MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE
Liberté
Égalité
Fraternité

Conseil général de l'économie

N° 2025/05/CGE/SG

JUILLET 2025

Mission de préfiguration d'un observatoire de souveraineté numérique

Rapport à

Madame la ministre déléguée chargée de l'Intelligence artificielle et du numérique

établi par

Arno AMABILE
Ingénieur en chef des mines

Paul JOLIE
Ingénieur général des mines

Laurent de MERCEY
Ingénieur général des mines

120 rue de Bercy – Télédoc 792 - 75572 Paris Cedex 12

SOMMAIRE

SYNTHESE

La création d'un observatoire de la souveraineté numérique doit permettre de réduire les risques associés à nos dépendances numériques en vue de renforcer la résilience des organisations et l'autonomie stratégique des Etats. Il s'agit d'amorcer un cercle vertueux, où les entreprises et les services publics souhaitent pouvoir acheter des solutions réduisant leurs risques, et trouvent des solutions satisfaisantes dans les offres nationales, européennes ou libres.

Dans une logique de co-construction, la mission de préfiguration de l'observatoire a réuni un groupe de travail constituant un « premier cercle » d'acteurs du numérique : administrations, établissements publics, comités stratégiques de filière, fédérations professionnelles représentant les utilisateurs ou les offreurs de solutions numériques.

Dans ce cadre, cinq besoins à satisfaire pour amorcer le « cercle vertueux » ont été identifiés : des statistiques macroéconomiques pour nourrir le débat public, des méthodes et outils pour que les organisations évaluent leurs dépendances, des catalogues pour qu'elles puissent trouver des offres substituables, des analyses de chaîne de valeur pour identifier les dépendances les plus critiques, enfin des analyses d'écart entre ces offres alternatives et les offres dominantes pour guider l'action publique.

Une liste de produits et services permettant de couvrir ces besoins a été élaborée, et cinq scénarios pour l'observatoire sont proposés : outre les activités de veille et de communication, communes à tous les scénarios, l'observatoire pourrait se concentrer sur l'analyse des chaînes de valeur, sur l'analyse comparative de produits, sur la mise en place d'un label de confiance promouvant la filière française, ou combiner les trois activités précédentes. Il est également envisagé un ensemble d'observatoires spécialisés sur les différents étages de la pile technologique.

Pour chaque scénario, sont précisés les avantages et les difficultés éventuelles, ainsi que des coûts prévisionnels y compris en nombre d'ETP.

*

* *

1 INTRODUCTION

Les technologies numériques sont devenues pour nos sociétés des infrastructures critiques, dans lesquelles les acteurs extra-européens tiennent une place prépondérante. L'importance des dépendances dans le domaine numérique a été particulièrement révélée pendant la pandémie du Covid-19 avec les problèmes d approvisionnement en composants et la réorganisation qui s'en est suivie concernant les chaînes de valeur associées.

Depuis la pandémie, la Commission européenne et les gouvernements européens se sont penchés sur nos dépendances critiques, car elles entraînent une perte de valeur et affaiblissent la résilience des économies européennes en cas de chocs systémiques, avec des coûts allant au-delà des pertes de profit de chaque entreprise.

Les tensions géopolitiques croissantes dans un monde de plus en plus éclaté, et l'accélération de l'intelligence artificielle renforcent la prise de conscience concernant les vulnérabilités des écosystèmes numériques européens. Des initiatives telles que celle d'Eurostack[1] ont soutenu les efforts visant à reprendre le contrôle de la pile technologique.

Le 14 avril 2025, la ministre déléguée chargée de l'intelligence artificielle et du numérique a annoncé le lancement d une mission de préfiguration, d'une durée de trois mois, d'un "observatoire de la souveraineté numérique", confiée au Conseil général de l'économie, l observatoire étant chargé à terme d objectiver nos dépendances critiques dans le numérique et d'identifier des leviers d action permettant d y faire face.

