple, repose entièrement sur le traitement de données et fait déjà l'objet d'une course au développement entre plusieurs Etats (Chine, Etats-Unis) (Nocetti, 2017). En plus de garantir la souveraineté d'un Etat et une certaine indépendance numérique, le contrôle des données est donc un facteur de puissance.

Olivier Kempf et Thierry Berthier avancent le concept de puissance data-numérique qu'ils évaluent selon cinq critères : les « data-infrastructures », les capacités de traitement des données, l'attractivité vis-à-vis des principaux acteurs de données, le degré de formation en sciences de la donnée, et la capacité d'un Etat à « prioriser » sa politique numérique (Berthier & Kempf, 2016). A partir de ce modèle, une autre grille de lecture de la puissance data-numérique d'une nation peut être envisagée. Elle reprendrait certains des critères énoncés mais les réorganiserait et y ajouterait quelques dimensions.

Elle comprendrait ainsi :

- Le nombre de dispositifs de gestion de données en fonction d'un territoire et d'une population et la capacité des dispositifs.

Par dispositifs sont entendus les infrastructures et les applicatifs permettant le stockage et le traitement de données. Leur nombre et leur puissance sont analysés relativement à la population de l'Etat évalué. Leur activité annuelle en volume de données traitées et leurs performances énergétiques peuvent également être prises en compte dans l'évaluation.

- Les acteurs économiques.

L'implantation de grandes multinationales du numérique[15] sur le territoire d'un Etat et leur implication avec les acteurs nationaux du même secteur sont un indice de puissance data-numérique. L'importance du nombre et du rayonnement des entreprises nationales doit également être considérée, d'autant qu'elles sont un moyen de limiter la dépendance à des infrastructures ou des applicatifs étrangers.

- Le niveau de formation et de recherche en sciences de la donnée.

Ce critère renvoie à la capacité d'innovation et de maîtrise d'un Etat dans les technologies relatives aux données. Il s'attarde sur le nombre de laboratoires, de publications, de « *clusters* de R&D et de chaires universitaires de recherche » (*ibid.*) travaillant sur ce domaine, ainsi que sur la reconnaissance internationale de la qualité des recherches et de la formation.

- L'existence d'une politique numérique.

L'existence même d'une politique numérique est signe d'une conscience et d'un éveil aux nouveaux enjeux soulevés par les données numériques. Une telle politique permet l'encadrement des usages et l'instauration, à terme, d'une capacité de gestion des données nationales.

- La maîtrise du *cloud computing*.

La vitesse d'expansion du *cloud computing* est telle que son usage systématique est à prévoir dans un futur imminent (Anderson & Rainie, 2010). Si la tendance actuelle se poursuit, la majorité des données mondiales seront concentrées dans le *cloud*. De plus, il est un préalable à beaucoup d'autres innovations qui reposent justement sur le traitement des données (*Big data*, *IoT*, *machine learning*…). La maîtrise et le contrôle de cet outil deviennent alors des facteurs de puissance à part entière.

[15] Parmi lesquelles, les GAFA(M). L'acronyme GAFA désigne les entreprises Google, Apple, Facebook et Amazon auxquelles on ajoute parfois Microsoft. Ces firmes aux chiffres d'affaires colossaux manipulent une très grande partie des données en circulation sur le réseau Internet.

La loi européenne au secours de la protection des données

Les Etats-Unis sont la première puissance data-numérique mondiale et leur prédominance sur le *cloud computing* renforce cette position. Leur suprématie est cependant contestée. Les révélations d'Edward Snowden au début des années 2010 ont mis en évidence les pratiques des services de renseignement américains et ont révélé l'étendue des programmes PRISM[16] et *Muscular*[17]. Elles ont ainsi permis de constater le mépris du Traité d'assistance judiciaire mutuelle[18] signé en 2003 avec l'Union Européenne et ont conduit à l'invalidation par la Cour de Justice Européenne des accords du *Safe Harbor*[19], le 6 octobre 2015.Un nouvel accord a été signé entre les Etats-Unis et la Commission Européenne en juillet 2016 - le *Privacy Shield* -, mais a été jugé encore insuffisant pour garantir la protection des données européennes face à l'hégémonie américaine.

Ces déceptions, conjuguées à l'évolution rapide des NTIC, ont amené l'Union Européenne à abroger sa Directive sur la protection des données personnelles de 1995 (95/46/CE) et à la remplacer par le Règlement général sur la protection des données (2016/679) (RGPD) qui entrera en vigueur le 25 mai 2018. Le règlement 2016/679 est impératif et vise une harmonisation des législations nationales. Il insiste sur un traitement « licite, loyal et transparent » des données personnelles (UE, 2016) et prévoit de nouvelles mesures pour garantir le droit au respect de la vie privée. Les implications du RGPD concernent particulièrement le *cloud*. En effet, contrairement à la Directive 95/46, il étend les obligations à l'ensemble des acteurs de la chaîne de traitement de données, y compris aux sous-traitants. Il s'applique dès lors qu'un prestataire conduit des activités sur le territoire de l'UE ou qu'il gère des données émanant d'un citoyen européen, quel que soit le lieu de collecte de ces données. Le règlement aborde également, au chapitre V, la protection des données lors de transferts hors de l'Union, et l'article 7 du règlement affirme que le consentement des personnes au traitement de leurs données ne peut plus être présumé mais doit être clairement signifié.

[16] Le programme de surveillance PRISM lancé par les Etats-Unis en 2007 prévoit une collecte massive et systématique de données grâce à un partenariat plus ou moins contraint sur la base du *Patriot Act* avec de grosses entreprises américaines (dont Google, Microsoft, Facebook, Apple, Skype, AOL, Yahoo !, Youtube, Paltalk…).

[17] Le programme Muscular est un passage en force qui permet au gouvernement américain d'accéder aux données qui échappent au *Patriot Act* par interception des flux de données entre deux *datacenters*, sur le modèle des écoutes téléphoniques.

