Mesdames, Messieurs,

Je tiens tout d'abord à vous présenter mes meilleurs vœux pour cette nouvelle année, et à vous remercier de m'avoir invité à échanger quelques mots à l'occasion de cet événement clé pour votre groupe.

J'ai l'honneur de diriger depuis 9 mois la toute récente Agence du Numérique de Défense (AND) au sein du Ministère des Armées, qui a été créée fin avril de l'année dernière.

L'AND est un service à compétence nationale, dont les 3 missions sont : la conduite de projets numériques sur tout le cycle de vie au profit de l'ensemble du Ministère ; le conseil aux autorités métier pour optimiser les ressources (effectifs, compétences, budgets) ; et la mise en œuvre de la politique industrielle dans le domaine des technologies numériques des systèmes d'information.

Pour mettre en œuvre la politique industrielle, le directeur de l'AND est représentant du pouvoir adjudicateur sans limitation de montant, donc a l'autorité pour signer les contrats ; il a aussi des leviers budgétaires. Mais évidemment, c'est surtout en amont des procédures de passation des contrats que l'on peut réellement mettre en œuvre une politique industrielle : en connaissant d'abord le marché (TPE, PME, ETI, ESN, éditeurs, grands groupes), en échangeant au niveau des stratégies respectives pour faciliter l'alignement entre client et fournisseurs potentiels, en suggérant des regroupements quand cela apporte a priori de la valeur pour nous client, en organisant au niveau de l'ingénierie contractuelle la stratégie d'acquisition pour qu'elle soit la plus cohérente possible avec la structuration du marché fournisseur.

D'où l'importance au préalable de créer et faciliter le dialogue entre acteurs, pour qu'ils se connaissent, se fassent confiance, construisent des alliances au-delà des opportunités immédiates. C'est entre autres pour cela que je suis avec intérêt les travaux du GINUM, le groupement des intervenants du numérique, lancé l'été dernier par Orange, ainsi que CS Group, une ETI, Mentor Consultant, une PME, et qu'ont déjà rejoint un certain nombre d'acteurs de toute taille du numérique intervenant dans les domaines de la défense, de la sécurité, des enjeux d'importance vitale.

Voilà en quelques mots ce qu'est l'Agence du numérique de défense. Au vu de ses missions, en tant qu'acteur clé des projets numériques du Ministère des Armées, il est donc logique que nous nous intéressions à des problématiques comme la souveraineté numérique.

Je vais donc parler de souveraineté numérique, mais aussi d'autonomie stratégique, de confiance, et aussi de résilience, et je vais essayer de placer au fur et à mesure ces différents concepts les uns par rapport aux autres. Cela me permettra aussi de donner, en particulier, un point de vue nécessairement personnel sur ces notions appliquées par exemple au Cloud.

Tout le monde s'accorde à dire aujourd'hui que la question de la souveraineté numérique est clé. Si l'on revient à la définition assez largement répandue de Louis Le Fur, né en 1870, « *la souveraineté est la qualité de l'État de n'être obligé ou déterminé que par sa propre volonté* ».

Il est intéressant de voir que dans un rapport des Nations Unies de 2015 rédigé par le groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, il est souligné l'importance du droit international et du principe de souveraineté comme fondements d'une meilleure sécurité, et il est stipulé que les Etats doivent prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux TIC.

Ce rapport reprend un précédent rapport de 2013, toujours des Nations Unies, qui disait déjà que la politique des Etats en matière informatique, et leur compétence territoriale pour ce qui est des infrastructures informatiques présentes sur leur territoire, relèvent de la souveraineté des Etats.

Par ailleurs, une résolution adoptée par l'Assemblée générale des Nations Unies le 31 décembre 2020 confirme que la souveraineté étatique, et les normes et principes internationaux qui procèdent de la souveraineté, s'appliquent à l'utilisation du numérique par les Etats ainsi qu'à leur compétence territoriale en matière d'infrastructures numériques.

