MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

Liberté
Égalité
Fraternité

DIRECTION DES RESSOURCES HUMAINES

SOUS-DIRECTION DE L'ATTRACTIVITÉ ET DES RECRUTEMENTS

Bureau des concours et examens professionnels

Concours externe et interne pour le recrutement dans le grade d'attaché des systèmes d'information et de communication au titre de l'année 2026

Épreuve écrite d'admissibilité n°1

Lundi 16 février 2026

Note de synthèse

Durée totale de l'épreuve : 3 heures - Coefficient : 2
Toute note inférieure à 6 sur 20 est éliminatoire.

Épreuve consistant en une note de synthèse, établie à partir d'un dossier à caractère scientifique et technique, de quarante pages maximum, permettant de vérifier les qualités d'expression, d'analyse et de synthèse du candidat dans les domaines scientifiques et techniques, ainsi que son aptitude à dégager des conclusions et à formuler des propositions

Ce dossier comporte 35 pages (page de garde, sujet et sommaire non compris)

Sommaire

Sujet

La directrice du numérique du ministère de l'Europe et des Affaires étrangères vous demande un point de situation sur la souveraineté numérique et ses possibles mises en œuvre au sein du ministère. Vous lui proposerez une synthèse des documents suivants ainsi qu'une courte proposition de pistes applicables pour le ministère.

Document 1 : Souveraineté numérique

Auteur(s) : Sciences Po

Source : Site Internet https://www.sciencespo.fr, consulté le 20/01/2026

L'expression de « souveraineté numérique » paraît renvoyer à la capacité des États d'agir dans le cyberespace et de faire respecter leurs règles par les différents acteurs du monde virtuel. A cet égard, cette notion permet d'exprimer les difficultés des Etats à assumer leurs fonctions traditionnelles face à des acteurs transnationaux puissants et dotés d'une avance technologique indiscutable, dont ils sont parfois dépendants car ils ont besoin de la technologie pour pouvoir accomplir leurs missions régaliennes. Ainsi, l'expression de « souveraineté numérique » comporte indiscutablement un aspect juridique puisqu'elle renvoie aux prérogatives de l'État et à sa capacité de réguler les géants technologiques contemporains. Mais elle est également dotée d'un versant économique et industriel en ce qu'elle traduit la nécessité de rattraper un retard technologique qui place l'Europe et la France en situation de dépendance.

Document 2 : Pourquoi Tchap ?

Auteur(s) : DINUM

Source : Site Internet https://tchap.numerique.gouv.fr, consulté le 19/01/2026

Dans le cadre de la transformation numérique de l'État et des organisations publiques, le choix d'une solution de messagerie sécurisée souveraine est un enjeu majeur. Tchap se présente comme une réponse idéale, alliant sécurité, souveraineté et efficience pour répondre aux besoins de l'Administration. Sur cette page, vous trouverez les points différenciants de Tchap par rapport aux autres outils disponibles sur étagère.

Confidentialité des échanges

Tchap assure une confidentialité optimale des échanges professionnels grâce à des protocoles de sécurité avancés, protégeant les données, sensibles ou non, des agents et des institutions contre toute intrusion ou compromission, un impératif face à une multiplication des risques et à la faible maitrise des données transitant par des services privés.

Souveraineté et autonomie stratégique

Développée et hébergée en France, Tchap garantit une souveraineté numérique totale, échappant aux législations extraterritoriales comme le Cloud Act, et offre une autonomie stratégique en éliminant la dépendance aux solutions étrangères et à des acteurs privés, renforçant ainsi la résilience de l'État et de l'action publique face aux enjeux géopolitiques actuels.

Maîtrise des coûts

En maintenant des prix bas de développement et d'opération, sans coût direct pour les administrations, Tchap optimise les finances publiques via une mutualisation efficace, évitant les dépenses élevées des alternatives externes tout en répondant aux besoins en termes de messagerie instantanée avec une solution économique et pérenne.

Construit par et pour les agents publics

Conçu par et pour les agents publics, Tchap vise à répondre aux besoins spécifiques de ces derniers, avec une maîtrise interne des évolutions définies en fonction de retours terrain. Des mises à jour pertinentes sont régulièrement mises en ligne, tandis que son annuaire intégré décloisonne les administrations, fluidifiant les échanges interservices pour une collaboration renforcée dans le secteur public.

Une solution libre, financée par l'Administration

Basé sur un protocole Matrix, Tchap s'appuie sur une technologie open-source, garantissant une transparence totale dans son code et son fonctionnement. Cette approche favorise la confiance et

la sécurité de ses utilisateurs, tout en permettant des évolutions adaptées aux besoins spécifiques des agents publics. Financé par la DINUM, Tchap incarne un investissement stratégique dans une infrastructure numérique souveraine, évitant les coûts récurrents et les dépendances à des licences propriétaires. Ce modèle collaboratif encourage également l'innovation, en permettant à la communauté des utilisateurs de Tchap de contribuer à son amélioration continue, assurant ainsi une solution pérenne, évolutive et alignée sur les valeurs.

Une messagerie sécurisée

Tchap est une messagerie sécurisée développée par l'État français, réservée aux agents de la fonction publique. Elle permet des échanges rapides et efficaces tout en assurant un haut niveau de sécurité et de confidentialité des données.

Conçue pour répondre aux besoins spécifiques des services publics, Tchap garantit la protection des informations et respecte la souveraineté numérique de l'État.

Des messages 100% privés et sécurisés

- Les échanges sur Tchap sont chiffrés de bout en bout entre les appareils des participants.
- Seuls les membres d'une conversation peuvent lire les messages.
- Les serveurs par lesquels les messages transitent ne peuvent pas les déchiffrer.
- Le chiffrement empêche également les administrateurs techniques d'accéder au contenu des discussions.

Un accès limité aux agents publics

- Il faut une adresse professionnelle (@gouv.fr, etc…) pour s'inscrire, et l'équipe Tchap (DINUM) se charge de valider les noms de domaines autorisés.
- La création du compte est confirmée par un lien reçu par email.
- Un "mail de vie" est envoyé une fois par an pour vérifier que l'agent est toujours en poste. Sinon, le compte est supprimé.

Des échanges avec l'extérieur encadrés

Il est possible d'inviter des personnes extérieures (prestataires, partenaires), mais :

- Uniquement dans des salons précis, ouverts aux externes
- Avec des droits limités (les externes ne peuvent pas créer et administrer un salon, inviter des membres sur un salon, accéder à l'annuaire).

Un contrôle total des appareils connectés

- La liste des appareils connectés à un compte est consultable à tout moment.
- En cas de perte d'un téléphone ou d'un ordinateur, il est possible de le déconnecter à distance.
- Lorsqu'un nouvel appareil est utilisé pour se connecter, une vérification d'identité est requise.

Des messages protégés, même après un changement d'appareil

- La récupération des messages nécessite la saisie d'un code secret connu uniquement de l'utilisateur.
- Ce code n'est enregistré ni sur l'appareil, ni sur les serveurs.

Un outil souverain, transparent et fiable

- Tchap est hébergé en France, sur une infrastructure de l'État.
- Il est développé par des équipes publiques de l'État (DINUM).
- Son fonctionnement est 100% transparent : le code est open-source.
- Personne ne peut lire vos messages en dehors de leurs destinataires.

Document 3 : SecNumCloud en (pas si) bref

Auteur(s) : Vincent STRUBEL, Ingénieur général des mines, directeur de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Source : Post LinkedIn – 6 janvier 2026

La qualification SecNumCloud, fin 2025, d'une première offre de cloud dite "hybride" - c'est-à-dire reposant sur une technologie cloud américaine opérée par un prestataire européen – a fait couler beaucoup d'encre virtuelle. Elle a surtout révélé en creux quelques incompréhensions persistantes sur ce que fait ou ne fait pas SecNumCloud. Le moment semble opportun pour quelques rappels, sur ce qu'est la qualification SecNumCloud, ce contre quoi elle protège, et ce qui ne relève pas de son champ.

N.B. : la distinction formelle souvent opérée entre offres "hybrides" et "non hybrides" a quelque chose d'assez artificiel, car le sujet des dépendances technologiques ne se prête pas à une lecture binaire. Mais je reprendrai ici ce terme d'"hybride" pour la simplicité de lecture.

Qu'est-ce que SecNumCloud ?

SecNumCloud est une qualification délivrée par l'ANSSI, autorité nationale de cybersécurité, attestant qu'un service de cloud présente un haut niveau de sécurité, adapté aux usages sensibles de l'Etat et des entreprises françaises.

Cela implique plusieurs principes fondamentaux, qui échappent parfois aux commentateurs pressés :

- La qualification d'une offre n'est ni une décision arbitraire, ni un choix politique : elle découle d'un processus formalisé d'évaluation de la sécurité de la solution candidate, sur la base des exigences du référentiel SecNumCloud ; les règles, le processus et le niveau d'exigence sont les mêmes pour tous ;
- La qualification apporte des garanties de cybersécurité, c'est-à-dire une assurance de couverture au juste niveau de l'ensemble des risques qui pourraient affecter la solution : de nature technique (i.e. le risque de cyberattaques au sens premier du terme), juridique (droit applicable aux données) ou organisationnel (dont les risques d'accès illégitimes par un employé du prestataire) ;
- Elle correspond au besoin de sécurité d'usages sensibles du cloud, et n'a pas vocation à s'appliquer à tous les cas d'usage. Une solution cloud "standard", quel que soit son fournisseur, ne satisfait en général pas les exigences de SecNumCloud.

Concrètement, cela se traduit par une procédure de qualification longue et exigeante, dans laquelle près de 1200 exigences ("points de contrôle") seront vérifiées *in situ* par un évaluateur indépendant, agissant sous le contrôle de l'ANSSI, qui ne se prive pas au demeurant de demander parfois à l'évaluateur d'approfondir son travail, ou de réévaluer de manière plus stricte ses conclusions. On peut également noter que les exigences, et la doctrine d'évaluation, ont désormais plus de dix ans (le premier référentiel SecNumCloud a été publié en juillet 2014) et ont été actualisées constamment au gré des retours d'expérience, de l'évolution des technologies et de notre meilleure compréhension des risques.

Bref, ce n'est pas une médaille en chocolat, et ce n'est pas pour tout le monde… Mais quels sont les risques couverts ?

Les risques liés au droit extraterritorial

Ce sont ceux dont on parle le plus (mais pas les seuls, voir plus bas). Il ne s'agit évidemment pas de se soustraire à l'application du droit, mais de garantir que les données et applications hébergées dans le cloud ne sont pas soumises à des dispositions qui ne relèvent pas du droit européen, contre lesquelles les clients européens du cloud n'auraient pas de voies de recours, et qui menaceraient la confidentialité, l'intégrité ou la disponibilité de ces données et applications.

SecNumCloud impose à ce titre plusieurs choses (principalement au chapitre 19 du référentiel) :

- Le prestataire qualifié doit être européen, en termes de siège social et de capitalisation ;
- S'il a recours à des sous-traitants ou fournisseurs non européens, il doit garantir que ces derniers n'ont en aucun cas accès aux données de ses clients ;
- Il doit être autonome dans l'exploitation de la solution : cela ne signifie pas que le prestataire a écrit 100% du code qui tourne dans son cloud, mais qu'il est capable de le faire tourner avec ses ressources et compétences propres, sans intervention extérieure.

Ces exigences permettent d'apporter des garanties utiles pour la cybersécurité des données et des applications, sans prétendre répondre à toutes les questions de dépendances.

SecNumCloud protège contre l'accès extraterritorial aux données

C'est souvent le premier risque auquel on pense : des prestataires numériques (pas que dans le cloud d'ailleurs) non européens peuvent se voir imposer, par les autorités de leur pays d'origine, de fournir les données de leurs clients y compris européens, sans voie de recours ni même information des clients ou des Etats tiers concernés. C'est *a minima* prévu par le CLOUD Act ou les lois FISA américaines, par la loi chinoise sur le renseignement de 2017, et pourrait exister dans d'autres cadres légaux.