Selon la lettre de mission figurant en annexe, la mission de préfiguration devait aboutir à des propositions concernant le périmètre pertinent de l observatoire, sa gouvernance ainsi que les outils à mettre en œuvre ; elle devait également répondre à un certain nombre de questions relatives notamment à la définition et à la détection des dépendances, aux principales vulnérabilités et à l'émergence de solutions européennes ou souveraines.

[1] EuroStack se présente comme une initiative industrielle et technologique visant à proposer une pile complète de services cloud européens, avec des logiques d'open source et d'interopérabilité. https://www.euro-stack.info/

2 DEROULEMENT DE LA MISSION DE PREFIGURATION

Les dépendances critiques concernant tant les acteurs privés que publics, la mission de préfiguration a réuni, dans une logique de co-construction, à trois reprises en mai et en juin 2025, un groupe de travail constituant un « premier cercle » d acteurs du numérique : administrations (DGE, DGT, DAE, DINUM, ANSSI), établissements publics (INRIA, IMT), comités stratégiques de filière (logiciels et solutions numériques de confiance, industries de sécurité), fédérations professionnelles représentant les utilisateurs ou les offreurs de solutions numériques (CIGREF, Numeum, Hexatrust). Des échanges bilatéraux ont également eu lieu avec plusieurs entreprises et administrations utilisatrices du numérique. Le groupe de travail, réparti en sous-groupes lors des deux premières réunions, s est penché sur les différents types de dépendances critiques et leurs critères d identification, sur les besoins que l observatoire de la souveraineté numérique devrait satisfaire et ses produits de sortie, sur des cas pratiques à tester, sur l articulation de l observatoire avec des organismes existants, enfin sur des scénarios pour le périmètre et le positionnement de l observatoire. La mission a pu constater que la création d'un observatoire de la souveraineté numérique représentait une véritable attente pour l'ensemble de ses interlocuteurs, même si les points de vue pouvaient différer sur les scénarios de mise en œuvre.

Le cabinet de la ministre a été tenu régulièrement informé de l'avancement des travaux. Le 2 juillet 2025, à l occasion de l'événement *Independance Tech Day* organisé par Alliancy[2] et la Caisse des dépôts et consignations sur les enjeux des dépendances technologiques, le CGE a brièvement présenté les résultats des travaux et la ministre a confirmé la création de l observatoire de la souveraineté numérique avec comme principales missions attendues de celui-ci : objectiver les dépendances, consolider le catalogue des solutions existantes.

[2] Média spécialisé dans la transformation numérique

3 LA NOTION DE SOUVERAINETE NUMERIQUE

La souveraineté numérique nécessite de gérer les risques liés aux dépendances critiques

De l'avis des acteurs rencontrés, la souveraineté numérique est avant tout **un attribut des États ou de collectifs d'Etats** comme l'UE, capables de faire des choix technologiques indépendants et réversibles, de choisir et de gérer leurs dépendances.

La souveraineté numérique d'un État est toutefois liée aux dépendances numériques critiques de ses services publics et des entreprises présentes sur son sol, qui elles-mêmes dépendent des offres pertinentes existantes. **Une dépendance devient critique lorsqu'elle expose l'Etat, des entreprises ou des services publics à un risque jugé inacceptable**. Il existe quatre types de risques, résumés ci-dessous.

Il est important de noter que **tous les acteurs n'ont pas intérêt à gérer tous les risques**. Les entreprises cherchent surtout à éviter une captation excessive de la valeur et à ne pas s'empêtrer dans des conflits géopolitiques. Pour distinguer ces risques de ceux qui intéressent principalement les gouvernements, nous pouvons **utiliser les notions de résilience et d'autonomie stratégique**.