[18] Le Traité d'assistance judiciaire mutuelle passé entre les Etats-Unis et l'Union Européenne stipule notamment les termes régissant les échanges d'informations et de données personnelles dans un cadre de coopération policière et judiciaire ; il impose un accord des parties.

[19] Le *Safe Harbor* est un traité transatlantique sur le transfert des données personnelles ratifié par des entreprises américaines qui s'engagent à protéger les données personnelles européennes. Il a cependant été prouvé qu'en dépit du traité, ces entreprises n'étaient pas en mesure de sécuriser les données des citoyens européens qui sont « exploitées en toute illégalité » (Extrait de l'exposé de l'amendement n°CL129 (adopté début 2016) de la loi « pour une République numérique » publiée au journal officiel le 8 octobre 2016).

Volonté d'émancipation des acteurs américains

La position dominante des Etats-Unis est en grande partie due à leurs acteurs économiques. Cependant, leur cadre juridique entrave les activités des entreprises. La confiance des utilisateurs, entamée par la surveillance massive des autorités américaines, est cruciale pour ces multinationales qui font des données personnelles leur fonds de commerce. Pour prouver leur fiabilité, elles veulent donc en préserver la confidentialité ; c'est ainsi qu'en 2013 et 2015, des affaires judiciaires ont opposé les autorités étatsuniennes et les sociétés Microsoft et Apple qui refusaient de communiquer les données de leurs clients (Cattaruzza & al., 2014). Si dans les deux cas les tribunaux ont statué en faveur des entreprises, les firmes américaines cherchent quand même à s'affranchir des contraignantes mesures légales des Etats-Unis. Dans le cas de l'UE dont le marché représente une part importante de leur chiffre d'affaires, elles s'abritent derrière les réglementations européennes. Le RGPD replaçant le territoire au cœur des questions juridiques, elles ouvrent des filiales dans les pays membres et construisent des centres de données directement sur le sol européen. Aussi, en cherchant à se dissocier des autorités américaines, les prestataires opèrent une forme de distanciation physique avec les Etats-Unis et contribuent finalement à la régionalisation du *cloud*.

Territorialisation du cloud : cloud souverain ou cloud interétatique ?

La régionalisation du *cloud* est liée à la volonté des Etats de retrouver la maîtrise de leurs données en les relocalisant dans un espace souverain, tangible ou non. Cela suppose le développement d'un *cloud* contenu dans des limites administratives connues.

Un cloud français et souverain

Dès la fin des années 2000, l'Etat français comprend qu'il doit avoir davantage de contrôle sur le devenir de ses données. Dans ce but, le gouvernement Fillon propose en 2009 le développement d'un *cloud* français souverain qui recourrait à des prestataires exclusivement nationaux et dont l'ensemble des dispositifs seraient situés sur le territoire national. C'est ainsi qu'en mai 2011, les entreprises Thalès, Dassault systèmes et Orange s'associent et lancent le projet Andromède dans lequel l'Etat se dit prêt à investir 150 millions d'euros. Des mésententes au sein du consortium en charge du projet ont provoqué sa scission en deux initiatives distinctes, Cloudwatt et Numergy, qui se sont finalement soldées par des échecs. Les difficultés de la mise en place du *cloud* souverain s'expliquent certes par la compétitivité des entreprises américaines, performantes et économiquement attractives, mais également par le manque de considération de la part de l'Etat français pour sa base industrielle déjà existante (OVH, Gandi, Ikoula…) (Danet, 2014).

Cela aura toutefois permis la définition de normes de sécurité et la création de labels délivrés par l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information). L'attribution du référentiel « SecNumCloud » au niveau « avancé » garantit par exemple qu'un prestataire remplit les conditions de la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) et permet au *cloud* qu'il propose d'obtenir la qualification de *cloud* souverain. Le difficile cantonnement du *cloud* dans des frontières étatiques ont par ailleurs poussé la France et l'Allemagne à développer des certifications communes. Cette harmonisation va dans le sens du marché unique du numérique en Europe et pourrait être perçue comme les prémices d'un *cloud* européen.

Vers un cloud européen ?

Les discours favorables à un *cloud* européen sont portés en premier lieu par les industriels qui regrettent la balkanisation du marché intérieur du numérique en Europe (*L'informaticien*, 2017). Selon eux, les logiques nationales empêchent la montée en puissance des acteurs économiques européens qui peinent alors à rivaliser avec les géants américains. Elles nuiraient donc à la fois aux prestataires et aux utilisateurs européens confrontés à un choix restreint d'offres de *cloud*.
Cette position est partagée, en second lieu, par les institutions européennes. Dans sa communication du 27 septembre 2012 au Parlement européen, la Commission Européenne a exprimé sa volonté de développer un *cloud* régional et a défini les possibilités de la mise en place d'une stratégie commune aux Etats membres (Commission européenne, 2012). Elle y souligne notamment le potentiel économique du secteur du *cloud* qui, selon une étude préliminaire, permettrait de générer 250 milliards d'euros de PIB en 2020 (contre 88 milliards si les initiatives restent nationales) et la création de 2,5 millions d'emplois (*ibid.*). Dans cet esprit, la Commission Européenne se dit en faveur d'une suppression des restrictions nationales au profit des libres hébergement et circulation des données en Europe[20].

Persistance de l'échelle nationale

Ce dernier point va à l'encontre des démarches du *cloud* souverain et questionne la compatibilité des échelles nationale et régionale en matière de *cloud*. C'est la raison pour laquelle, en dépit de la volonté des entreprises et des institutions, l'élaboration d'un *cloud* européen rencontre des obstacles. Les réticences émanent principalement des Etats et sont motivées par le refus de l'ingérence d'une autorité multiétatique, par la crainte d'une inégalité de capacités entre les pays membres, ou tout simplement par le souci de préservation de données jugées stratégiques.