SecNumCloud protège contre ce risque, en attestant que seul un prestataire européen dispose du contrôle des données (au sens des termes *possession, custody or control* présents par exemple dans le CLOUD Act). Nous estimons que ce critère, et ce qu'il implique sur la localisation des dirigeants et l'origine des capitaux, offre une bonne garantie que le prestataire ne suivra pas une injonction d'une autorité non européenne affectant ses clients européens, en tout cas pas sans la contester en en référant aux autorités nationales et européennes.

Cela n'empêche pas d'avoir recours à des sous-traitants ou fournisseurs non européens, mais SecNumCloud garantit dans ce cas qu'ils n'ont pas accès aux données, et que leur exposition au droit extraterritorial est donc sans conséquence sur la sécurité de ces dernières. C'est vrai même dans le cadre d'une offre "hybride" qualifiée : le fournisseur de la technologie cloud est soumis aux lois américaines, mais n'a pas accès aux données et ne peut par conséquent pas donner suite à une injonction.

SecNumCloud protège contre le scénario du kill switch

Un autre risque extraterritorial a été remis en lumière par l'actualité récente : celui de voir des prestataires non européens contraints de couper le service qu'ils fournissent à certains de leurs clients, en fonction de sanctions ou de restrictions d'exportations imposées par le pays d'origine de ces prestataires. C'est ce qu'ont notamment vécu récemment certains magistrats de la Cour Pénale Internationale.

Là aussi, SecNumCloud offre une protection contre ce risque de coupure brutale : le prestataire européen n'est pas tenu de donner suite à une injonction de cette nature, et pour être qualifié il a dû démontrer son autonomie dans l'exploitation de la technologie. Un sous-traitant non européen du prestataire ne dispose donc pas de la capacité à couper le service à tel ou tel client, car ce n'est pas lui qui administre la solution et ses utilisateurs. C'est tout aussi vrai pour une offre "hybride" que "non hybride".

Mais SecNumCloud ne signifie pas l'absence de dépendance

Une qualification SecNumCloud ne signifie pas que le prestataire de cloud peut opérer à long terme en autarcie complète, sans s'appuyer sur des fournisseurs non européens ni disposer de mises à jour fournies par des tiers. Une coupure de l'accès à ces fournisseurs, et aux mises à jour associées, entraînerait une dégradation progressive du niveau de sécurité.

Une offre SecNumCloud dite "hybride" est sans doute plus exposée à ce risque, mais ce n'est pas un choix binaire : toutes les offres de cloud, "hybrides" ou non, dépendent de composants électroniques (CPU, GPU, etc.) et logiciels (systèmes d'exploitation, bases de données, couches d'orchestration, …) dont la conception ou la mise à jour ne sont pas maîtrisées à 100% en Europe. L'utilisation de briques *open-source* apporte indiscutablement une plus grande liberté d'action et une meilleure maîtrise potentielle (pour peu qu'on s'en donne les moyens), mais elle n'est pas pour autant la panacée : aucun acteur, Etat ou entreprise, ne maîtrise entièrement, et ne peut prétendre *forker* et maintenir en autarcie toute la *stack* technologique du cloud, depuis le noyau Linux jusqu'à Openstack, PostgreSQL etc., en passant par les milliers de modules python, javascript ou autre sans lesquels rien de tout cela ne fonctionne vraiment.

Bref, il est évident que si nous sommes un jour privés de l'accès à la technologie américaine, chinoise, ou plus généralement non européenne, nous aurons un problème global de dégradation du niveau de sécurité en l'absence de mises à jour, dans le cloud comme ailleurs. Mais imaginer que ce problème serait limité aux offres de cloud "hybrides", ou même d'ailleurs aux seules offres de cloud, est une pure vue de l'esprit qui ne résiste pas à la confrontation aux faits. Le traitement des risques liés à nos dépendances dans le cloud, mais aussi dans le numérique de manière plus générale, est un chantier qui dépasse très largement le seul cadre SecNumCloud. Et le fait de monter en compétence dans notre capacité à exploiter, en Europe, des technologies américaines, est en soi un progrès dans la prise en compte de ces dépendances.

Et la localisation dans tout ça ?

SecNumCloud impose également la localisation des données au sein de l'Union européenne. Il est évident que cette localisation ne protège pas à elle seule du droit non européen à portée extraterritoriale (c'est même pour ça qu'on l'appelle "extraterritorial"…).

En revanche, c'est une disposition complémentaire indispensable, pour assurer que les infrastructures physiques qui hébergent les données sont soumises au droit européen, et pas exposées par exemple au pouvoir de réquisition de tiers qui ne seraient pas régis par ce droit.

C'est également une mesure utile pour un éventuel traitement d'incident, pour faciliter l'intervention de prestataires de réponse à incident européens, ou des services étatiques compétents comme le CERT-FR de l'ANSSI. Ces différents "cyberpompiers" peuvent théoriquement intervenir hors des frontières européennes, mais c'est généralement beaucoup plus compliqué, avec des délais incompressibles peu adaptés à une situation de crise.

Les autres risques

Les risques liés au droit extraterritorial sont ceux dont on parle le plus, mais de loin pas les seuls qui doivent être pris en compte dans l'usage du cloud. Dans le référentiel SecNumCloud, les critères liés à la nationalité du prestataire, à sa gestion des sous-traitants non européens ou à son autonomie d'exploitation ne représentent qu'une petite partie des exigences.

Les prestataires de cloud, quelle que soit leur nationalité, sont pour les cyber attaquants de tout poil des cibles à très haute valeur ajoutée. Ils subissent en permanence des tentatives d'attaque, y compris particulièrement avancées, dont certaines réussissent forcément, aussi bien chez les *hyperscalers* non européens que chez les prestataires européens. Ces cyberattaques demeurent la menace la plus tangible pesant sur les usages sensibles du cloud.

C'est pour contrer cette menace que le référentiel SecNumCloud impose des exigences très contraignantes sur l'architecture et les caractéristiques techniques du cloud : cloisonnement fort entre les différents clients, chaîne d'administration et de supervision isolée du reste, gestion sécurisée des mises à jour, chiffrement systématique des données *at rest* et en transit, etc. Ces exigences répondent directement aux différentes menaces connues par l'ANSSI, et sont adaptées à des cas d'usage sensibles. Il est important de noter qu'elles ne sont généralement pas toutes satisfaites par une offre de cloud standard, quelle que soit son origine.

Par ailleurs, le risque humain doit aussi être pris en compte pour des infrastructures aussi stratégiques que le cloud. Il est parfaitement vraisemblable qu'un acteur malveillant parvienne à obtenir, par corruption, contrainte ou infiltration, la coopération d'employés d'un prestataire de cloud pour accéder aux données de ses clients ou compromettre la disponibilité ou l'intégrité de celles-ci.

C'est pour répondre à cette menace que le référentiel SecNumCloud consacre un chapitre entier à la gestion des ressources humaines du prestataire, et impose par ailleurs un certain nombre d'exigences techniques pour garantir qu'aucun employé du prestataire ne peut porter une atteinte grave à la sécurité du service de cloud sans être détecté.

Ces autres menaces sont souvent passées sous silence dans un débat passionné qui se concentre sur la question du droit extraterritorial. Mais on ne les ignore qu'à ses risques et périls…

Quelques FAQ pour conclure

Un certain nombre de questions reviennent régulièrement sur la table au sujet de SecNumCloud. Tentons d'y apporter quelques éléments de réponse, quitte à répéter certains des points précédents.

Est-ce que SecNumCloud est un label de souveraineté ?

Il est dans l'absolu difficile de répondre à cette question, vu que le concept de souveraineté numérique n'est quasiment jamais défini, et que tout le monde lui donne un sens différent, voire une interprétation arbitraire et circonstancielle peu ancrée dans l'objectivité.

Mais vu de l'ANSSI, la notion de souveraineté numérique renvoie à au moins trois enjeux distincts et complémentaires :

1. Ne pas être une victime facile dans nos usages numériques, à la merci de la première cyberattaque venue ;
2. Faire appliquer nos règles, plutôt que subir celles des autres sans avoir voix au chapitre ni possibilité de recours ;
3. Disposer d'une liberté de choix éclairé et d'usage dans le recours aux technologies indispensables à nos missions (en disposant de solutions européennes, en maîtrisant des briques *open-source*, ou en s'appuyant sur une diversité d'offres suffisantes pour ne pas être dans une dépendance critique).

Par rapport à cette définition, SecNumCloud répond directement aux enjeux 1 et 2 : il garantit une bonne protection contre les cyberattaques et l'application exclusive de notre droit, national et européen. Il contribue également au troisième enjeu, en permettant un choix éclairé sur la base d'une évaluation approfondie des offres du marché, par une tierce partie neutre. ***Les offres qualifiées SecNumCloud sont donc, sans le moindre doute, "souveraines", et cette qualification est un levier indispensable pour défendre notre souveraineté numérique.***

Mais cette qualification ne va en revanche pas faire naître des solutions alternatives ou des briques technologiques maîtrisées pour résoudre toutes les questions de dépendances. Elle n'a pas vocation à le faire : c'est un outil de cybersécurité, pas de politique industrielle. Il faut indiscutablement des actions complémentaires pour soutenir le développement d'offres et de technologies cloud européennes, qui ne sont pas du ressort d'une qualification de cybersécurité.

Est-ce que les offres "hybrides" qualifiées offrent le même niveau de garanties ?

Oui, elles satisfont exactement les mêmes exigences que les autres.

Dans une offre "hybride" qualifiée, le prestataire doit être européen, et garantir son étanchéité et son autonomie d'exploitation par rapport au fournisseur de la technologie qu'il opère, comme dans une offre "non hybride". Il n'est pas forcément en mesure d'assurer la maintenance dans la durée de sa solution s'il est privé de tout accès à la technologie non européenne, mais les offres "non hybrides" sont également soumises à ce risque fondamental, même si leurs dépendances peuvent être moindres, plus réparties ou plus complexes à identifier.

De fait, la différence entre offre "hybride" et offre "non hybride" est assez artificielle : il n'y a pas d'un côté des offres totalement dépendantes de fournisseurs non européens et de l'autre des offres 100% européennes. Tous les fournisseurs de cloud dépendent - à un niveau certes variable - de composants électroniques et de logiciels qu'ils ne maîtrisent pas à 100% et qui ne sont pas européens.

Pourquoi ne pas faire un label reprenant uniquement les critères capitalistiques, sans les exigences techniques ?

Cette demande revient souvent, pour faire un SecNumCloud "pas cher" couvrant juste les enjeux de droit applicable. Mais du point de vue de la cybersécurité, ça n'aurait aucun sens de couvrir uniquement certaines menaces, et pas d'autres. Une solution adaptée aux cas d'usage sensibles que vise SecNumCloud doit couvrir tous les risques, car les attaquants visent toujours le maillon faible. Un cloud échappant au droit non européen, mais à la merci des cyberattaques, ça n'a pas plus de sens qu'une maison avec des volets blindés et des barreaux aux fenêtres, mais dont la porte serait fermée par un rideau.

Par ailleurs, les critères techniques de SecNumCloud sont fondamentalement indissociables des exigences de nationalité, car ils garantissent l'étanchéité du prestataire et son autonomie d'exploitation vis-à-vis de ses sous-traitants et fournisseurs. En leur absence, on ne peut pas garantir que les données confiées à un prestataire européen ne seront pas également accessibles à un sous-traitant non européen, soumis à du droit extraterritorial.

Appliquer une préférence européenne dans le choix de prestataires cloud, cela a évidemment un sens en termes de politique industrielle, mais ce n'est pas le rôle de SecNumCloud.

Pourquoi ne pas faire *a contrario* un label uniquement technique ?

Même réponse qu'au point précédent : mettre une porte blindée et une serrure 5 points à sa maison, mais laisser les fenêtres ouvertes en sortant de chez soi, ça n'a pas de sens non plus.