	Niveau où s'applique le risque	
Type de risque	Organisation	Système (Pays ou collectif)
Economique	**Captation de valeur excessive** : la position dominante du fournisseur lui permet d'augmenter ses prix (par exemple VMWare) ou de captation de la valeur par le biais de données obtenues illégalement. Elle peut exposer l'entreprise à la législation d'un pays tiers.	**Dépendance technologique** : les profits, les données, le savoir-faire et les talents sont drainés à l'étranger, légalement et parfois même illégalement. Cela entrave la capacité à maîtriser les prochaines vagues technologiques. **Point de défaillance unique** : l'interruption involontaire du service met en péril des pans entiers de l'économie en une seule fois
Politique	**Pression géopolitique** : l'entreprise/les services publics dépendants deviennent une monnaie d'échange dans une négociation (par exemple menace d'interruption de service)	**Perturbation politique** : la concentration de l'écosystème dans un autre pays accroît la difficulté de le réglementer (par exemple les réseaux sociaux)
	Résilience	Autonomie stratégique
	Objectif visé par la réduction des risques	

Un cas d'actualité illustre l'inconvénient des dépendances : à la suite de l'acquisition fin 2023 de VMware, fournisseur de services de virtualisation, par Broadcom, les clients de VMware se sont vu imposer une nouvelle offre commerciale remplaçant la vente de licences perpétuelles par une souscription annuelle. Au lieu de la granularité des offres qui prévalait, le catalogue des solutions VMware consiste désormais en un petit nombre de *bundles*[3], avec des tarifs beaucoup plus élevés. Les entreprises clientes se trouvent donc confrontées à un dilemme : rester avec VMware en payant le prix fort, ou en sortir à l'issue d'une transition complexe de plusieurs années.

La souveraineté numérique n'est pas un label, c'est un cercle vertueux qu'il faut amorcer

Gérer ces risques de dépendances numériques a un coût, qui peut devenir prohibitif. Tout comme pour les dépendances en matière de médicament, de masques, d'énergie ou de produits agricoles, **la souveraineté numérique ne correspond pas à l'autarcie mais à un point d'équilibre jugé satisfaisant au vu des risques et du coût pour les réduire**. Ce point d'équilibre peut varier :

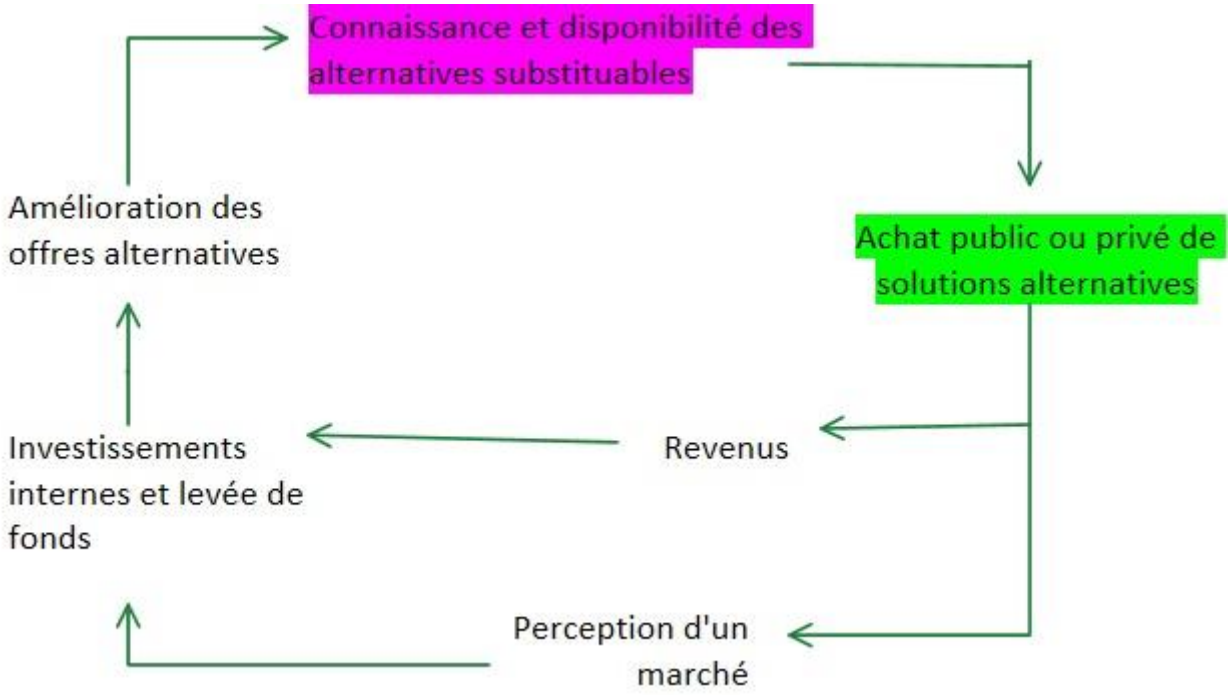
- Dans l'espace, tous les pays n'ayant pas les mêmes ressources, la même exposition ou la même perception de ces risques
- Dans le temps, parce que les risques qui semblaient acceptables hier ne le sont plus aujourd'hui ou parce que le coût de réduction du risque qui était abordable hier ne l'est plus aujourd'hui.