[20] « L'analyse coût-avantage de la suppression des exigences relatives à l'emplacement des données pour les fournisseurs de services d'informatique en nuage montre des avantages nets globaux pour les utilisateurs, les fournisseurs, l'économie et la société. » (Commission Européenne, 2012).

La base territoriale sur laquelle développer un *cloud* interétatique européen est donc encore à définir et le travail d'harmonisation des politiques numériques sur le *cloud computing* reste grand. La sensibilité de certaines données nationales est l'argument le plus souvent opposé aux projets européens et le plus difficilement réfutable : si les données relevant de la défense et de la sécurité publique sont évidemment sensibles, la qualité stratégique des données peut varier en fonction des Etats. La France juge par exemple que toute donnée produite par les collectivités territoriales relève du régime des archives publiques et est considérée comme trésor national ; elle ne peut alors plus quitter le sol français (ministère de l'Intérieur, 2016). Ce type de loi empêche le fonctionnement optimisé d'un *cloud* européen mais ne peut être contesté, puisque remettre en question la qualification stratégique d'une donnée par un Etat, c'est questionner sa gouvernance et s'ingérer dans ses affaires intérieures.

Pour une approche géostratégique du *cloud computing* par les armées

Face à la numérisation de l'espace de bataille (NEB) et à la massification des données sur les théâtres d'opérations, le *cloud computing* est de plus en plus utilisé dans le dispositif de défense français. Son intégration dans les armées est néanmoins influée par les enjeux identifiés précédemment.

Les TIC dans les milieux militaires : de la RMA aux débuts du cloud

L'intégration du *cloud computing* dans les milieux militaires n'est pas un processus *ex nihilo*. S'il est important de s'interroger sur les impacts d'une nouvelle technologie dans un domaine, il l'est tout autant de chercher à identifier les motivations et les choix organisationnels qui y président (Tiers, Mourmant & Leclercq-Vandelanoitte, 2013).

Des technologies au service de la supériorité informationnelle

L'information et sa communication sont au cœur des processus décisionnels et orientent la stratégie militaire. Leur maîtrise est donc essentielle : bien informées, les troupes gagnent en efficacité et en force de frappe ; mal renseignées, les forces armées peuvent être induites en erreur, ce qui peut au mieux, ralentir l'action, au pire avoir des conséquences dramatiques (tirs fratricides) (Maulny, 2006). Les divers systèmes d'information sont donc un multiplicateur de la puissance militaire, mais peuvent également être des cibles en cas de conflit. La capacité informationnelle compte ainsi parmi les ressources militaires d'un pays (Breton, 1991) et est décisive dans la réussite d'une mission (Reddy & Monika, 2011).

Le *Livre Blanc de la Défense et de la Sécurité nationale* de 2008 énonce d'ailleurs que l'information et la communication seront à l'horizon 2025 les principaux facteurs de la supériorité opérationnelle (France, 2008[21]).

C'est dans le but d'augmenter leur capacité informationnelle que les armées ont intégré les NTIC dans leurs systèmes d'information. Ces nouvelles technologies, en plus de faciliter les échanges, contribuent à la « datafication » des théâtres d'opérations ; cela signifie qu'elles participent à leur retranscription en données numériques. Elles ont notamment conduit à la multiplication et la diversification des senseurs[22] sur la zone de combats, directement en lien avec les principes de « Surveillance (S) » et de « Reconnaissance (R) » des C4ISR[23]. L'une des meilleures illustrations de ce phénomène au sein de l'armée de terre est sans doute le programme Félin (Fantassin à équipements et liaisons intégrées), qui intègre plusieurs senseurs directement dans les équipements militaires (armements, uniforme, casque…).

En termes informationnels, la datafication présente trois intérêts majeurs : 1) grâce à sa mise en données, l'information peut être communiquée plus rapidement et plus objectivement, 2) les données se prêtent davantage aux modélisations et alimentent les représentations des théâtres d'opérations, 3) les données numériques peuvent être traitées, ce qui permet la production d'informations supplémentaires. Dans ce contexte, la maîtrise des technologies de gestion de données devient un enjeu majeur pour les armées.

Transformation numérique et guerre en réseau

L'utilisation par les milieux militaires des technologies relatives au cyberespace a conduit à ce qui est souvent désigné comme la plus récente des Révolutions dans les Affaires Militaires (RMA). Leur intégration dans les opérations militaires a été accélérée par l'apparition du principe de guerre en réseau - ou Network Centric Warfare (NCW) -, qui s'est développé durant les années 1990 et repose sur une meilleure exploitation des SIC militaires. Le NCW a été conceptualisé aux Etats-Unis en 1998 par le vice-amiral Arthur Cebrowski et John Garstka qui ont constaté qu'avec le développement des NTIC, les opérations militaires étaient de plus en plus « réseau-centrées » (Cebrowski et Garstka, 1998). Les opérations réseau-centrées (ORC) se caractérisent par la dispersion géographique des forces qui maintiennent un contact fort par de nombreuses communications et le partage de données au moyen d'un réseau cybernétique.

[21] Chapitre 12 « Intervenir »

[22] Un senseur est un dispositif technologique qui détecte un signal et le retranscrit ; les senseurs peuvent être thermiques, mécaniques, optiques, chimiques, ioniques… Ils sont les principales sources de données « brutes » à la base des informations circulant sur les SI militaires.

[23] C4ISR : *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*

Elles participent donc à la numérisation du champ de bataille et se traduisent par une augmentation des flux d'information entre les différentes composantes de l'écosystème militaire mobilisées sur une même mission (y compris entre armée de Terre, marine et armée de l'Air ou même avec les armées de pays alliés) (Maulny, 2006). Ainsi, en théorie, la guerre en réseau facilite les opérations combinées par la communication interarmées, apporte davantage de réactivité et renforce la supériorité informationnelle grâce à une bonne circulation des données recueillies par les senseurs.