Ce qui est clé, est donc la protection des intérêts de l'Etat, et en particulier sa continuité d'action en cas de crise, c'est la question de sa résilience. Sans détailler, la résilience c'est la capacité à retrouver un nouvel équilibre après une perturbation a priori déstabilisante. Etymologiquement, mais l'image est parlante, on saute en arrière après une perte d'équilibre (re-salio en latin), un peu comme les gymnastes quand leur réception n'est pas parfaitement exécutée. C'est toute la différence avec la robustesse où il s'agit plutôt d'absorber la perturbation, dans la mesure où on revient au même état d'équilibre qu'avant.

La résilience nécessite une analyse des risques : rappelons qu'un risque, contrairement au sens usuel du terme, est la combinaison de la probabilité d'occurrence d'un événement et de l'impact dudit événement sur le système considéré. Il faut donc identifier les événements

potentiels susceptibles d'avoir un impact sur l'Etat, leur occurrence potentielle, et évaluer cet impact, c'est-à-dire évaluer son coût quant à la continuité d'action de l'Etat.

En particulier : Quel est le coût de l'arrêt d'un service numérique s'il n'est plus disponible ? Quel est le coût d'une malversation au niveau d'un service numérique clé, tant individuellement (par exemple pour une industrie critique, ou un établissement public critique) que collectivement (par exemple au niveau de la société) ?

Les mêmes rapports des Nations Unies mentionnent également les notions de confiance et de transparence. Mais remarquons tout de suite que la confiance et/ou la transparence ne sont pas des gages de souveraineté : on peut être transparent sur ses produits, sur leur contenu, et pourtant en limiter l'usage, mais aussi la copie, ce qui intuitivement apparaît comme un obstacle à une quelconque souveraineté, vous en conviendrez.

Si je voulais oser une métaphore, le numérique est aujourd'hui un peu comme l'agriculture et son industrialisation explosive lors de la 2e moitié du 20e siècle ; avec cette analogie, la souveraineté numérique, c'est du bio et de la traçabilité complète des processus de fabrication et de distribution. La confiance, c'est la composition des produits, voire éventuellement leur traçabilité mais pas des processus de fabrication et de distribution.

J'aurai l'occasion de reparler de confiance plus tard dans mon exposé, quand je parlerai de Clouds. Revenons à la notion de souveraineté. Notons d'abord que la souveraineté numérique est un pan de la souveraineté économique et industrielle : quels acteurs garder, préserver, coconner, développer, et à chaque fois pendant combien de temps ? Je ne développerai pas ce point, mais une question à se poser est aussi : quelle politique des brevets dans le domaine du numérique, pour garantir une protection des savoir-faire et des données, à des fins de production industrielle et d'exploitation commerciale ? A ce propos, souvenons-nous qu'a priori l'Europe est numéro 1 en termes de données industrielles, j'ai bien dit industrielles et non personnelles, où c'est a priori la Chine qui l'est.

Ensuite, on peut se poser la question de savoir si la souveraineté nationale nécessite un champion sur le plan industriel. En fait cela ne m'apparaît pas nécessaire, dans la mesure où un champion industriel ne peut aussi réussir en tant que champion que s'il a une assise multinationale, ce qui peut alors aller à l'encontre de certaines visions de souverainetés nationales. Encore faut-il savoir ce que l'on entend par « souveraineté ».

Si on veut tenter une première définition, la souveraineté est la capacité de l'Etat à agir indépendamment : c'est le pouvoir du capitaine sur le bateau. Notons bien que c'est la qualité de la puissance et non la puissance elle-même.

Revenons un peu sur l'histoire du concept de souveraineté, car l'évolution des acceptions au cours des siècles est intéressante à plus d'un titre, certains questionnements philosophiques trouvant des résonances particulièrement intéressantes pour la souveraineté numérique.

Sous Henri III de France, le dernier des Valois, la souveraineté est assimilée au pouvoir absolu, illimité, qui établit la loi, mais n'est pas contrôlé par la loi. Je ne rentre pas dans les détails quant à savoir si cette souveraineté serait ou pas de droit divin, ou simplement incarnée par celui que l'on appelle justement le souverain, en tant qu'individu. Ce qu'il faut retenir, c'est ce caractère absolu et l'absence de contrôle.