Or il est impossible de couvrir les risques liés au droit applicable par des exigences purement techniques. Le chiffrement des données par exemple, ne protège pas du CLOUD Act : le prestataire de cloud a forcément, tôt ou tard, accès à la clé de chiffrement (ou alors ce n'est pas du cloud, mais du stockage en ligne sans traitement…). Même les approches de *confidential computing* ne permettent pas, dans notre analyse à date, de couvrir ces risques. Les critères d'implantation et de structuration capitalistique du chapitre 19 du référentiel SecNumCloud sont à date le seul moyen identifié de couvrir le risque lié au droit non européen.

Document 4 : Souveraineté numérique : Pourquoi Airbus, Dassault Systèmes, Orange, OVHcloud et 7 autres champions européens font alliance

Auteur(s) : Julien Bergounhoux

Source : L'usine digitale, 20 novembre 2025

Onze grandes entreprises européennes, dont cinq françaises, se réunissent pour pousser l'Union européenne à définir clairement le concept de "cloud souverain" et à instaurer une politique de préférence européenne pour l'achat public lorsqu'il question du traitement de données sensibles.

A l'occasion du Sommet sur la souveraineté numérique européenne, onze entreprises européennes, dont cinq françaises, se sont réunies pour annoncer l'European Sovereign Tech Industry Alliance (ESTIA) ce 20 novembre. Il s'agit d'A1 Digital, Airbus, Dassault Systèmes, Deutsche Telekom, evroc, OpenNebula Systems, Orange, OVHcloud, Post Luxembourg, Schwarz Digits, Sopra Steria et Telecom Italia. La structure sera officiellement lancée en 2026.

L'objectif de cette alliance ? Coordonner les efforts pour promouvoir l'autonomie stratégique de l'Union européenne dans les domaines du cloud et des services numériques. Dassault Systèmes y figure au nom de sa filiale Outscale, tandis qu'Orange et OVHcloud y représentent leurs business cloud respectifs. Sopra Steria est concerné en tant qu'intégrateur et gestionnaire de systèmes sensibles voire critiques, notamment dans la finance.

Favoriser les acteurs cloud européens pour les achats publics

Au travers d'un engagement baptisé l'European Sovereign Cloud Pledge, le groupe promet notamment de faire inscrire une définition juridique claire de ce qu'est le "cloud souverain" dans le futur Cloud and AI Development Act (CAIDA). D'après Sopra Steria, elle sera inspirée du standard EUCS High+ et aura pour but de garantir la localisation des données et leur protection contre les lois extraterritoriales. Seul problème : ce schéma européen de certification cloud est aujourd'hui dans une impasse car plusieurs pays, dont l'Allemagne, refusent d'appliquer les critères demandés par la France (qui protègent justement contre les lois extraterritoriales).

Autre objectif d'Estia : faire instaurer un principe de préférence européenne dans la commande publique pour le cloud. Il faut dire que, pour tous leurs discours sur l'économie de marché, les Etats-Unis n'auraient jamais l'idée de faire appel à des acteurs étrangers pour héberger les données du secteur public. La France ne peut pas en dire autant. Ni l'Union européenne dans son ensemble, puisque d'après le rapport Draghi, 90% des données européennes sont transférées hors de l'UE.

Document 5 : Sommet sur la souveraineté numérique européenne : des engagements emblématiques pour une Europe plus compétitive et souveraine.

Auteur(s) : Communiqué de presse conjoint de la France et de l'Allemagne du 18/11/2025

Source : Site de l'ambassade de France au Royaume-Uni (https://uk.diplomatie.gouv.fr), publié le 20/11/2025

Le Sommet sur la souveraineté numérique européenne s'est tenu à Berlin le 18 novembre. Il a réuni plus de 900 décideurs, industriels, investisseurs, chercheurs et représentants de la société civile provenant des 27 États membres de l'Union européenne (UE) et des institutions européennes.

Le Sommet a été l'occasion de présenter des mesures concrètes afin de favoriser des infrastructures et des solutions innovantes au niveau européen et de renforcer notre résilience tout en réduisant nos dépendances technologiques et en protégeant nos avoirs stratégiques. La France et l'Allemagne ont ciblé sept domaines stratégiques prometteurs pour stimuler la compétitivité européenne et bâtir la souveraineté numérique de l'UE.

Simplification : la France et l'Allemagne réaffirment leur volonté d'élaborer un cadre réglementaire de l'UE qui soit simple, compétitif et favorable à l'innovation. En particulier, elles appellent à un moratoire de 12 mois sur les dispositions du règlement sur l'intelligence artificielle (IA) relatives aux systèmes d'IA à haut risque et elles demandent instamment à la Commission européenne d'intégrer la simplification souhaitée du règlement général sur la protection des données (RGPD) dans le train de mesure sur le numérique.

Des marchés numériques plus justes : des conditions réglementaires justes, contestables et compétitives sont indispensables pour permettre le développement d'une offre européenne sur les marchés numériques stratégiques. La France et l'Allemagne se félicitent de la décision de la Commission européenne de lancer une enquête de marché sur la désignation qualitative des hyper-échelles en nuage.

Souveraineté des données : la sauvegarde des données les plus sensibles et le contrôle des technologies numériques sont indispensables pour favoriser la stabilité et la croissance économiques ainsi que l'innovation en Europe. Ensemble, la France et l'Allemagne appellent la Commission européenne à définir des normes de protection extrêmement strictes pour les données les plus sensibles, notamment des normes adéquates pour protéger les données face aux risques relevant de la cybersécurité, en particulier les effets de législations extraterritoriales adoptées hors de l'UE et l'utilisation obligatoire de technologies protégeant mieux la vie privée, s'approchant au plus près du cadre européen de la cybersécurité.

Communs numériques : la France et l'Allemagne soutiennent le développement des communs numériques en créant avec les Pays-Bas et l'Italie le consortium pour une infrastructure numérique européenne - communs numériques.

Infrastructures numériques publiques et outils de source ouverte pour l'administration publique : la France et l'Allemagne soutiennent fermement le développement du portefeuille européen d'identité numérique qui constitue un moyen protégé, fiable et sûr d'identification numérique pour les citoyens européens et la clé de voûte de la souveraineté numérique de l'Europe. La France et l'Allemagne s'engagent également à développer l'utilisation des outils de source ouverte dans leurs

administrations en s'appuyant par exemple sur le succès des produits LaSuite/OpenDesk qu'ils ont développés conjointement.

Groupe de travail sur la souveraineté numérique : la France et l'Allemagne lancent un groupe de travail conjoint sur la souveraineté numérique européenne. Ce groupe de travail œuvrera à la définition commune de services numériques européens. Il concevra également des indicateurs de souveraineté en mettant l'accent sur des secteurs essentiels tels que les services en nuage, l'intelligence artificielle et la cybersécurité. L'objectif sera d'élaborer des mesures concrètes pour élaborer cette définition grâce à des instruments européens pertinents tels que l'aide des États à la réglementation sectorielle et le Fonds européen pour la compétitivité. Les résultats de ses travaux seront présentés lors du Conseil des ministres franco-allemand en 2026.

Intelligence artificielle européenne d'avant-garde : la France et l'Allemagne souhaitent favoriser une innovation de rupture dans l'IA d'avant-garde. Ensemble, elles veulent créer un environnement de premier plan international pour le développement public-privé de l'IA d'avant-garde en Europe.

Le Sommet a représenté une plateforme importante de coordination et de mobilisation d'investissements du secteur privé. La France et l'Allemagne se félicitent de l'attachement à la souveraineté numérique manifesté par les entreprises technologiques européennes de pointe.

Le Chancelier allemand, Friedrich Merz, a déclaré :

« Le Sommet marque une étape importante sur la voie d'une Europe numérique plus souveraine, plus sûre et plus compétitive. Je tiens à remercier la France de travailler avec nous dans cet objectif. Pour l'Europe, la souveraineté numérique, c'est la capacité à façonner la technologie sur toute la chaîne de valeur en tenant compte des intérêts et des besoins européens. Notre objectif est la concurrence sur un pied d'égalité, sans exclure personne. En tant que communauté d'États, nous devons harmoniser en conséquence nos cadres juridiques, ainsi que nos procédures de marchés publics et d'investissements. Je tiens également à remercier les dirigeants des entreprises technologiques européennes qui ont uni leurs forces aux nôtres aujourd'hui et annoncé un large éventail de projets entres entreprises françaises et allemandes. Je me réjouis vivement de l'annonce par nos entreprises d'investissements de plus de 12 milliards d'euros dans les technologies clés. C'est là un signal important : l'Europe sera à la hauteur. »

Le Président français, Emmanuel Macron, a déclaré :

« Le Sommet sur la souveraineté numérique adresse un message clair : l'Europe a tout pour être à l'avant-garde de l'ère numérique. Aux côtés de l'Allemagne et dans le prolongement du Sommet pour l'action sur l'intelligence artificielle qui s'est tenu à Paris au début de l'année, ce sommet apporte des progrès concrets. L'Europe redouble d'efforts pour accélérer le rythme de l'innovation européenne, maintenir une protection des données très forte et demander des conditions de marché équitables. Ce sommet symbolise également une convergence historique de nos entreprises nationales championnes de l'IA et des technologies numériques et montre que la coopération transfrontalière n'est pas seulement une aspiration, mais un impératif stratégique. Les acteurs privés et publics doivent désormais intensifier leurs efforts pour développer et adopter des technologies européennes. »

Document 6 : Assurer la souveraineté européenne pour les données et l'informatique en nuage

Auteur(s) : Communication de l'Elysée

Source : Site de l'Elysée (https://www.elysee.fr), publié le 18/11/2025

Garantir la sécurité des données sensibles et contrôler les technologies numériques est essentiel pour la souveraineté de l'Europe.

La libre circulation des données en toute confiance est cruciale pour la croissance économique car elle permet le commerce numérique sans heurt, des chaînes d'approvisionnement intégrées et la diffusion rapide de l'innovation sur les marchés. Cependant, les politiques intérieures et extérieures de l'Union européenne (UE) doivent faire l'objet d'une coordination stratégique au vu des évolutions géoéconomiques tout en préservant son autonomie stratégique. Il est donc important de promouvoir des infrastructures basées dans l'UE, de réduire les dépendances à l'égard des acteurs extérieurs à l'UE et de renforcer la protection des flux de données essentiels. Le cadre européen doit instaurer un mécanisme capable de traiter tous les risques associés ou inhérents aux technologies en matière de cybersécurité, notamment l'application extraterritoriale de législations adoptées hors de l'UE concernant les technologies numériques, par exemple l'informatique en nuage. **Une issue favorable aux discussions en cours renforcerait la confiance dans le marché de l'informatique en nuage européen et améliorerait la protection des données les plus sensibles détenues par les États membres et les entreprises de l'UE. Même si une plus grande utilisation des solutions européennes est recommandée, conformément aux accords de l'OMC, les entreprises qui respectent les critères du cadre de l'UE sont bienvenues sur le marché européen.**

1. L'Europe doit poursuivre ses efforts pour assurer la souveraineté numérique.

La France et l'Allemagne soutiennent les efforts de l'UE dans sa stratégie européenne pour les données et prennent acte des travaux accomplis concernant la libre circulation des données en toute confiance ainsi que de l'importance des clauses liées aux données dans les accords commerciaux. Il est également important de reconnaître le rôle des flux de données internationaux fiables pour atteindre les objectifs de développement durable des Nations Unies.