Une évolution naturelle vers le cloud

La technologie du *cloud computing* apparaît alors comme l'outil de mise en pratique de la doctrine de la guerre en réseau et son intégration dans les armées semble être la suite logique des récents bouleversements qui ont impacté la Défense (RMA et ses suites). La capacité des commandements à agir rapidement, conjointement et efficacement dépend des informations disponibles au moment de la prise de décision. La prolifération des données est un avantage dans cette situation mais ces dernières nécessitent une bonne prise en charge pour être correctement exploitées. Elles requièrent des capacités de stockage et de traitement importantes qu'offre justement le *cloud computing*. Il est aujourd'hui difficilement imaginable qu'un environnement opérationnel intégrant toujours plus de senseurs et comportant des véhicules autonomes terrestres (engins robotisés) et aériens (drones) fonctionne sans le recours à l'informatique en nuage (Dyèvre, Goetz, de Maupeou, 2016).

Par ailleurs, la conduite d'opérations communes aux trois armées suppose un partage d'informations efficient et en temps réel. C'est ce qui a donné lieu, en France, au développement du concept de « combat collaboratif infovalorisé » (Maldera, 2016 ; Barraco, 2006) et au lancement du programme SIA (Système d'information des Armées) dont le but est, à terme, le rassemblement des SIC des trois armées aux niveaux stratégique, tactique et opérationnel. Or, l'une des caractéristiques fondamentales du *cloud computing* est de permettre la mutualisation quasi-instantanée des données par le partage des ressources informatiques. Il concourt donc à la création d'un environnement informationnel commun, fiable et substantiel.

Entre opportunités et vulnérabilités

Le *cloud* pourrait donc renforcer le lien entre supériorité informationnelle et efficacité opérationnelle. Technologie nouvelle, il n'en est toutefois qu'à ses prémices dans les armées et son intégration est retardée par des craintes concernant les failles sécuritaires qu'il pourrait occasionner.

Le cloud, technologie de l'économie et de la performance

Si le *cloud* intéresse les ministères de la Défense de plusieurs Etats, c'est avant tout parce qu'il permet de considérables économies, dont des économies d'échelle. Il est en effet une solution à la fragmentation des ressources informatiques, à la pénibilité de leur utilisation, ou encore à la permanence de duplicatas de SI qui sont des difficultés fréquemment rencontrées par les armées (Lele & Sharma, 2014). C'est donc dans une optique de rationalisation des SIC de la Défense qu'est lancé en 2009 le projet français INCAS (INfrastructure Communicante Adaptive et Sécurisée). Basé sur la technologie du *cloud computing*, il prévoit notamment la réduction du nombre de serveurs sur l'Intradef, le réseau intranet de la Défense, ainsi qu'une meilleure rentabilité des infrastructures d'hébergement et de stockage par leur partage (DIRISI, 2013). En 2017, ce sont 12,78 millions d'euros qui lui sont consacrés (Sénat, 2017) ; cet investissement autoriserait en retour une économie d'environ 60 millions d'euros par an (Helo, 2013). Par ailleurs, l'externalisation des dispositifs informatiques auprès d'un opérateur commun soulage les armées des tâches informatiques et les libère de la nécessité d'acquérir les compétences adéquates. Leurs budgets s'en trouvent soulagés et les efforts peuvent être concentrés sur leurs cœurs de métier. L'infogérance et la concentration des ressources permettent également une meilleure surveillance des SIC et donc davantage de sécurité : les mises à jour de l'ensemble des systèmes sont assurées et l'intégration d'avancées techniques est facilitée. Enfin, l'élasticité du *cloud* permet le déploiement de nouvelles capacités informatiques sur simple demande, à distance et quasi instantanément. Pour pallier un imprévu, il n'est plus nécessaire de prévoir des dispositifs supplémentaires et coûteux qui resteront, pour la majorité, inutilisés.

Un autre avantage majeur du *cloud computing* pour les forces militaires est d'assurer, grâce à la mutualisation systématique des données et de grandes capacités de traitement, la disponibilité immédiate d'informations nombreuses et contextualisées. En plus de prévenir la saturation des récepteurs et la disparité des informations, le *cloud* facilite l'organisation et la hiérarchisation de l'information. Il est en outre à la base de nombreuses innovations technologiques de traitement de données, telles que le *big data*. La mutualisation des dispositifs informatiques cause le rapprochement de bases de données jusqu'alors séparées (données météorologiques, état de santé des combattants…) et autorise leur agrégation. L'information qui résulte du traitement conjoint de ces bases de données apporte des renseignements précis et inédits qui, agrémentés d'une connaissance approfondie de l'environnement et de l'ennemi, peuvent avoir des conséquences directes sur le déroulement des opérations (lieu de déploiement des unités, moment choisi pour accomplir une mission…).

La collecte et le traitement de données de masse offerts par le *cloud computing* sont aussi de bons moyens de surveillance d'un adversaire ; l'analyse systématique et en temps réel permet par exemple de déceler des récurrences et donc d'anticiper le comportement des forces ennemies ou d'alerter en cas de comportement inhabituel.