Cet aspect d'absolu a évolué au cours du siècle suivant avec les traités de Westphalie (1648, fin de la guerre de 30 ans, pour mémoire), introduisant le concept d'Etat Nation, où la souveraineté est le moyen pour les princes et les Etats de revendiquer vis-à-vis du dehors leur indépendance, une indépendance qui est un attribut de l'Etat souverain en droit international.

La question a ensuite été de décider si les individus avaient certains droits naturels mais pouvaient en abandonner une partie au profit d'une autorité instituée par l'Etat, qui lui garantirait la protection et préservation de ses autres droits.

Emerge encore un siècle plus tard la notion de contrat social, le dilemme étant alors de savoir s'il fallait mettre une limitation morale, voire légale, à l'autorité instituée par l'Etat (c'est le débat Hobbes versus Rousseau, et la question abordée par les premières constitutions américaine et française quant à une souveraineté nationale versus populaire). Ces réflexions sont clé, car posant la différence entre les théories de gouvernement et celles d'Etat : un gouvernement, c'est une magistrature ; l'Etat a quant à lui un caractère transcendantal.

Pour souligner l'actualité de ces questions, replaçons-nous dans le domaine numérique, l'analogie avec le domaine politique étant immédiate : si la souveraineté est une forme de pouvoir de contrôle, comment l'exercer dans des topologies de réseaux complètement connectés, chaque nœud pouvant légitimer localement l'exercice de sa souveraineté, éventuellement par sécession, mais le réseau global n'ayant pas la légitimité propre sur la légitimité de ses nœuds. Et réciproquement, la souveraineté ne désignant pas une somme de pouvoirs que l'Etat détient d'une manière légale sur le plan international.

Dans des réseaux en étoile ou des réseaux dits de petit monde (des gros nœuds avec beaucoup de connexions et des petits nœuds avec peu de connexions), on peut imaginer une légitimité centralisée, mais elle n'est pas nécessairement populaire parmi les électeurs attachés à des valeurs et politiques nationales. C'est tout le problème de l'Union Européenne.

Le mécanisme de « coopération accrue » pourrait alors être mis en œuvre, avec une notion de « souveraineté combinée » s'inscrivant dans une vision fédérative. Pas gagné à court terme dans l'Europe que nous connaissons actuellement !

Ceci dit, cette balkanisation, même si elle semble populaire aux yeux des citoyens européens pour préserver leur « identité nationale » est fondamentalement source de frictions et d'inefficacité. Certes des solutions peuvent être mises en place, mais lentement : si chaque pays a ses opérateurs de télécommunications, il est dorénavant possible de faire du roaming (dimension technique) et même sans frais (dimension économique) entre pays partenaires. Mais que de temps et de réglementations ont été nécessaires !

Historiquement, on est donc passé d'une conception absolue et hors du champ du contrôle, à une conception limitative et régulée potentiellement de différentes manières. Revenons sur cet aspect de régulation.

C'est alors une décision politique d'équilibrer le coût économique de la régulation par rapport aux bénéfices de la sécurité et la protection privée. Réguler, c'est se priver potentiellement de certains bénéfices économiques de la connectivité, c'est poser potentiellement une barrière à une expansion internationale. Mais cela n'empêche pas de se développer : la Chine en est l'exemple extrême.

Une régulation peut aussi venir par exemple par la normalisation (et pas que par l'outil juridique). Les Etats-Unis, la Chine, l'ont très bien compris, imposant leurs standards, leurs normes, perdant quelquefois, gagnant plus souvent. Une norme, c'est un condensé de l'état de l'art du moment, de R&D, et de logique économique promue par un pouvoir public ou un privé ou les deux alliés, sur une fenêtre de temps ni trop courte ni trop longue.