La souveraineté numérique revêt une importance stratégique croissante pour la résilience et l'économie numérique de l'UE. La réalisation du marché unique numérique de l'UE, la promotion des investissements dans les entreprises européennes spécialistes de l'informatique en nuage et la réduction des dépendances à l'égard des infrastructures de données non sécurisées créent des vulnérabilités qui requièrent des réponses coordonnées. En outre, une action est rendue nécessaire par l'augmentation du nombre d'incidents liés à la cybersécurité et les cyberattaques contre les infrastructures européennes. Nous lutterons avec détermination contre le respect insuffisant des règles européennes en matière de vie privée et de sécurité des données. Le marché unique numérique européen devra également être renforcé et un cadre robuste devra être mis en place pour réexaminer le règlement sur la cybersécurité et l'acte législatif sur le développement de l'informatique en nuage et de l'intelligence artificielle (IA) afin de traiter la question des dépendances et celle des risques.

La France et l'Allemagne considèrent que l'UE doit mettre en place de toute urgence une architecture européenne unifiée et résiliente de gouvernance des données qui sauvegarde et protège ses données les plus sensibles, favorise la compétitivité économique et préserve l'autonomie stratégique de l'Union dans l'écosystème numérique mondial. Par conséquent, nous demanderons à la Commission européenne de réexaminer et, si nécessaire, d'ajuster ses règlements sur les données et la cybersécurité afin de parvenir à la souveraineté européenne des données. Il faudra à cet effet :

- une proposition de cadre pour la souveraineté des données,
- la définition de normes de protection extrêmement strictes pour les données les plus sensibles, notamment des normes adéquates pour protéger les données face aux risques relevant de la cybersécurité, en particulier les effets de législations extraterritoriales adoptées hors de l'UE et l'utilisation obligatoire de technologies protégeant mieux la vie privée, s'approchant au plus près du cadre européen de la cybersécurité.

Pour les données moins sensibles ou non sensibles, le cadre pourrait proposer un cadre à plusieurs niveaux qui comprend des incitations à l'innovation, un équilibre entre les exigences de localisation des données et l'utilisation de technologies renforçant le respect de la vie privée avec des possibilités améliorées d'utilisation des données à caractère personnel. L'UE doit affirmer sa position de chef de file dans la libre circulation des données en toute confiance au G7, au G20, à l'OCDE, aux Nations Unies et dans d'autres enceintes multilatérales et chercher à conclure des accords qui intègrent ses principes de protection des données dans les règles commerciales numériques mondiales.

2. Parvenir à la souveraineté numérique européenne doit se faire en lien avec le secteur privé.

Les autorités publiques doivent jeter les fondements d'une protection au plus haut niveau pour les données sensibles, ce qui nécessite un cadre réglementaire et de gouvernance européen robuste et cohérent ainsi qu'une politique industrielle ambitieuse. Dans ce contexte, les fournisseurs de services numériques, notamment des services en nuage, doivent prendre toutes les mesures techniques, juridiques et organisationnelles adéquates pour garantir la cybersécurité de leurs services, empêcher l'accès non autorisé par les autorités de pays tiers et, par conséquent, mettre au point des capacités et des structures capables de protéger les données européennes les plus sensibles. Ils doivent également assurer la portabilité et l'interopérabilité des données, proposer des interfaces sécurisées pour les échanges de données entre plateformes et des formats normalisés d'importation et d'exportation des données.

La France et l'Allemagne s'engagent à soutenir activement le développement et l'adoption de solutions européennes dans le domaine des données, de l'informatique en nuage et de l'IA. Dans le cadre des futurs projets importants d'intérêt européen commun concernant l'IA et les infrastructures et services en nuage, la France et l'Allemagne soutiendront des projets conjoints visant à renforcer la souveraineté européenne. De même, les usines géantes de l'IA doivent contribuer de manière concrète au renforcement de la souveraineté européenne dans toute la chaîne de valeur de l'informatique en nuage et de l'IA. Des positions communes robustes doivent être présentées concernant les critères de sélection et la gouvernance des usines géantes de l'IA, tant lors de la révision du règlement établissant l'entreprise commune pour le calcul à haute

performance européen que dans le futur programme d'action annuel pour faire en sorte que ces usines géantes soutenues par les États et l'UE apportent une valeur ajoutée à l'UE et prennent en compte la sécurité et la résilience des chaînes d'approvisionnement.

Les marchés publics doivent être mis à profit pour encourager le développement à grande échelle des acteurs européens dotés d'un savoir-faire dans l'ensemble du secteur des technologies en nuage.

Nous attendons avec intérêt les efforts déployés actuellement par la Commission européenne dans le domaine de la souveraineté numérique et de la réalisation du marché unique numérique, concernant en particulier la stratégie pour une union européenne des données, le train de mesures omnibus sur le numérique, le règlement sur la cybersécurité, l'acte législatif sur le développement de l'informatique en nuage et de l'intelligence artificielle, et le cadre sur la souveraineté de l'informatique en nuage.

Document 7 : La souveraineté numérique européenne est un défi d'ordre civilisationnel

Auteur(s) :

- Sandrine Dixson-Declève, Présidente honoraire du Club de Rome
- Jean-Marc Lieberherr, Président de l'Institut Jean Monnet
- Maria-Joao Rodrigues, Ancienne ministre portugaise

Source : Tribune dans « Le Monde » du 15/11/2025

Le 18 novembre, à Berlin, doit avoir lieu le Sommet sur la souveraineté numérique européenne. On peut espérer que cette rencontre sera l'occasion d'une prise de conscience au plus haut niveau du risque existentiel que fait peser sur l'Europe sa dépendance presque totale vis-à-vis des technologies et infrastructures numériques américaines et chinoises.

Cette dépendance n'est pas nouvelle, comme ne l'est pas non plus notre dépendance sécuritaire. Mais elle est désormais insupportable dans le contexte géopolitique actuel, qui marque le retour des rapports de force, de l'esprit de domination, et remet en cause nos alliances historiques. Cette dépendance n'est pas uniquement technologique : elle porte en elle les germes d'une vassalisation durable de l'Europe dans tous les domaines qui fondent sa souveraineté et son identité – sécurité, économie, industrie, technologie, santé, culture, éducation, démocratie… Cette dépendance, en somme, pose pour les Européens un défi civilisationnel, qu'il est vital d'appréhender collectivement avec un sentiment d'urgence.

Si, comme l'écrivait Jean Monnet dans ses Mémoires, « les hommes n'acceptent le changement que dans la nécessité et ne voient la nécessité que dans la crise », nous sommes dans un moment de grande nécessité qui peut ouvrir la voie au changement. Les retards et insuffisances de l'Union européenne (UE) ont été bien diagnostiqués et documentés, notamment par Mario Draghi et Enrico Letta, dont les excellents rapports servent de base à de nombreux débats, réflexions et échanges.

Mais force est de constater que nous peinons à transformer ces constats en actions claires, lisibles et coordonnées. Il peut être utile de chercher de l'inspiration dans un moment fondateur de notre histoire européenne qui, à bien des égards, présentait des similitudes avec celui que nous vivons aujourd'hui : un moment de danger et de tension dans lequel il était difficile d'y voir clair.

Renouer avec l'action collective

Au printemps 1950, le monde semblait au bord du gouffre. Les pays d'Europe demeuraient divisés et affaiblis. Dans les esprits, l'Allemagne de l'Ouest redevenait une menace potentielle. La guerre froide pouvait à tout moment dégénérer en conflit ouvert. Jean Monnet, alors commissaire au plan, analysait la situation ainsi : « Il faut changer le cours des événements. Pour cela, il faut changer l'esprit des hommes. Des paroles n'y suffisent pas. Seule une action immédiate portant sur un point essentiel peut changer l'état statique actuel. »

Ce point essentiel, en 1950, c'est le charbon et l'acier. Faire de l'outil, de l'enjeu même de la domination un bien commun géré dans l'intérêt de tous permettra de le neutraliser bien sûr, mais surtout d'enclencher une nouvelle dynamique européenne en jetant les bases d'un projet commun.

Cette idée, traduite dans la déclaration Schuman du 9 mai 1950, puis concrétisée dans les premières institutions européennes, est au cœur du projet européen.

Nous ressentons aujourd'hui l'urgence vitale pour l'Europe de renouer avec l'action collective et de reprendre le contrôle de son avenir. Mais quelle action ? Le monde d'aujourd'hui est encore plus complexe que celui de 1950, et l'UE à 27 ne simplifie rien. Cette complexité est paralysante en ce qu'elle rend difficile l'émergence d'une stratégie claire, commune et opérationnelle. Et pourtant, plus que jamais, la clarté est indispensable à l'action.

Toutes les grandes avancées de l'Europe se sont faites autour de projets concrets, clairs et priorisés. Jacques Delors, avec le marché unique et la monnaie unique, avait consciemment appliqué les recommandations de Jean Monnet, qui avaient inspiré la « révolution charbon-acier » de 1950 : « Tous nos soins devraient aller d'abord à ces puissants moteurs d'action qui retransmettent dans tous les organes. »

Aujourd'hui, sans aucun doute possible, ce « moteur d'action », qui irriguera pour longtemps tous les organes de l'Europe, de notre sécurité à notre fonctionnement démocratique, en passant par l'industrie et l'éducation de nos enfants, c'est l'écosystème numérique. Or, nous en avons perdu le contrôle au profit d'entreprises privées ou d'acteurs géopolitiques qui, dans le meilleur des cas poursuivent des stratégies de profit, dans le pire des cas des stratégies de domination et d'impérialisme.

Stratégie d'ensemble

Plus de 80 % des infrastructures et technologies numériques utilisées en Europe sont importées, et 85 % des modèles d'Intelligence artificielles sont développés aux Etats-Unis et en Chine. Trois entreprises américaines dominent 70 % du marché du cloud européen, la part du premier fournisseur européen ne dépassant pas 2 %. En somme, nous ne contrôlons ni nos infrastructures, ni nos données, ni nos algorithmes.

Il ne s'agit pas de se lancer dans une course consistant à vouloir répliquer ou concurrencer les grands acteurs actuels, mais de placer la souveraineté numérique au centre de nos priorités, d'identifier ensemble une voie commune et de renouer dans ce domaine avec l'action collective. D'excellents programmes ont été lancés, comme l'EuroStack, permettant pour la première fois de visualiser et d'évaluer l'écosystème numérique/IA européen.

Nous devons nous appuyer sur ceux-ci pour faire émerger une stratégie d'ensemble, identifier les quelques « projets-clés », clairement étiquetés comme des priorités, derrière lesquels focaliser nos énergies et nos ressources, et mettre en place les outils de planification et d'action collective sans lesquels aucune grande transformation ne pourra être réalisée. Il s'agit, pour les Européens, non seulement de répondre à un défi existentiel, mais aussi – et surtout – de construire ensemble l'Europe de demain sur des valeurs communes.

« Tout devient possible, disait Jean Monnet, si l'on sait se concentrer sur un point précis qui entraîne le reste. » Ce levier, à nous de l'actionner sans tarder.

Document 8 : Souveraineté numérique de l'Etat : un enjeu stratégique

Auteur(s) : La rédaction du site Vie-publique.fr

Source : Site internet https://www.vie-publique.fr, le 05/11/2025

Dans un contexte de cybermenaces mais aussi notamment de lois extraterritoriales étrangères permettant d'accéder à des données détenues par un autre pays, garantir la souveraineté numérique de l'État revêt un caractère stratégique. La sécurité des systèmes d'information civils de l'État est au cœur d'une récente publication de la Cour des comptes.

Selon les observations de la Cour des comptes publiées le 31 octobre 2025, des progrès restent à effectuer, en particulier dans la connaissance et la cartographie des données sensibles.

Pour la Cour des comptes, le coût de la souveraineté numérique n'est pas particulièrement élevé mais requiert une volonté de généraliser des normes d'hébergement plus strictes concernant les données sensibles. Le montant des dépenses de fonctionnement et d'investissement réalisées par la Direction interministérielle du numérique (Dinum), en charge de la transformation numérique de l'État, est évalué, sur la période 2014-2023, à 40 millions d'euros (M€) annuels. La Dinum consacre, entre autres, un budget de 5,5 M€ à FranceConnect (en 2024). Le réseau interministériel de l'État (RIE), géré par la Dinum représente un effort budgétaire de 10 M€ par an.