Le *cloud*, enfin, répond aux nouveaux besoins opérationnels que génère l'évolution de la conflictualité contemporaine[24]. En augmentant la rapidité de la circulation de l'information entre les plateformes, il améliore la synergie entre les groupes opérationnels et la réactivité des forces. Le *cloud* permet ainsi de faire face à l'accélération du rythme des opérations. Il accompagne aussi l'évolution qualitative des actions militaires à l'heure où la réflexion porte davantage sur l'effet produit que sur les ressources mobilisées. Adjuvant de la capacité informationnelle, le *cloud computing* facilite effectivement la conduite d'opérations directement sur des cibles identifiées et facilite les frappes chirurgicales[25]. Cela limite l'exposition des armées à des sanctions juridiques internationales dans un contexte de judiciarisation croissante des conflits (DGRIS, 2017). Dans la continuité des préceptes de la guerre en réseau, le *cloud* offre, en sus, davantage de mobilité aux forces qui sont confrontées depuis quelques décennies à un agrandissement des champs de bataille et à la transnationalisation des conflits. Malgré leur répartition sur le globe, les unités doivent pouvoir communiquer entre elles, maintenir le contact avec la métropole et les commandements, et accéder aux bases de données, quel que soit l'endroit où elles se trouvent. Le caractère ubiquitaire du *cloud* en fait un instrument particulièrement adapté pour les structures constituées de plusieurs entités géographiquement dispersées dont les armées sont l'archétype.

La supériorité informationnelle à laquelle contribue le *cloud* augmente ainsi la précision, la rapidité et l'amplitude des opérations et des frappes, et donc *in fine* la puissance militaire. En augmentant sa puissance militaire, un Etat se dote d'une « influence préventive » (*ibid.*, p.65) qui induit une forme de dissuasion. En France, le ministère des Armées insiste sur ce point et estime que cette dimension doit être priorisée.

Des enjeux sécuritaires

Si le *cloud computing* est créateur d'opportunités, son intégration ne présente pas un risque nul et ce sont surtout des préoccupations sécuritaires qui freinent son développement dans les armées. En théorie, le *cloud* repose sur les principes de confidentialité (l'information n'est accessible qu'aux personnes autorisées), d'intégrité (l'information n'est pas modifiée sans consentement) et de

[24] La DGRIS (Direction Générale des Relations Internationales et de la Stratégie), dans son document *Horizons Stratégiques*, relève plusieurs de ces évolutions. Elle reprend les objectifs du plan prospectif à 30 ans (PP30) et cherche à « éclairer la préparation des programmes d'armement, en identifiant notamment les facteurs et les risques de ruptures opérationnels et technologiques. » (DGRIS, 2017).

[25] Une frappe chirurgicale désigne une action militaire dont la cible est précise et exclusivement militaire ; les dommages collatéraux sont évités (populations civiles, bâtiments, véhicules, infrastructures publiques…).

disponibilité des données (l'information n'est ni détruite ni perdue et peut être consultée à n'importe quel moment depuis n'importe quel endroit). Dans le cas d'un usage militaire du *cloud*, aucun de ces principes ne peut être négligé puisqu'il y va de la planification d'une opération voire même d'une stratégie de long terme.

Pourtant, en tant que NTIC, il entraîne les mêmes vulnérabilités que tout élément ayant un rôle à jouer dans la guerre de l'information. Par exemple, les forces armées sont dépendantes des informations dont elles disposent ; la migration de ces informations vers le *cloud* entraînerait une dépendance des forces à cette technologie qui pourrait être endommagée lors d'affrontements. De nombreux pays cherchent d'ailleurs à développer des outils de lutte informatique offensive afin d'entamer les capacités de commandement et de contrôle (C2) de leurs adversaires. La difficulté serait alors d'assurer la continuité d'une opération même en cas de dysfonctionnement ou d'indisponibilité du *cloud* militaire. Si le *cloud* garantit une certaine résilience des informations, il faut donc également assurer la résilience du *cloud* lui-même[26].

Mais le *cloud* soulève aussi des enjeux sécuritaires qui lui sont propres. L'une de ses particularités est d'occasionner la concentration des ressources informatiques ; cette concentration accroît les risques. Le rassemblement des dispositifs physiques et logiciels dans les *datacenters* fait de ces établissements des cibles de choix pour des attaques physiques ou des cyberattaques, visant leur destruction, l'appropriation des données ou les deux simultanément. Les centres de données sont donc des infrastructures critiques qu'il convient de protéger. La proximité physique et logicielle des machines virtuelles (MV) peut aussi poser des problèmes d'étanchéité lorsque celles-ci sont hébergées sur un même hyperviseur (Owens, 2010). Or, toutes les forces n'ont pas droit d'accès aux mêmes niveaux d'information. Il faut par ailleurs parfaire les systèmes d'authentification, tant au niveau de l'accès des données qu'au niveau de leur envoi sur le *cloud* ; si les senseurs sont directement reliés au *cloud*, les données pourraient être faussées dans le cas où les appareils tomberaient entre des mains ennemies. La réunion de nombreuses données en un seul et même lieu – le *cloud* – augmente également le risque de vols. Son fonctionnement réticulaire oblige à considérer la menace comme systémique : si une unité est compromise, c'est certes les données auxquelles elle accède qui sont exposées, mais également toutes celles des unités qui interagissent avec elle. Le moindre appareil d'extrémité présente alors un risque d'intrusion pour l'ensemble du système. Bien qu'il soit possible de crypter les données pour les protéger, ces méthodes sont contraignantes et peuvent s'avérer inefficaces si leur traitement nécessite leur déchiffrement.

[26] Pour davantage d'informations sur la résilience dans le *cloud*, voir : BÔMONT Clotilde, « Résilience des SIC militaires : *cloud* défense et hyperconnectivité des théâtres d'opérations », *Revue de la gendarmerie nationale*, n°260, pp. 38-45 http://fr.calameo.com/read/002719292d3eff1e8eb9a?page=38

Pour finir, la disponibilité des données dans le *cloud* est conditionnée par la connectivité au réseau et les performances de ce dernier. Les SIC militaires ne peuvent pas s'appuyer sur le réseau public, aussi la Défense doit-elle disposer d'un réseau propre. L'attention doit donc également être portée sur le développement des capacités de bande passante pour éviter la surcharge et l'indisponibilité. La structure doit être suffisamment résistante pour recevoir des flux de données aux volumes toujours plus importants et les relayer.