Arme économique pour celui qui la manie, c'est aussi un vecteur de fragilité pour celui qui la subit : la conformité aux normes et aux lois internationales, la « compliance » comme on dit en franglais, n'est pas nécessairement gage d'interopérabilité. En fait c'est un acte de confiance, voire un acte de foi, que de s'y plier, car on rentre *de facto* dans le jeu de celui qui a édicté, qui a concocté, ces normes ou ces lois. Il est intéressant de regarder rapidement cela à l'aune d'un exemple d'actualité. RGPD versus Cloud Act. Deux régulations relevant de deux philosophies politiques et économiques différentes. Le RGPD est un bouclier interdictif,

limitant le champ d'action des acteurs étrangers à l'intérieur de sa zone géographique d'origine, bref il relève de la défense. Le Cloud Act est une arme intrusive, renforçant le champ d'action des acteurs étrangers à l'extérieur de sa zone géographique d'origine, bref il relève de l'attaque.

Si on revient à notre sujet de la souveraineté, on voit que la confiance n'est pas un gage de souveraineté, que la souveraineté ne se bâtit pas que sur la confiance. En fait, déjà à la base, la souveraineté relève de soi-même, alors que la confiance relève d'une relation de soi à l'autre. Les deux ne sont pas comparables.

La souveraineté relève donc d'une capacité à réguler, et la régulation impacte la souveraineté quant à son influence sur la capacité à agir, c'est-à-dire sur l'autonomie stratégique. Cette dernière, l'autonomie, est à la souveraineté ce que les moyens sont aux fins. L'autonomie stratégique, c'est la souveraineté en acte. L'autonomie stratégique, c'est être en mesure de faire des choix, réduire des dépendances, ne pas exclure certaines dépendances mais en choisir les modalités, pour mieux défendre les intérêts et valeurs.

C'est donc choisir et maîtriser nos dépendances, et par conséquent nos indépendances, qu'elles soient au niveau technologique, au niveau de la production, au niveau de la distribution.

Comme le disait le président du Conseil Européen, Charles Michel, il y a 1 an, l'autonomie stratégique signifie davantage de résilience et d'influence, moins de dépendance. Il est indéniable que l'Union Européenne, en tant que première puissance commerciale dans le monde, constituant une économie de marché ouverte avec ses 450 millions de consommateurs, ayant négocié des accords commerciaux avec d'autres grandes économies et blocs régionaux, compte.

Affirmer notre souveraineté numérique pour exercer notre autonomie stratégique suppose d'avoir le choix entre différentes solutions technologiques viables industriellement et commercialement, au niveau national, pour pouvoir compter ensuite au niveau européen. En effet, il paraît nécessaire de bâtir sur la complémentarité des stratégies nationales et européennes, la dimension européenne venant en complément et non en concurrence du niveau national. Encore faut-il avoir analysé et fait ses propres choix capacitaires, s'approprier, pérenniser, renforcer certaines compétences de savoir et de savoir-faire.

Une telle analyse doit se faire sur toute la chaîne de valeur du numérique : maîtrise des technologies ; maîtrise de la production de ces technologies, des produits et services associés ; maîtrise de la vente et de la distribution des produits et services. Ces 3 dimensions sont à considérer, de la même manière qu'une maison a des fondations, des murs, et un toit.

La maîtrise des technologies numériques doit s'analyser suivant les différentes couches suivantes, un peu comme dans le modèle OSI :

- Électronique, matériels (disponibilité des matières premières, une filière de recyclage adaptée pouvant dégager des marges de manœuvre, conception et fabrication de composants clés) ;
- Infrastructures réseaux (intégrité des câbles sous-marins et terrestres, fibres, poteaux et antennes, 4G/5G/6G, satellites…) ;
- Logiciels systèmes d'exploitation ;
- Environnements collaboratifs, Cloud ;
- Plates-formes d'accès ;
- Logiciels métier.

Mais si la maîtrise de certaines technologies est clé pour garantir la capacité à utiliser certains moyens d'action, encore faut-il savoir les produire, et ensuite les distribuer et en rendre possible l'accès. Sans répéter ce que j'ai déjà dit, comme il paraît difficile de maîtriser tout seul tous les maillons de cette chaîne de valeur, c'est la complémentarité des stratégies nationales qui peut contribuer à crédibiliser les souverainetés nationales au sein d'une logique de mutuelle dépendance assumée, mais maîtrisée.