Les failles des systèmes d'information civils de l'État

Dans certains domaines, comme l'éducation ou la santé, des entreprises privées manient des données sensibles et effectuent des missions qui pourraient être considérées comme relevant du service public. Par exemple, les données du ministère de l'éducation nationale sont hébergées via le cloud (nuage) dans des data centers (centre d'hébergement des données numériques) privés et situés hors de France.

De manière comparable, s'agissant des données de santé publique, la plateforme "Health Data Hub", regroupant des données médicales pseudonymisées à des fins de recherche, est hébergée par l'entreprise américaine Microsoft. Cet exemple illustre certaines incohérences dans la politique de l'État. De surcroît, ces données peuvent potentiellement être consultées par les États qui accueillent les data centers.

La Cour reconnaît aussi la difficulté pour la France de respecter l'obligation d'appliquer les règles du marché intérieur européen. L'État ne peut pas imposer des règles de souveraineté qui excluraient de manière trop large des marchés publics une entreprise installée dans un autre État membre. Pour répondre à cette difficulté, la "stratégie nationale pour le cloud", lancée par le gouvernement en 2021, met l'accent sur la notion de "cloud de confiance", qui se substitue à la notion de "cloud souverain" et ne vise plus seulement une solution de cloud interne, mais une solution permettant d'assurer une protection des données, fondée sur le SecNumCloud, et permettant de sécuriser l'hébergement, même s'il est réalisé par des acteurs extra-européens.

Quelles solutions pour mieux garantir la souveraineté numérique ?

La Cour recommande de diffuser la certification "Hébergeur de données de santé", alignée sur les exigences de la qualification "SecNumCloud", élaborée par l'Agence nationale de la sécurité des

systèmes d'information (Anssi) et qui propose un ensemble de règles de sécurité à suivre par les prestataires de cloud. Cette qualification s'impose aujourd'hui à l'État pour l'hébergement de ses données sensibles, au titre de la loi du 21 mai 2024 visant à sécuriser et réguler l'espace numérique (loi SREN) mais pas aux entreprises.

La France a aussi créé des solutions d'hébergement des données pour les ministères. Deux infrastructures ont été développées, d'une part, par le ministère des finances (cloud Nubo) et, d'autre part, par le ministère de l'intérieur (cloud Pi). Ces deux clouds sont peu utilisés, non seulement par les services des ministères qui les ont créés, mais aussi par les autres administrations. Ils ont mobilisé 55 M€. Toutefois, ces solutions pourraient être davantage appropriées par les services de l'État d'autant plus qu'elles représentent un coût modéré au regard de l'ensemble des dépenses numériques totales de l'État, d'environ 3 milliards d'euros par an.

La Cour recommande en outre, dès 2026 :

- de mettre en place, avec les ministères un calendrier de déploiement d'outils de bureautique et de communication respectant la souveraineté des données ;
- de cartographier les données sensibles à héberger de manière souveraine dans tous les ministères.

Document 9 : Les enjeux de souveraineté des systèmes d'information civils de l'État

Auteur(s) : Cour des Comptes

Source : Synthèse du rapport de la Cour des comptes 2025-1479, 31/10/2025

La souveraineté numérique est une préoccupation qui a émergé depuis les années 2010. Elle implique une maîtrise par un État des technologies numériques et du droit qui leur est applicable, pour conserver une capacité autonome d'appréciation, de décision et d'action dans le cyberespace. Elle suppose ainsi de ne pas se faire dicter des choix technologiques structurants par un tiers et que soient protégées les données d'une sensibilité particulière des systèmes d'information de l'État. Il s'agit des données qui relèvent de secrets protégés par la loi ou qui sont nécessaires à l'accomplissement des missions essentielles de État et dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et à la vie des personnes, ou à la protection de la propriété intellectuelle.

L'ambition affichée par la France en matière de souveraineté numérique peine à être satisfaite du fait notamment de la position prééminente des entreprises américaines et de la législation qui leur est applicable, mais aussi d'un environnement européen qui encadre la latitude dont la France dispose en la matière.

Dans ce contexte, l'autonomie technologique est un objectif difficile à assurer dans le champ des matériels et composants. En revanche l'identité numérique et les applications sont des domaines où la maîtrise de la souveraineté est atteignable. Par ailleurs, un enjeu majeur pour les systèmes d'information de l'État est celui de la maîtrise des données les plus sensibles de l'administration, des citoyens et des entreprises, notamment avec le développement de l'informatique en nuage (cloud). Même si le coût de la souveraineté numérique est resté jusqu'ici modéré pour l'État, une tension se fait jour entre les enjeux de souveraineté et de performance des administrations.

La souveraineté des systèmes d'information civils de l'État sous la pression des cyberattaques et des lois extraterritoriales américaines

Garantir la sécurité de ses systèmes d'information est l'élément de base de l'exercice de la souveraineté numérique. L'actualité a montré que certains systèmes d'information civils (hors domaines de la défense et du renseignement) sont particulièrement exposés. Les attaques informatiques sont de plus en plus nombreuses et peuvent paralyser des administrations publiques, sans compter la perte ou le vol de données confidentielles. Ces intrusions émanent le plus souvent d'entités criminelles, mais peuvent également provenir d'États.

Au-delà, certains pays ont légalement la possibilité d'accéder à des informations confidentielles détenues par un autre pays. C'est le cas notamment des États-Unis qui ont adopté plusieurs décrets ou lois à portée extraterritoriale, dont le décret présidentiel (Executive Order 12333) de 1981 ; l'article 702 du Foreign Intelligence Surveillance Act, adopté en 2008 ; le Cloud Act de 2018 qui autorisent la collecte de données sur des personnes ou des entités, même si ces données sont stockées en dehors des États-Unis.

Les opérateurs américains du numérique, présents sur tous les continents, sont soumis à ces lois. Si certains rendent compte approximativement du nombre de demandes qu'ils ont reçues à ce titre de la part des autorités américaines, ces procédures restent marquées par une grande opacité. La

dépendance des administrations publiques à ces entreprises peut être une entrave à l'objectif de souveraineté numérique qu'il convient de dépasser par une maîtrise des conditions d'exploitation et de stockage des données les plus sensibles.

La vigilance de l'État pour protéger ses données les plus sensibles dans toutes les composantes de la chaîne de production numérique

Pour atteindre la souveraineté numérique, il est nécessaire de contrôler la chaîne de production des systèmes d'information. Cet enjeu comporte trois volets : la maîtrise des matériels, celle des logiciels, et désormais le sujet majeur de la maîtrise des données sensibles.

Concernant les matériels, très peu d'industries sont présentes en Europe. La production des semi-conducteurs se fait principalement aux États-Unis et en Asie. De même, les équipements réseau, les ordinateurs et les smartphones, fabriqués à l'aide de ces composants électroniques, proviennent des États-Unis et d'Asie. L'État veille néanmoins à ce que les matériels qu'il acquiert soient pleinement fiables et sans risques sécuritaires. L'Agence nationale de sécurité des systèmes d'information (Anssi), créée en 2009, s'y emploie et la mutualisation des achats via des marchés interministériels facilite ce contrôle.

La résilience des communications gouvernementales est assurée depuis 2015 par le réseau interministériel de l'État (RIE) qui garantit un bon niveau de fonctionnement, même en cas de défaillances majeures d'Internet. Conformément aux recommandations passées de la Cour, la Direction interministérielle du numérique (Dinum) consolide encore ce réseau en préparant un plan de continuité et de reprise d'activité.

En ce qui concerne les logiciels, la plupart des applications métier des administrations sont hébergées dans des centres informatiques ministériels ou interministériels. L'État en maîtrise ainsi l'exploitation et garantit la sécurité des données hébergées.

En revanche, se pose la question de la dépendance de l'État vis-à-vis des éditeurs de logiciels. Certaines administrations se prémunissent de ce risque en développant ou en faisant développer des applications propres. Si elles gardent ainsi la main sur le logiciel, cette démarche n'est pas sans défaut, notamment pour respecter les budgets alloués et les délais de réalisation. Beaucoup d'exemples de dérapages financiers et opérationnels ont été constatés par la Cour au fil de ses précédents contrôles.

D'autres administrations préfèrent recourir à des logiciels du marché, pour offrir à leurs agents des fonctionnalités déjà éprouvées et assurer une plus grande rapidité de déploiement. Si cette démarche peut apporter une plus grande performance à court terme, elle crée une dépendance de fait vis-à-vis de l'éditeur qui risque de confronter l'administration à des revirements de politiques techniques et commerciales, notamment avec des éditeurs qui basculent vers de nouveaux modèles, fondés sur le cloud, et augmentent leurs tarifs. Même lorsque les marchés incluent formellement des clauses de réversibilité, les changements de logiciels sont généralement des projets longs et coûteux. Tel a été le cas avec l'usage, très répandu, des logiciels de bureautique et de messagerie qui composent la suite Microsoft Office. L'entreprise a annoncé basculer son offre sur le cloud, et la Dinum a demandé aux ministères de ne pas y souscrire, pour des raisons de souveraineté des communications électroniques.

Pour autant, deux approches coexistent au sein de l'État : le ministère de l'éducation nationale (MEN) a entrepris de remplacer la suite Office par un ensemble d'applications sous licence logicielle libre ;

la Dinum, de son côté, développe par elle-même une nouvelle suite bureautique et de messagerie, en coordination avec ses homologues allemand et néerlandais. S'il est regrettable qu'il n'y ait pas convergence d'approche entre le ministère aux effectifs les plus nombreux et la Dinum, ces deux exemples illustrent l'existence d'alternatives, même face à un éditeur en position de force.

Enfin, la Dinum a porté le projet d'identité numérique FranceConnect pour des motifs de souveraineté face à des offres d'authentification émanant de grandes entreprises américaines, comme Facebook et Google. Ce produit est aujourd'hui massivement utilisé, montrant qu'il répond à des besoins de simplicité et de confiance des citoyens. Dans la conduite de ce projet, la Dinum apparaît toutefois dépendante de ses prestataires et n'a pris que tardivement des mesures de sécurisation, aussi bien face aux risques liés aux sous-traitants qu'à ceux, plus globaux, d'usurpation d'identité. Le renforcement de la sécurisation de FranceConnect, via l'outil FranceConnect+, a permis de lutter contre des fraudes parfois massives.

La question de la gestion des données est devenue encore plus prégnante avec le développement du cloud, dont le marché est largement dominé par quelques grandes entreprises américaines, dites hyperscalers, qui ont investi des sommes très élevées dans des infrastructures robustes, sécurisées et performantes. Tout en incitant les administrations à recourir au cloud, l'État a édicté des règles visant à protéger les données les plus sensibles vis-à-vis des lois extraterritoriales auxquelles sont soumises ces entreprises.

La priorité donnée au cloud dans un équilibre complexe entre enjeux de souveraineté et respect réglementaire du cadre européen

Le Premier ministre a édicté une doctrine, dite « Cloud au centre », pour que les administrations privilégient les infrastructures cloud pour leurs nouveaux projets numériques. La première version de la circulaire, diffusée en juillet 2021, indiquait que toute application maniant des données d'une sensibilité particulière, et notamment des données personnelles de citoyens français, devait être hébergée sur une infrastructure souveraine. Une seconde version de mai 2023 a restreint l'obligation de recours à une offre souveraine en ne l'exigeant que lorsque deux critères cumulatifs sont observés : les données doivent relever de secrets protégés par la loi et leur violation doit être susceptible *« d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et à la vie des personnes, ou à la protection de la propriété intellectuelle »*. Ces critères cumulatifs ont été élevés au niveau législatif avec la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (loi SREN) en son article 31.

Le choix de restreindre ainsi les obligations de recours à une infrastructure souveraine s'explique notamment par la nécessité de respecter les règles du marché intérieur européen et le principe du pays d'origine. La France ne peut pas imposer des règles de souveraineté qui excluraient de manière trop large des marchés publics une entreprise installée dans un autre État membre. La Commission européenne n'a, à cet égard, pas émis d'objection à l'issue de la période dite de statu quo sur le projet de décret d'application de l'article 31 de la loi SREN présenté par la France.