Le cloud Défense français

Les Etats sont préparés à combattre dans un monde de plus en plus digitalisé où les forces, comme l'ensemble de la population en général, sont dépendantes des NTIC. Présentant de nombreux avantages et déjà approprié à divers degrés par d'autres Etats (Etats-Unis, Chine, Russie), le développement d'un *cloud* militaire français s'est imposé en dépit des risques qu'il comporte. Le besoin impérieux de sécurisation des données ne permet pas que leur gestion soit assurée par des prestataires extérieurs ; en France, c'est donc la DIRISI (Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la défense) qui joue le rôle d'opérateur des télécommunications et d'infogérant des SI de la Défense. Dans le cadre de sa mission de modernisation des armées, elle est en charge depuis 2014 de l'élaboration du c*loud* défense qui prévoit la réunion des ressources et des moyens des trois armées (terre, mer, air). S'il est encore en construction, il est d'ores et déjà possible de distinguer deux niveaux dans ce *cloud* : l'échelle tactique à travers la mise en place d'un « *cloud* de théâtre » qui assurerait à l'Arrière le stockage et le traitement des données recueillies par les équipements de contact, et l'échelle stratégique qui centraliserait l'information sur une sorte de « méta-*cloud* » défense (Dyèvre, Goetz, de Maupeou, 2016).

Développer une stratégie du cloud

La dernière partie de ce travail de recherche constitue un début d'analyse prospective sur le devenir du *cloud computing* au sein des forces armées. Cette analyse, en s'appuyant sur l'ensemble des problématiques déterminées précédemment, part du constat d'une inadéquation entre les bouleversements induits par l'intégration du *cloud computing* et la façon dont est abordé ce nouvel objet.

De l'outil technique à une approche conceptuelle

L'intégration du *cloud* dans les armées suppose quelques ajustements techniques mais il pose aussi des questions organisationnelles. La première difficulté vient de la rapidité de développement des technologies numériques qui se sont imposées à l'ensemble de la population en une génération à peine.

Alors qu'elles sont en pleine transformation numérique, les forces françaises sont confrontées à une complexification supplémentaire et incontournable avec l'arrivée de l'informatique en nuage. L'absence de recul sur cette technologie et les déjà nombreuses et récentes adaptations des SIC expliquent que le *cloud* ne soit encore qu'en construction.

Au sein de l'action militaire, le *cloud computing* modifie les « cloisonnements » des armées tant verticaux qu'horizontaux. Le second obstacle pourrait donc éventuellement venir d'une rigidité des systèmes de commandement. Par « cloisonnement vertical » est entendue la séparation traditionnelle entre les trois armées (terre, mer, air). En contribuant au fonctionnement interarmées systématique et à l'accomplissement d'opérations conjointes, le *cloud* modifie cette organisation. Le « cloisonnement horizontal » renvoie aux différents niveaux hiérarchiques. Les actions militaires répondent à un objectif politique ; or, le *cloud* concourt à leur accélération, ce qui suppose un raccourcissement du cycle décisionnel qui s'opère souvent au détriment du contrôle politique (Maulny, 2006). De plus, en mettant à disposition l'information déjà choisie, traitée et donc dirigée vers un objectif, le *cloud* permet davantage d'initiatives directement au niveau des forces sur le terrain. Dans l'environnement opérationnel actuel, la prise de décision immédiate peut se révéler avantageuse.

Ces appréhensions seront dépassées si l'on considère le *cloud* comme un atout à part entière. La complexification des SIC redoutée peut à l'inverse être perçue comme une simplification grâce à une gestion centralisée par un opérateur spécialisé —la DIRISI. Par ailleurs, les décideurs politiques et militaires jouent un rôle déterminant dans l'établissement d'une véritable stratégie autour du *cloud computing* qui pourra, elle seule, garantir la sécurité du dispositif.

La sécurité d'un *cloud* comprend bien sûr sa protection par des mesures techniques (pare-feu, antivirus, cryptologie…). Il faut toutefois y ajouter une dimension supplémentaire et indispensable qui envisage la sécurité du *cloud* comme un procédé géopolitique et géostratégique. Les décideurs doivent avoir une bonne connaissance des enjeux sous-jacents au déploiement du *cloud* défense et la nécessité d'une stratégie propre à cet outil technique se fait jour. Celle-ci doit être pensée dès l'élaboration du *cloud* qui répond alors à des décisions politiques et des positionnements stratégiques. Conceptualiser le *cloud* en amont de sa construction et de son utilisation par les forces permet donc une meilleure sécurisation.

Guider le déploiement du cloud défense : définir son périmètre

Maîtriser le *cloud computing* revient dans ce cas à guider le déploiement du *cloud* défense. Après identification des diverses variables intervenant dans la construction et le fonctionnement d'un *cloud,* il s'agit de déterminer sur lesquelles faire reposer une stratégie.

Chacune d'entre elles peut ensuite être évaluée selon un rapport bénéfices/risques, en fonction des opportunités et des vulnérabilités qu'engendre leur paramétrage. Forts de cet éclairage, les décideurs peuvent établir le périmètre *optimum* d'un *cloud* défense relativement à un objectif, soit choisir sciemment les limites et les modalités de déploiement du *cloud*.

Le tableau ci-contre est une proposition de grille d'évaluation du périmètre stratégique d'un *cloud*.