Avant de conclure, je voudrais illustrer les différentes notions pour les rendre moins théoriques, moins nébuleuses, d'où quelques mots sur le nuage, le Cloud. Je sais que c'est un sujet quelquefois délicat, 2009 est toujours dans les esprits, mais c'était il y a plus d'une décennie ! 2009 c'est l'Iphone3. Cela vous semble loin : eh bien NumEnergy et CloudWatt aussi. Et puis, Apple aussi a eu des échecs avec son Apple III (l'ordinateur sans ventilateur interne), son système d'exploitation Copland, son organisateur portable Newton, Microsoft a eu Vista. Apprenons de nos échecs au lieu de toujours sombrer dans la palingénésie mortifère.

Donc, Cloud de confiance, Cloud résilient, Cloud souverain, qu'en est-il ?

Déjà, si je peux me permettre une pointe d'humour, il est assez ironique de voir apparaître dans différents pays des labels de « Cloud de confiance », ou de « Trusted Cloud », au même moment où on parle aussi tout autant de « zero-trust » ! Ironique en effet de voir que l'outil ne me fait pas confiance à moi en tant qu'usager, mais moi je dois avoir confiance dans l'outil. Pourtant la confiance devrait être une relation à deux en principe…

Le label de confiance se base d'une part sur un ensemble d'exigences de SecNumCloud (sécurité physique, habilitation des personnels, contrôle d'accès et gestion des identités, mise

en œuvre de techniques de chiffrement, définition de processus de sécurité pour l'exploitation, règles régissant les relations avec des tiers), et d'autre part sur une localisation des infrastructures et systèmes en Europe, vue comme une réponse à la connectivité transfrontalière et aux législations liées à l'extra-territorialité. Ceci permet en fait *de facto* et *de jure* le partage commercial et opérationnel par une entité européenne de solutions technologiques qui ne le sont pas. En fait la confiance est reliée à l'usage de l'objet, mais pas l'objet lui-même.

Par ailleurs les labels de confiance, s'ils traitent les données dites au repos, ne s'appliquent pas a priori aux données en transit en fonctionnement courant, par exemple pour la maintenance ou la résolution d'incident.

Même s'il y a chiffrement chez l'hébergeur, et chiffrement des transports (par SSL via https par exemple, ou par IPSEC si on est sur ligne dédiée entre le système d'information et les serveurs hébergés), il n'y a pas de garantie systématique de bout en bout sans couture.

Peut-on alors réellement parler de résilience, si l'on revient à l'analyse de risques qui prévaut à la définition de la résilience ? et a fortiori de souveraineté ?

Si l'on regarde maintenant les « trusted Clouds », avec la certification « tier IV », ce sont des exigences de redondance (au niveau des datacenters, ainsi que de l'approvisionnement eau et énergie). Rien à voir avec la souveraineté et l'autonomie stratégique, mais par contre cela contribue à la résilience.

Donc le Cloud de confiance n'est pas souverain et n'est pas résilient, le « trusted Cloud » n'est pas de confiance mais est résilient. Et vous allez me dire : « comment je définis le Cloud souverain ? ». Je réponds : suivant les 3 dimensions de la chaîne de valeur dont j'ai parlées, donc maîtrise des technologies, de leur production, de leur distribution pour accès au consommateur.

En complément de ce point de vue personnel, je rajouterais que si l'on veut avoir un véritable Cloud souverain, je pense qu'il faut investir, au niveau industriel privé, avec une logique de rentabilité assez rapide garantie par un usage payant de la part de la puissance publique, usage accompagné par une politique incitative. Ce n'est pas irréalisable, et on pourrait dégager des montants financiers réalistes. Typiquement, si l'on regarde l'ensemble de la fonction publique, on a de l'ordre de 5,5 millions d'agents, tant dans les ministères que dans les collectivités territoriales et la fonction hospitalière.

Partons sur une base de 3 millions d'agents dont on peut estimer que l'outil de travail repose en partie sur le numérique et aurait à gagner d'un Cloud. En gros cela représente les

catégories A et B, ou alors une grande partie des fonctionnaires, ou alors grosso modo les ministères et collectivités territoriales.