L'Union européenne (UE) peut imposer des règles uniformes en son sein, comme elle l'a fait sur la protection des données personnelles avec le RGPD. Elle est alors en mesure d'infliger de lourdes sanctions aux entreprises qui ne respectent pas ces règles. Mais elle ne s'est pas approprié les enjeux de souveraineté de façon aussi exigeante que la France. Ainsi, ses deux premières décisions dites d'adéquation, ayant pour objet d'instaurer un cadre de confiance pour l'échange des données personnelles entre l'UE et les États-Unis (Safe Harbour en 2000 et Privacy Shield en 2016), ont été annulées par la Cour de justice de l'Union européenne (CJUE) qui a considéré que les États-Unis

n'apportaient pas suffisamment de garanties aux citoyens de l'Union. La troisième décision d'adéquation, le Data Privacy Framework, est en vigueur depuis juillet 2023.

Enfin, la Commission travaille sur un schéma de certification des fournisseurs de services de cloud (EUCS4), comportant plusieurs niveaux d'exigence de sécurité selon la sensibilité des données concernées. La France a plaidé pour y introduire un niveau de supérieur de sécurité inspiré de la qualification SecNumCloud de l'Anssi qui garantirait une immunité face aux lois extraterritoriales. Cela reconnaîtrait à l'échelle européenne l'exigence de souveraineté et sécuriserait juridiquement cette approche. La démarche de la France est restée jusqu'à présent isolée au sein de l'UE.

Le coût de la souveraineté : un investissement de l'État jusqu'ici modéré ; un marché de l'hébergement souverain non stabilisé

La Dinum a arrêté des orientations qui intègrent un axe relatif à la souveraineté numérique. Celles-ci ne constituent cependant pas une stratégie de l'État opposable aux ministères. Ces derniers disposent d'ailleurs de budgets informatiques propres et aucun pilotage transversal de leurs investissements numérique n'est organisé.

Pour accompagner le développement du cloud au sein de l'État, deux infrastructures développées, d'une part, par le ministère des finances (*cloud* Nubo) et, d'autre part, par le ministère de l'intérieur (*cloud* Pi), ont été ouvertes aux autres administrations. Ces deux *clouds*, qui ont mobilisé des niveaux de financement modérés (55 M€ en neuf ans pour Nubo au regard des dépenses numériques de l'État d'environ 3 Md€ par an), restent peu utilisés, non seulement par les services des ministères qui les ont créés, mais aussi par les autres administrations. La gamme des services offerts demeure limitée (en termes de disponibilité, d'expérience utilisateur ou de capacité à recourir à l'intelligence artificielle) et leur tarification apparaît inadaptée.

Il conviendrait d'engager la convergence de ces deux *clouds* pour qu'ils atteignent une taille critique et les rendre plus attractifs pour accroître significativement leur utilisation par l'ensemble des ministères. Le réseau interministériel de l'État (RIE) a été réalisé grâce à un effort budgétaire raisonnable (10 M€ par an) qui a permis de surcroît des économies d'exploitation. Cet exemple illustre le fait que, en sus de la mutualisation des enveloppes budgétaires ministérielles, de l'ordre de 15 à 20 M€ par an, consacrées aux clouds Nubo et Pi, leur convergence pourrait être réalisée à un coût modéré.

Concernant l'offre émanant de prestataires privés, l'Anssi a développé la qualification SecNumCloud qui assure le plus haut niveau de sécurité et une immunité aux lois extraterritoriales. À l'heure actuelle, seulement une dizaine de prestataires offrent des services ayant obtenu cette qualification. Le surcoût d'exploitation d'une infrastructure SecNumCloud par rapport à un hébergement cloud traditionnel se situe entre +25 et +40 %, sans compter le coût de migration pour des applications déjà existantes. Par ailleurs, à ce jour, les services qualifiés SecNumCloud n'ont pas la profondeur des hyperscalers.

Aussi, face à des données financières éparses, la définition d'une stratégie de souveraineté des systèmes d'information de l'État devrait impérativement être complétée par un chiffrage des investissements à réaliser.

Une tension entre les enjeux de souveraineté et de performance : un niveau de performance à mettre en regard des besoins réels et surtout de la préservation de la souveraineté

Les diligences menées par la Cour dressent un panorama de situations très diverses selon les ministères pour la gestion des données sensibles, sans que la Dinum soit en mesure de faire prévaloir une doctrine claire.

Le système d'information des ressources humaines (recrutements, évaluations, formations) du ministère de l'éducation nationale, Virtuo, est opéré en mode cloud par une entreprise appartenant à un groupe américain. Si cette application gère des données d'une sensibilité particulière, le ministère estime qu'il n'est pas contraint de recourir à une solution souveraine, car leur éventuelle divulgation n'entrerait pas dans une catégorie prévue dans la loi SREN. La Dinum ne se prononce pas sur cette appréciation. Dans le cadre juridique actuel, de telles données personnelles pourraient être considérées comme ne relevant pas des exigences de souveraineté, mais sans que cela résulte d'une analyse interministérielle partagée.

Les données confidentielles des entreprises relèvent quant à elles des deux critères inscrits dans la loi SREN (données sensibles et divulgation pouvant causer un trouble à l'ordre public ou à la protection de la propriété intellectuelle). Ainsi, le portail public chargé de la généralisation de la facturation électronique, porté par le ministère des finances, est hébergé dans un environnement souverain. En revanche, tel n'est pas encore le cas de la plateforme d'achat public. Le fait que le ministère recoure, pour une partie des prestations, à une entreprise d'un groupe canadien, a inquiété plusieurs parlementaires et montré que la migration vers un environnement souverain devrait être plus fermement programmée.

La plateforme des données de santé (dite Health Data Hub), regroupant des données médicales pseudonymisées à des fins de recherche, témoigne aussi des difficultés de faire prévaloir une position unanime. Le choix d'un hébergement par l'entreprise Microsoft a permis de disposer d'un service opérationnel en quelques mois ; en revanche il a suscité la méfiance des fournisseurs de données de santé, ce qui a entravé son bon fonctionnement et son développement. Une plateforme initialement moins performante, mais souveraine, aurait probablement permis un déploiement moins heurté et un usage plus répandu.

Aussi la Cour recommande-t-elle à l'État de réaliser et régulièrement actualiser une cartographie des données sensibles qui nécessiteraient un hébergement souverain.

Enfin, des entreprises privées proposent des offres liées à des missions de service public et manient des données d'une grande sensibilité. Dans le champ de la santé, c'est le cas de Doctolib, par exemple, qui recueille des informations médicales très précises. À cet égard, la certification « hébergeur des données de santé » à laquelle ces entreprises sont soumises mériterait d'intégrer des critères de souveraineté qui s'imposeraient à tous les acteurs, y compris privés. Dans le domaine de l'éducation, c'est le cas de Pronote qu'utilisent la plupart des établissements publics du second degré pour retracer la vie scolaire de leurs élèves. Ces entreprises ne sont aujourd'hui pas couvertes par les exigences de souveraineté, même si Docaposte, éditeur de Pronote et filiale du groupe La Poste, a fait le choix d'un hébergement qualifié SecNumCloud.

Tant que l'Europe ne dispose pas d'opérateurs capables de rivaliser avec les hyperscalers, les administrations publiques devraient viser une performance des systèmes d'information plus strictement adaptée à leurs besoins. Le parfait exercice des missions de service public peut être garanti sans nécessairement aligner les spécifications des systèmes d'information sur le plus haut niveau technologique dès lors qu'un degré trop élevé de performance à court terme peut constituer

un double écueil : par la mise en cause de la souveraineté sur les données et par une dépendance de l'administration vis-à-vis de la politique commerciale d'un éditeur dominant.

À l'issue de cette enquête, la Cour formule cinq recommandations visant à mieux prendre en compte les enjeux de souveraineté dans les systèmes d'information civils de l'État qui deviennent de plus en plus prégnants dans le contexte du développement rapide de l'intelligence artificielle et la perspective de l'informatique quantique.

Recommandation n° 1. (Direction interministérielle du numérique) : Mettre en place en 2026 avec les ministères un calendrier de déploiement d'outils de bureautique et de communication respectant la souveraineté des données.

Recommandation n° 2. (Direction interministérielle du numérique) : À l'occasion de la révision de la feuille de route de la Dinum, intégrer une stratégie de souveraineté numérique qui définisse, notamment, les modalités de développement et d'exploitation des applications informatiques de l'État, et procéder à son chiffrage.

Recommandation n° 3. (Direction interministérielle du numérique, Direction générale des finances publiques, Secrétariat général du ministère de l'intérieur) : Définir la trajectoire de convergence des clouds interministériels pour les rendre plus performants et augmenter significativement leur utilisation mutualisée par l'ensemble des ministères civils.

Recommandation n° 4. (Direction interministérielle du numérique, Agence nationale de la sécurité des systèmes d'information) : Veiller à ce que chaque ministère cartographie en 2026 l'ensemble de ses données sensibles à héberger de manière souveraine.

Recommandation n° 5. (Délégation au numérique en santé) : Assurer la souveraineté de l'hébergement des données de santé en alignant la certification « Hébergeur de données de santé » sur les exigences de la qualification SecNumCloud en matière de protection vis-à-vis du droit extra-européen.

Document 10 : Avec DiploIA, le Quai d'Orsay met la traduction et la transcription au centre de sa stratégie IA

Auteur(s) : Victoria Beurnez

Source : Acteurs Publics (23/06/2025)

Le ministère de l'Europe et des Affaires étrangères a lancé récemment DiploIA, un dispositif de traduction et de transcription multilingue à destination de ses quelque 13 000 agents, dont une part exerce à l'étranger. Pour répondre aux besoins des missions sensibles, le ministère a dû articuler sécurité et technologie.

Comme quelques uns avant lui, le ministère de l'Europe et des Affaires étrangères s'est désormais lancé dans le déploiement d'outils d'intelligence artificielle internes, à destination de ses agents. Contrairement à ce qui se fait ces derniers mois, il n'est pas question ici d'un chatbot, mais d'outils pensés précisément pour les besoins des agents, notamment en dehors de la France. C'est en réfléchissant au plus près de ces besoins que la direction du numérique du ministère a déployé DiploIA auprès de ses quelque 13 000 agents, en France et à l'étranger, depuis le mois de mai.

« Nous avons une vraie attente de la part de nos agents sur de tels outils », explique Virginie Rozière, directrice du numérique au ministère de l'Europe et des Affaires étrangères, auprès d'Acteurs publics. Pour autant, il n'était pas question de se lancer dans des outils sans réflexion en amont, qui pourraient dès lors *« relever du gadget »*, tempère la directrice. *« On cherche vraiment la maximisation d'impact et ce qui va répondre aux besoins les plus précis de nos utilisateurs – ce sont les usages de terrain, enregistrement, transcription multilingue, traduction spécialisée – qui ont guidé le développement de DiploIA »*, continue-t-elle.

Transcription et traduction

Et c'est donc en deux outils que ces besoins se sont illustrés : un système de traduction, presque évident pour les agents déployés à l'étranger et notamment dans les ambassades, et un outil de transcription multilingue, qui comprend une centaine de langues et peut traduire en deux minutes une heure de dialogue. *« Ça leur facilite la vie, parce qu'ils ont déjà des compétences linguistiques et de traduction de par leur métier, mais ils peuvent de cette manière se concentrer davantage sur de la relecture et de la mise en qualité »*. Et c'est aussi parce que tous ces dispositifs sont réfléchis au plus près des demandes des agents qu'on ne trouve pas, dans cette boîte à outils IA, de chatbot : selon Virginie Rozière, les agents n'ont pas fait émerger un tel besoin pour les appuyer dans leurs tâches quotidiennes.