Grille d'évaluation du périmètre stratégique d'un cloud

Périmètre	Nature	Opportunité(s)	Vulnérabilité(s)	Puissance data-numérique française
Géographique	Terrains sur lesquels il est ou non possible de l'utiliser ; localisation des infrastructures ; mobilité des infrastructures	Concentration des moyens et des ressources (meilleure gestion et protection)	Infrastructures critiques à protéger (protection des bâtiments et des logiciels), contraintes de localisation, consommation énergétique	Présence sur le territoire d'infrastructures de droit français
Acteurs (prestataires)	Mindef, entreprises, gouvernements étrangers, organisations multinationales ; déploiement IaaS, PaaS ou IaaS ; *cloud* hybride…	Gain de compétences	Relâchement dans la restriction de l'accès aux données ; souveraineté ; dépendance	Compétences, entreprises spécialisées…
Usages	Stockage, traitement, mutualisation	Big Data, IoT, Data mining, Machine learning, temps réel, résilience des informations…	Capacités de gestion des données	Infrastructures et applicatifs, formation et recherche…
Champs d'application	*Cloud* privé, public ou communautaire ; commandements, terrain ; interarmées…	Efficacité, interopérabilité, économie et rationalisation (ex : éviter les duplicatas de systèmes), résilience des informations	Réunion d'informations et de données	Niveau et profondeur de développement du *cloud* défense
Réseau	Internet ou intranet, étendue de l'intranet (aire de desserte), nature des connexions (filaires, électromagnétiques, satellitaires)	Agilité, adaptabilité, redistribution et création de performance	Interception, parasitage	Maturité technique
Données	Types de données, provenance, sensibilité, « brutes » ou traitées…	Création de valeur ajoutée	Sources d'informations	Attraction des flux de données

Bômont Clotilde, 2017

Conclusion

Le verbe maîtriser connaît trois définitions que l'on peut appliquer au *cloud*. Il renvoie d'abord au fait de savoir utiliser correctement et pleinement cette technologie. Maîtriser le *cloud*, c'est donc déjà le comprendre et être conscient de son fonctionnement ; sa spatialisation contribue à cet effort. La notion de maîtrise amène également celle de domination, ce qui fait écho aux rapports de force entre les acteurs pour le contrôle du *cloud* et aux moyens qu'ils mettent en œuvre pour y parvenir. Le troisième sens du verbe maîtriser se rapproche de celui de dompter ; rester maître du *cloud* permet de profiter de ses potentialités tout en se prémunissant des risques qui lui sont inhérents. Cela n'est possible qu'à condition de mener une réflexion géostratégique dès l'élaboration d'un *cloud*.

Les résultats présentés dans cet article ont été obtenus au cours d'un mémoire de recherche ; ces travaux sont poursuivis dans le cadre d'un doctorat dont l'objectif est la mise en application des recommandations formulées dans la dernière partie. Le but de la thèse est de créer un outil, à disposition des commandements, qui rendra opérationnelles les analyses portant sur l'évaluation du périmètre stratégique d'un *cloud*. Cet objectif de recherche répond à l'urgence de développer des cyber-capacités nationales solides et rend compte de la place centrale du *cloud computing* dans l'écosystème numérique.

Bibliographie

Ademe, 2017, *La face cachée du numérique : réduire les impacts du numérique sur l'environnement*, décembre 2017, consulté le 24/03/2018 et disponible à l'URL : http://www.ademe.fr/sites/default/files/assets/documents/guide-pratique-face-cachee-numerique.pdf

Anderson Jana et Rainie Lee, 2010, « The future of cloud computing », Pew research institute, internet and technology, consulté le 08/06/2017 et disponible à l'URL : http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing/

Bakis Henry, 2013, « Les facteurs de localisation d'un nouveau type d'établissements tertiaires : les datacenters », *Netcom*, Vol.27, n°3-4

Barraco Laurent, 2006, « La bulle opérationnelle aéroterrestre », *Le Jaune et la Rouge : Revue mensuelle de l'association des anciens élèves et diplômés de l'école Polytechnique*, n°615, consulté le 28/05/2017 et disponible à l'URL : http://www.lajauneetlarouge.com/article/la-bulle-operationnelle-aeroterrestre#.WSrn4-vyiM8

Bensamoun Alexandra et Zolynski Célia, 2015, « Cloud computing et big data : quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux*, n°189, La Découverte

Bloch Laurent, 2015, *Révolution cyberindustrielle en France*, Collection Cyberstratégie, Economica

Breton Thierry, 1991, *La Dimension invisible : le défi du temps et de l'information*, Editions Odile Jacob

Cattaruzza Amaël, Danet Didier, Desforges Alix, Douzet Frédérick, Naccache David, 2014, *La balkanisation du web : chance ou risque pour l'Europe?*, ministère de la Défense

Cebrowski Arthur et Garstka John, 1998, "Network-Centric Warfare : Its Origin And Future", communication, janvier 1998

Chartron Ghislaine et Broudoux Evelyne, 2015, « Enjeux géopolitiques des données, asymétries déterminantes », actes du colloque *Open data, big data : quelle valeur?*, Rabat, Maroc, Edition De Boeck

Commission européenne, 2012, *Exploiter le potentiel de l'informatique en nuage*, COM(2012) 529 final

Danet Didier, 2014, « Quelle souveraineté numérique à l'âge du Cloud Computing ? », lors du colloque *Droit et souverainetés à l'âge d'Internet*, Rennes, 12 septembre 2014

De Filippi Primavera et McCarthy Smari, 2012, « Cloud computing : centralization and data sovereignty », *European Journal of Law and Technology*, Vol. 3, n°2

Desmedt Patrice, 2012, « Où sont vos données ? », *L'Usine nouvelle*, n°3274, Groupe Industrie Services Info

DGRIS, 2017, *Horizons Stratégiques*, ministère de la Défense, France, consulté le 30/05/2017 et disponible à l'URL : http://www.defense.gouv.fr/dgris/recherche-et-prospective/prospective-de-defense/horizons-strategiques

Dirisi, 2013, *Stratégie du système d'information de l'Etat : synthèse des contrats de progrès ministériels 2013-2015*, Décembre 2013, 54 p., consulté le 18 mars 2018 et disponible à l'URL : http://www.modernisation.gouv.fr/sites/default/files/fichiers-attaches/contrats_progres_ministeriels_2013-2015_0.pdf