Si l'on imagine un coût mensuel par agent de 50 euros (ce qui est largement inférieur à certains coûts moyens d'outils logiciels de base aujourd'hui dépensés dans un certain nombre d'administrations, et ce qui est inférieur à ce que dépense en moyenne un Français chez lui pour les différents services d'abonnements pour Internet, la téléphonie, et les plates-formes de films), cela donne sur une période de 5 ans (une présidence, un peu moins qu'une loi de programmation militaire, une durée standard de vie dans le monde informatique) une somme de 9 milliards d'euros. C'est beaucoup ? oui et non. Regardez l'investissement annuel de Google.

Une telle somme pourrait donc amortir sur la période un investissement permettant de mettre en place des infrastructures de transport résilientes, protégées, maîtrisées, ainsi qu'un Cloud digne de ce nom avec infrastructures et services, maîtrisé de bout en bout, permettant la souveraineté numérique au niveau national.

Vous allez m'objecter le fait qu'un Cloud c'est bien beau, mais qu'il faut l'utiliser pour ne pas retomber dans les échecs passés. Qu'à cela ne tienne : en plus d'une politique un peu plus incitative, pour ne pas dire aussi un peu plus coercitive, de « Cloud au centre », pourquoi ne pas avoir un accompagnement via une offre commerciale ciblée sur cette population de la fonction publique, par exemple en plus de l'usage professionnel payé par ailleurs, en offrant à chacun « gratuitement » la capacité « à la maison » pour son usage personnel. Cela donne alors 5 voire 10% de la population française (si l'on prend cette fois toute la fonction publique dans son ensemble) servie, manque à gagner certain sur le papier, mais potentiellement c'est un réel levier de changement disruptif. Et si c'est gratuit à la maison, cela sera utilisé, et cela motivera l'utilisation au travail. Le gratuit, Google l'a fait.

Un acteur unique peut-il mettre en place ces infrastructures de transport résilientes, protégées, maîtrisées, ainsi qu'un Cloud digne de ce nom avec infrastructures et services, maîtrisé de bout en bout ? Assurément non. Mais un groupement économique le pourrait, rassemblant quelques acteurs industriels motivés, petits, moyens, gros, jouant collectif, capables de tenir leurs engagements de coopération dans la durée.

Rassembler les forces vives de maîtrise d'œuvre est clé pour faire face à ces enjeux ; il en est de même des investissements publics.

Certes les politiques actuelles d'investissement ne sont pas encore tournées vers ce modèle d'investissement constructif (construire une compétence ciblée), mais sont actuellement davantage tournées vers des politiques d'investissement dynamique avec les plans

de relance, les programmes d'investissements d'avenir, qui arrosent et nourrissent un large écosystème.

Pour prendre une analogie, c'est la différence entre fertiliser un terrain et cultiver un verger. Il faut évidemment le premier pour avoir le second, mais le second ne se fait pas sans stratégie, sans choix délibéré, les finalités et les résultats sont fondamentalement différents.

Dans le cas présent, je pense que c'est donc ce qu'il faudrait faire.

Comme mot de fin, ce qui est en jeu c'est notre capacité à décider et notre capacité à agir. Dans le domaine militaire, ce sont respectivement d'un côté la capacité d'anticipation et de renseignement ainsi que les processus décisionnels, de l'autre les forces et les capacités industrielles de recherche et de maîtrise des technologies pour les armements. Il en est de même dans le domaine du numérique ou de la cyber, ce n'est que l'outil qui n'est pas nécessairement le même. Comme le souligne le SGDSN, la capacité autonome d'appréciation, de décision, d'action dans le domaine cybernétique, tout en protégeant les autres composantes, permet de conserver la maîtrise de son destin dans l'espace numérique.

La construction d'une souveraineté numérique nationale, amplifiée par la dynamique européenne, doit être le fruit d'une ambition politique forte. Le cadre européen doit être considéré de façon pragmatique : il est le niveau d'efficience à mobiliser au service de la vision du numérique que portent ses Etats membres et de la défense des intérêts numériques européens.

Je vous remercie.