Pour faire tourner ses modèles, le ministère dispose déjà de longue date de deux *data centers* maison, qu'il a renforcés en fin d'année dernière avec la mise en place de processeurs graphiques destinés à faire tourner ces outils d'IA, efficients depuis début 2025. Le Quai d'Orsay, historiquement, dispose de ses propres moyens et technologies de communication, en raison des missions sensibles qui sont celles de ses agents. *« En maîtrisant nos outils, nous maîtrisons aussi les risques : fuites de données, hallucinations, biais… Ces dangers existent, mais nous les anticipons en faisant de la sécurité des données une priorité dans nos développements »*, précise la directrice. De fait, *« aucun contenu ne transite par des plateformes externes »*, dit-elle, ajoutant qu'il s'agit d'une *« garantie forte pour notre sécurité informationnelle et notre indépendance stratégique »*. Par ailleurs, le projet pourrait faire des

émules : Virginie Rozière se félicite ainsi que *« cette réussite ouvre des perspectives de mutualisation avec d'autres ministères régaliens. Des discussions sont déjà engagées au niveau interministériel. »*

D'autres outils prévus

Et le ministère réfléchit déjà à la suite : si Virginie Rozière insiste sur la nécessité de garder à l'esprit l'articulation entre frugalité et performance, la direction songe, *« si le plan de charges le permet »*, à se tourner, d'ici à la fin de l'année, sur un outil supplémentaire de synthèse automatique, toujours pour alléger les tâches des agents. *« DiploIA est une première pierre. D'autres cas d'usage, d'autres outils viendront : nous construisons une capacité IA souveraine et durable »*, précise la directrice.

Dans le même temps, la direction du numérique du Quai d'Orsay a la volonté de renforcer ces outils en intégrant de manière pérenne le langage diplomatique – ce que ne lui a pas permis l'entraînement de modèles *« sur étagère »* ou open source. *« C'est une complexité supplémentaire parce qu'on ne prend plus des modèles sur étagère, open source, qu'on ajuste. Ce qui veut dire qu'on doit se doter d'une capacité d'entraînement de modèles spécialisés sur les besoins spécifiques de la diplomatie, impliquant plusieurs mois de travail avec les diplomates qui devront faire leur retour pour adopter la bonne dynamique. »* Un changement d'échelle qui sera, ceci dit, aussi soumis au contexte des finances publiques.

Document 11 : Numérique et cyber : enjeux de souveraineté

Auteur(s) : Dominique LUZEAUX, Ingénieur général de 1 ère classe de l'armement, directeur de l'Agence du numérique de défense (AND).

Source : Revue Défense Nationale 2023/4 n°859

Contexte géostratégique : la Revue nationale stratégique

La Revue nationale stratégique, publiée en novembre 2022 par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), rappelle les intérêts nationaux de sécurité :

– protection du territoire national ;

– sécurité des États en application des traités par lesquels nous sommes liés ;

– stabilité de notre voisinage compte tenu des répercussions immédiates que toute crise y émergeant aurait sur notre propre territoire, métropolitain comme ultramarin ;

– liberté d'accès aux espaces communs dont le cyberespace, mais aussi le spatial et les espaces aéromaritimes.

La cybersécurité, la cyberdéfense, plus généralement la résilience cyber, sont donc affirmées comme clés pour maintenir l'autonomie de décision et d'action de la France qui, rappelons-le, est membre permanent du Conseil de sécurité des Nations unies, 7 e économie mondiale contrôlant la 2 e Zone économique exclusive (ZEE), et est dotée de l'arme nucléaire.

Les espaces communs (cyber, spatial, fonds marins et espaces aéromaritimes) font aujourd'hui l'objet d'une compétition de puissance renouvelée. Leur importance opérationnelle comme géographique croît alors que les règles communes qui les gouvernent sont insuffisantes, fragilisées ou contestées.

Sans rentrer dans le détail, en attaques physiques, il suffit de se remémorer les dommages subis en octobre 2022 par certains câbles sous-marins qui ont ralenti le trafic Internet pour certaines régions mondiales, les dommages sur des fibres terrestres en Allemagne, récemment, ou en France, il y a deux ans. En attaques cyber, rappelons-nous en novembre 2015 l'attaque subie par l'aéroport d'Arlanda à Stockholm qui a perturbé le trafic aérien pendant de nombreuses heures, sans oublier les attaques sur certaines infrastructures énergétiques (distribution de carburant en Iran en 2022) ou sur des centrifugeuses de centrales. Ainsi, certains États utilisent de plus en plus systématiquement l'arme cyber afin de défendre leurs intérêts stratégiques ou dans le cadre de tensions géopolitiques. Ces stratégies hybrides (attaques cyber et numérique, Espace) exploitent la difficulté, pour la plupart des États démocratiques, d'apporter une réponse efficace compatible avec le respect des engagements, traités et principes politiques au fondement de l'ordre international.

Un de nos enjeux est donc d'accélérer, d'adapter, de compléter notre posture stratégique face à des menaces qui évoluent dans leur allure, dans leur nature et dans leur espace, dans un cadre de plus en plus marqué par ces stratégies hybrides ou de déni d'accès pour peser sur nos intérêts (exploitation des vulnérabilités des flux ou infrastructures logistiques, des espaces aéromaritimes). Ceci amène à de nouveaux modes de réponse : LID (Lutte informatique défensive), LIO (Lutte informatique offensive) et désormais LII (Lutte informatique d'influence), qui s'exerce dans les différentes dimensions diplomatique, militaire, économique, mais aussi culturelle, sportive, linguistique, informationnelle.

Cette posture est d'autant plus nécessaire que des entreprises privées développent progressivement des capacités offensives, des armes et des outils d'espionnage cyber sophistiqués prêts à l'emploi. Cette course à l'armement cyber accroît le risque d'escalade. La menace cybercriminelle, qui atteint un niveau inédit de sophistication et de désinhibition, constitue donc un défi stratégique pour notre sécurité nationale.

La France doit intégrer l'inéluctabilité du rattrapage et de la dissémination dans le domaine technologique. Les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) ou d'autres acteurs privés, s'imposent comme des acteurs non étatiques dont les contributions actives ou passives, par les outils qu'ils mettent à disposition, doivent être intégrées comme données d'entrée dès les phases de contestation.

En conséquence, la recrudescence de comportements inamicaux dans nos approches territoriales implique de disposer de moyens robustes de détection, remédiation et réponse, y compris dans l'Espace et dans le cyberespace. Ces capacités demandent ainsi à être renforcées et articulées dans le cadre de l'effort global de l'État pour affronter des crises de grande ampleur. Aucun moyen ne suffit pour envisager un bouclier cyber qui mettrait en échec toute cyberattaque menée contre la France, mais renforcer son niveau de cybersécurité est essentiel pour préparer le pays à davantage de menaces. De même, l'application d'une logique dissuasive dans le cyberespace qui forcerait tout attaquant à la retenue contre la France est illusoire mais adopter des stratégies de réponses mobilisant l'ensemble des leviers de l'État, européens et internationaux permet de rendre les cyberattaques particulièrement coûteuses pour les attaquants.

L'effort doit porter sur l'amélioration de notre résilience cyber. Celle-ci consiste à disposer de capacités adaptées et organisées, permettant de prévenir ou, le cas échéant, de réduire l'impact et la durée des cyberattaques menées à l'encontre de la France, a minima pour les fonctions les plus critiques.

Renforcer la résilience cyber et numérique

Les acquis fondamentaux du modèle français, établi en 2008 puis régulièrement renforcé et adapté, doivent être consolidés. La gouvernance de la sécurité numérique de l'État a été rénovée et peut désormais être déployée. La capacité nationale à concevoir et mettre en œuvre des politiques publiques est illustrée par la création d'Équipes régionales de réponse aux incidents (CSIRT), par l'ouverture du Campus Cyber et par l'émergence d'un écosystème de cyberdéfense à Rennes. Enfin, à l'issue de sa présidence du Conseil de l'Union européenne (janvier-juin 2022), la France est reconnue par ses pairs comme une référence sur les questions de cybersécurité.

Ceci dit, le niveau de cybersécurité de l'ensemble des services publics doit être fortement rehaussé. Cela passe par des actions à mener selon plusieurs axes, techniques, financiers, sociétaux, juridiques, politiques :

• **L'investissement dans des infrastructures résilientes :** consolider un socle numérique de l'État homogène et sécurisé, et renforcer les établissements et administrations encore trop fragiles (réseau physique dédié pour assurer une résilience des acteurs d'importance vitale en cas de crise, architecture multi-cloud pour la résilience des données vitales et administratives).

• **La mise en place d'un écosystème industriel souverain :** l'action de la France doit être démultipliée en s'appuyant sur un écosystème cyber public et privé dynamique. L'État ne peut agir seul sur les enjeux de cybersécurité et doit être en mesure de mobiliser l'ensemble des acteurs en cas de crise

majeure. Il doit pouvoir exploiter les gisements de compétences disponibles au niveau des réservistes, mais aussi des retraités ayant travaillé au profit de cet écosystème cyber et numérique public et privé. L'effort doit également porter sur la responsabilité des fournisseurs de services numériques et la sécurisation des chaînes d'approvisionnement (stocks de matériels : des éléments actifs de réseau aux solutions de calcul et de stockage). Enfin, la France peut soutenir et favoriser l'apparition d'offres de confiance robustes et souveraines au niveau national comme européen.

• **La sensibilisation et la formation :** tous les acteurs du monde numérique doivent être formés et sensibilisés au risque cyber. Il s'agit de mobiliser le grand public, systématiser son intégration dans les cursus éducatifs et renforcer l'attractivité des métiers de la filière. Des actions sont à mener de type Bac Pro numérique, mais aussi en formation continue. Un effort particulier doit porter sur les départements, régions et collectivités d'outre-mer, du fait tant de leur position géostratégique que de la nécessité de ne pas créer de fracture numérique entre la métropole et les DROM-COM : l'éloignement de certains territoires par rapport aux grandes voies mondiales du numérique peut être une vulnérabilité stratégique, qu'il faut compenser en investissements, d'une part en infrastructures (satellites, câbles sous-marins, fibres), d'autre part en éducation et formation.

• **Le développement d'un arsenal juridique et technique au service de la détection et de la riposte :** la France doit poursuivre son investissement sur le renseignement nécessaire à l'entrave des flux illicites ou déstabilisants avec un focus particulier sur les intangibles, particulièrement vulnérables aux actions cyber, tout en confortant ses capacités d'action pour contrecarrer ces flux illicites ou déstabilisants. Dans le champ de la lutte contre les manipulations de l'information venant de compétiteurs étrangers, la France doit disposer d'un large éventail d'options de réponse. En particulier, il y a un besoin d'outils de riposte tant juridiques que numériques contre les intermédiaires (« proxies ») que des puissances hostiles utilisent afin de démultiplier leurs actions de contestation ou de compétition, tout en maintenant un déni plausible.

• **La solidarité européenne :** la résilience de la France dépend de la sécurité et de la stabilité du cyberespace dans son ensemble. Il faut donc contribuer à la montée du niveau de résilience des institutions européennes, internationales et des partenaires de la France, ainsi que poursuivre la structuration d'un marché européen des produits et des services de cybersécurité. Sur la scène internationale, la France doit porter des propositions permettant d'encadrer le commerce et de lutter contre la prolifération des armes cyber, grâce notamment à une meilleure utilisation des outils de contrôle des exportations des biens et technologies. En complément, un référentiel commun de gestion de crise cyber, tout comme des mécanismes de coopération et d'entraide permettraient aux États d'éviter les risques d'incompréhension et d'escalade incontrôlée.