Dyevre Axel, Goetz Pierre et de Maupeou Martin, 2016, *Emploi du cloud dans les armées : première approche des concepts et contraintes*, Les notes stratégiques, CEIS, août 2016

Flipo Fabrice, Deltour François, Gossard Cédric, Dobre Michelle, Michot Marion, et al., 2009, *Technologies numériques et crise environnementale : peut-on croire aux TIC vertes*, Rapport de recherche, Projet Ecotic

Flechaux Reynald, 2014, « Efficacité des datacenters : l'indicateur européen DCEM veut enterrer le PUE », consulté le 7/04/2017 sur le site www.silicon.fr et disponible à l'URL : www.silicon.fr/efficacite-energtique-datacenters-dcem-europe-enterrer-pue-95088.html

France, éd. 2008, *Défense et sécurité nationale 2008 : livre blanc*, La Documentation française

Gibson William, 1984, *Neuromancer*, Mass Market Paperback Edition

Greenpeace, 2012, *How clean is your cloud?*, Greenpeace International

Helo Philippe, 2013, « Le Cloud Computing dans les applications militaires : la défense française peut mieux faire », *Pensées Mili-Terre*, CDEC, consulté le 28/02/2017 et disponible à l'URL : http://www.penseemiliterre.fr/le-cloud-computing-dans-les-applications-militaires-la-defense-francaise-peut-mieux-faire_2015825.html#_edn6

Hintermann Francis, 2010, « Informatique : la révolution des nuages », *L'expansion management review*, n°139, L'express – Roularta

Kitchin Rob, 2014, *The Data revolution: Big Data, Open Data, Data infrastructures and their consequences*, Sage

L'informaticien, 2017, « Cloud souverain : mythes et réalités », *L'informaticien*, février 2017, n°154, PC Presse

Lohard Audrey, 2008, « La Genèse inattendue du cyberespace de William Gibson », *Quaderni*, n°66, Editions de la Maison des sciences de l'homme

Maldera Nicolas, 2016, « La mutation technologique de l'Armée de Terre, le cas du programme Scorpion », *Etat et collectivités*, Fondation Ifrap, consulté le 25/05/2017 et disponible à l'URL : http://www.ifrap.org/etat-et-collectivites/la-mutation-technologique-de-larmee-de-terre-le-cas-du-programme-scorpion

Maulny Jean-Pierre, 2006, *La Guerre en réseau au XXIème siècle : Internet sur les champs de bataille*, Collection « Echéances », Le Félin Kiron

Maxwell Winston et Wolf Christopher, 2012, « A Global Reality: Governmental Access to Data in the Cloud », *A Hogan Lovells White Paper*, Hogan Lovells

Mell Peter et Grance Timothy, 2011, *The NIST Definition of Cloud Computing : Recommandations of the National Institute of Standards and Technology*, US Department of Commerce

Ministère de L'intérieur (France), 2016, *Note d'information du 5 avril 2016 relative à l'informatique en nuage (cloud computing)*

Morel Camille, 2017, « Les câbles sous-marins : un bien commun mondial ? », *Etudes*, 2017/3, S.E.R.

Nocetti Julien, 2017, « L'intelligence artificielle s'apprête à bouleverser la politique internationale », *Le Monde*, 25 octobre 2017, consulté le 8 mars 2018 et disponible à l'URL : http://www.lemonde.fr/idees/article/2017/10/25/l-intelligence-artificielle-s-apprete-a-bouleverser-la-politique-internationale_5205453_3232.html

Nye Jospeh Jr., 2010, *Cyber power*, Harvard Kennedy School

Okta, 2017, « Business @ work », consulté le 4 mai 2017 et disponible à l'URL : https://www.okta.com/Businesses-At-Work/2017-01/

Owens Dustin, 2010, « Securing elasticity in the Cloud », *Communication of the ACM*, vol.53, n°6

Plouin Guillaume, 2011, *Cloud computing : Une rupture décisive pour l'information*, 2ème édition, Dunod

Reddy Mounika et Monika Mary, « Integrate Military with Distributed Cloud Computing and Secure Virtualization », *International journal of enhanced research in management and computer applications*, Vol.2

Sénat, 2017, *Projet de loi de finances pour 2017 : Défense : Préparation et emploi de forces*, consulté le 30/05/2017 et disponible à l'URL : http://www.senat.fr/rap/a16-142-6/a16-14263.html#fnref7

Song Z., Zhang Xiaojing et Eriksson J., 2015, « Data center energy and cost saving evaluation », *Energy Proceedia*, vol.75

Synergy Research Group, 2017a, « Amazon Cloud Growth is Hardly Hampered by the Chasing Pack », 27 avril 2017, consulté le 4 mai 2017 et disponible à l'URL : https://www.srgresearch.com/articles/amazon-cloud-growth-hardly-hampered-chasing-pack

Synergy Research Group, 2017b, « Cloud Market Keeps Growing at Over 40%: Amazon Still Increases its Share », 27 octobre 2017, consulté le 6 mars 2018 et disponible à l'URL : https://www.srgresearch.com/articles/cloud-market-keeps-growing-over-40-amazon-still-increases-share

Tiers Grégoire, Mourmant Gaëtan et Leclercq-Vandelanoitte Aurélie, 2013, « L'envol vers le Cloud : un phénomène de maturations multiples », *Systèmes d'information & management*, 2013/4, Vol.18, ESKA.

Union europénne, 2016, *Règlement général sur la protection des données*, Journal officiel de l'Union Européenne, L119/1.

Ullmann Charlotte, Vidal Philippe, Bourcier Alban, 2008, « L'avènement d'une société de l'information durable », *Networks and communication studies*, Vol.22, n° 3-4, NETCOM

Van Hoboken Joris, Arnbak Axel Et Van Eijk Nico, 2012, *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act*, Ivir.