Le numérique : un enjeu de puissance et de souveraineté

Comme rappelé supra, la cybersécurité et le numérique ont bonne place dans la RNS, et contribuent directement aux fonctions stratégiques – dissuasion, prévention, protection, intervention, connaissance et anticipation, influence – sur lesquelles repose la stratégie de défense et de sécurité nationale. De plus, la souveraineté numérique est clairement un pan de la souveraineté économique et industrielle. Ce constat nous amène à nous questionner sur la politique à mettre en œuvre pour aboutir à la finalité recherchée : quels acteurs sont à préserver, à déployer, à développer ? Pour quelle durée l'État doit-il mettre en œuvre des mesures protectionnistes ? Quelle politique des brevets doit être dessinée pour garantir une protection des savoir-faire et des données, à des fins de production industrielle et d'exploitation commerciale ?

La réponse réside dans l'équilibre du choix politique entre indépendance et dépendance technologique. Ce juste degré d'interdépendance suppose d'avoir le choix entre différentes solutions technologiques viables au niveau national, puis européen, le cas échéant. Afin d'arbitrer sur ses propres choix capacitaires, l'État doit être en mesure de s'approprier et pérenniser les compétences de savoir-faire sur l'ensemble du spectre numérique.

Le cyberespace peut être divisé macroscopiquement en trois domaines : les données qui sont le cœur de l'enjeu, les applications qui permettent leur traitement, et les réseaux qui transmettent les échanges au sein de l'espace numérique. Chaque domaine a ses propres enjeux de maîtrise. Pour les données, il faut en contrôler la quantité, la qualité, la propriété. Les applications nécessitent l'acquisition de calculateurs et logiciels de nouvelle génération ayant en particulier des capacités d'apprentissage, d'où des questions de maîtrise de la confiance. Enfin, pour les réseaux, la maîtrise physique de bout en bout (terre, mer, air et espace) se décline au travers de leur sécurisation, de leur intégrité et de leur approvisionnement énergétique.

Si l'on rentre un peu plus dans le détail de l'espace numérique, sans être dans la sophistication technique, il est possible de dégager les différentes couches suivantes avec certains enjeux clés :

• **La couche de l'électronique et les matériels**

– La vulnérabilité principale est la disponibilité des matières premières, et la sécurité de leur approvisionnement : une filière de recyclage adaptée pourrait alors dégager des marges de manœuvre.

– L'autre enjeu est la conception et fabrication de composants clés, et là encore se pose la question de la sécurité de leur approvisionnement comme on le voit actuellement : redévelopper des capacités nationales ou européennes dans le domaine est une réponse, adapter les stocks stratégiques en est aussi une.

• **La couche des infrastructures réseaux**

– L'intégrité des câbles sous-marins et terrestres, fibres, poteaux et antennes 3G/4G/5G a montré leur vulnérabilité et l'importance de leur sécurisation ; au vu des attaques régulières sur ces infrastructures et de leur impact en termes de disponibilité mais aussi de cybersécurité, on est en droit de se poser la question de la nécessité d'un réseau résilient, protégé, dédié aux opérations d'importance vitale de l'État. N'oublions pas que le cyberespace n'est pas que virtuel et la couche de transport en est une empreinte physique majeure.

– Si le conflit en Ukraine a montré l'apport opérationnel des satellites pour les communications en cas de crise, via la mise à disposition de 25 000 terminaux connectés à la constellation Starlink, cela démontre en même temps la dépendance totale par rapport à ces moyens et aux services associés, dont la disponibilité en termes géographiques et de performance est programmable à distance : sans accès aux satellites, que ce soit par déni de service ou par destruction vu que l'Espace est devenu un sujet de tension et de concurrence militaire, plus de communications spatiales. Le projet européen IRIS² et la capacité GOVSATCOM sont une réponse clé à venir à ces préoccupations.

• **La couche des logiciels** (systèmes d'exploitation, environnements collaboratifs, plateformes d'accès, Cloud, etc.)

– La sécurisation de l'accès à ces technologies est critique au vu de la transformation numérique de notre société ; là encore, la problématique est celle de la sécurité d'approvisionnement des logiciels,

et ce n'est pas qu'une question d'éditeurs propriétaires : un exemple récent concernant les logiciels libres est le blocage, pour des comptes dans certaines régions géographiques (Crimée, Iran), de Github qui permet justement l'accès aux logiciels libres nécessaires pour faire fonctionner les applications informatiques ; quand on évoque le Cloud, il ne faut pas uniquement se focaliser sur la protection des données que l'on y met, il convient aussi de maîtriser les technologies permettant d'y avoir accès et de le faire fonctionner : c'est une des faiblesses actuelles des démarches dites de confiance où l'on se concentre sur le contenu, en ignorant ou en feignant d'ignorer la problématique du contenant.

Tout ceci montre l'importance de la sécurisation et de la maîtrise de certaines technologies pour garantir la capacité à utiliser certains moyens d'action. Mais encore faut-il savoir les produire, et ensuite les distribuer et en rendre possible l'accès. 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 commercialisation 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. C'est via la considération de ces différents points que nous pouvons envisager de construire la souveraineté numérique nécessaire à notre autonomie stratégique. Encore faut-il l'organiser.

Un cadre pour construire la souveraineté numérique dans la durée

Pour élaborer un tel cadre, nous proposons de partir de ce qui existe déjà dans le domaine, en complétant et en s'inspirant de ce qui a été fait dans le secteur de l'énergie, où sécurisation, autonomie, souveraineté, résilience sont aussi des objectifs recherchés. Le cadre proposé repose sur la mise en place d'une organisation systémique, alliant approches descendante (« top-down ») pour la gouvernance et ascendante (« bottom-up ») pour la mise en œuvre, avec une boucle de régulation, et alliant forces vives publiques et privées pour en tirer les avantages de chacun.

Cela conduit à une organisation sous forme d'un triptyque : gouverner (avec un secrétariat général), réguler (avec une commission de régulation), administrer (via décentralisation territoriale et délégations de service public, avec coordination solidaire pour ne pas renforcer les fractures territoriales numériques).

Gouverner et conduire

Créer un Secrétariat général pour la souveraineté numérique (SGSN) permet une coordination étroite des instances de gouvernance. En effet, la mise en œuvre efficace d'une politique de souveraineté numérique passe par une organisation alliant d'une part, gouvernance et conduite, et d'autre part, centralisation des investissements et autonomie territoriale pour l'utilisation. Ceci évite tant la dispersion initiale des efforts technologiques et industriels en conception et réalisation, que l'inertie ultérieure due à un dirigisme excessif ou une méconnaissance de spécificités territoriales en exploitation et utilisation. Le SGSN aurait comme objectif de planifier les étapes de définition capacitaire et de construction budgétaire des axes de la politique de souveraineté numérique. Il aurait également pour mandat de piloter une politique industrielle performante dans la définition et l'exécution des projets structurants via leur responsabilité contractuelle.

Une des premières tâches du SGSN doit être de définir les capacités clés à maîtriser au niveau national, puis les articuler selon des chaînes de valeur cohérente. Un tel exercice de définition capacitaire, accompagné d'une veille stratégique permanente, permet alors de choisir quoi préserver, quitte à renoncer à certains domaines accessoires ou inaccessibles. Par exemple, au niveau

des infrastructures numériques, il est nécessaire de développer un réseau dédié en vue de disposer de moyens de communication sécurisés et résilients, sur l'ensemble des territoires français. La mise en œuvre d'un réseau dédié renforcerait la maîtrise et la protection des infrastructures numériques dans les domaines vitaux de la santé, l'énergie, l'aéronautique et la défense.

Suite à cette réflexion capacitaire, il faut établir une cartographie des acteurs industriels et étatiques, tant sur les technologies maîtrisées que sur les secteurs de vulnérabilité des chaînes de valeur, afin d'appréhender l'empreinte française, voire européenne, dans l'espace numérique. Cette cartographie priorisera les besoins à court et moyen termes pour élaborer la construction budgétaire du réseau résilient des opérateurs d'importance vitale (OIV) de demain. Pour avoir l'effet escompté, une telle politique doit, sur le plan financier, éviter tout saupoudrage et donc amener à des choix et des renoncements, assumés dans la durée.

Enfin, le pilotage des projets structurants exige la priorisation des moyens et la mise en œuvre d'une politique industrielle cohérente. Cela passe par : revoir les dispositifs visant à mettre en synergies les acteurs publics et privés, définir des modes de gouvernance appropriés et mettre en place des structures coopératives dans la durée, sans tomber dans le piège des structures intégratives. La définition et la conduite des projets doivent être coordonnées via le SGSN, afin d'éviter des projets potentiellement concurrents favorisant la dispersion des efforts.

Administrer, opérer et exploiter

Autant la conduite des projets gagne à être centralisée pour pouvoir définir et mettre en œuvre une réelle politique industrielle et pour éviter des doublons potentiels, autant il faut décentraliser et confier à un acteur dédié la gestion, l'exploitation, le soutien des livrables des projets. Cet acteur pourrait être une entreprise (qui pourrait s'appeler RSF – Réseaux sécurisés de France), où seraient présents l'État et la Caisse des dépôts et consignations (CDC). Elle s'appuierait sur des ancrages territoriaux et opérerait dans le cadre d'une délégation de service public conforme à la politique industrielle numérique.

Dans le cadre de la gestion et l'exploitation de l'infrastructure, ses attributions seraient aussi d'entretenir, surveiller (en lien avec les CSIRT en cas d'incident de cybersécurité), moderniser et faire le lien avec les utilisateurs, ainsi que d'élaborer une tarification de l'utilisation des réseaux sécurisés numériques.

Dans le cadre du soutien, elle aurait également la responsabilité des migrations de l'existant, accélérant la transformation de l'État par le numérique et participant ainsi de l'ambition de France 2030. Concernant le financement de l'utilisation des livrables, il doit être à la charge de l'ensemble des acteurs publics (ministères, collectivités territoriales) et des OIV, avec une double logique de forfait de base (proportionnel à la taille de l'acteur concerné) complété par un coût à l'usage. Évidemment, la viabilité de l'ensemble de ces mesures repose sur un cadre législatif astreignant les acteurs concernés à l'utilisation des ressources déployées.

Réguler et normaliser

À l'instar du domaine de l'énergie, où a été mise en place la Commission de la régulation de l'énergie qui a une mission de régulation des réseaux, concourt au bon fonctionnement des marchés et est au service de la transition énergétique, il apparaît nécessaire de créer une Commission de régulation du numérique (CRN).

La CRN assurerait la surveillance de la gestion, la modernisation, le déploiement de l'infrastructure de réseau numérique. Outre la régulation des espaces numériques, elle serait le garant d'une

cohérence globale des référentiels normatifs. En effet, le nombre de normes, référentiels, directives applicables au numérique croît en permanence, couvrant la protection des données (RGPD), l'accessibilité des applications (RGAA), la sécurité des systèmes d'information, l'utilisation de l'Intelligence artificielle (IA), etc.

La CRN aurait donc un rôle clé de cohérence d'ensemble, au service de la transition numérique sous ses différentes dimensions techniques, économiques, sociales, environnementales et de souveraineté. En particulier, elle participerait à certains travaux de normalisation menés au sein des forums internationaux correspondants, et mettrait en place les actions de régulation qui en découlent. Parmi les sujets d'importance pour ces activités, citons le multi-cloud avec une vision particulière liée à la protection des données personnelles et la sobriété énergétique, ainsi que le edge-cloud amené à représenter une nouvelle révolution des usages dans les années à venir avec le développement de l'Internet des objets (IoT) et l'hyperconnectivité.

Ces activités liées à la normalisation sont clé, car si la normalisation est une arme économique pour celui qui la manie, elle est aussi un vecteur de fragilité pour celui qui la subit. D'où l'impérieuse nécessité d'exercer cette volonté de normalisation à une échelle suffisante, a priori européenne plutôt que nationale. Par ailleurs, cela concourt indirectement au soutien à l'innovation technologique et au développement économique d'une partie de la filière numérique.

En guise de conclusion

Ce qui est en jeu 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. La construction d'une souveraineté numérique nationale, amplifiée par la dynamique européenne, doit être le fruit d'une ambition politique forte. Les enjeux sont de taille, et il en est de la posture de la France, comme puissance politique et économique.