Ce caractère dynamique explique la difficulté à "définir" la souveraineté numérique de manière générale à partir de critères précis, sauf de façon maximaliste. Les efforts de définition[4] tendent à accumuler des critères, réduisant la capacité à agir ou à prioriser certaines dimensions. **Plutôt que de faire de la souveraineté numérique une ligne d'arrivée, un endroit à définir avant de commencer à nous y diriger**, il serait plus productif de se concentrer sur la dynamique des dépendances.

L'objectif est d'inverser le cycle par lequel notre dépendance numérique se renforce de jour en jour. **Il s'agit d'amorcer un "cercle vertueux de la souveraineté numérique", où les entreprises et les services publics souhaitent réduire leurs risques en achetant des solutions alternatives (nationales, européennes ou libres selon les cas), et peuvent le faire car ils trouvent des offres substituables.**

[3] Regroupement de produits proposés à la vente de manière conjointe

[4] Voir par exemple https://euro-stack.com/blog/2024/9/draft-sovereignty-criteria-software-digital-systems



- **L'exemple de l'informatique en nuage**

Il n'existe pas de définition officielle du nuage souverain - chaque pays possède son propre ensemble de réglementations en matière de confidentialité et de protection des données. Les DSI doivent interpréter ces réglementations lorsqu'ils décident de la manière dont les données sont stockées et traitées, et qui peut y accéder. Le cabinet d'études de marché Omdia a identifié sept caractéristiques clés de ce que tout nuage souverain doit offrir. L'importance de ces caractéristiques dépend des réglementations locales.

Confidentialité des données : Elle couvre la manière dont les données sont protégées, les personnes qui y ont accès et la manière dont l'accès est contrôlé et signalé.

Le **contrôle juridictionnel** : Il couvre les aspects de propriété et d'exploitation du nuage souverain et, plus précisément, la question de savoir qui a le contrôle sur ces aspects. Il s'agit également de déterminer s'il est possible d'empêcher l'accès extraterritorial.

Offres de services : Les nuages publics offrent une pléthore de services différents que les clients peuvent utiliser. Pour les nuages souverains, nous examinons les offres de services et l'étendue des services disponibles pour les clients.

Compétence opérationnelle : Les considérations opérationnelles liées à l'exploitation et à l'utilisation d'un nuage souverain couvrent des aspects tels que la sauvegarde et la récupération, les solutions tierces et la tarification.

Couverture et utilisation : Ce domaine examine dans quelle mesure la solution de cloud souverain est applicable aux différents pays et combien de pays utilisent le cloud souverain.

Stratégie et exécution : Elles évaluent la manière dont le fournisseur d'informatique en nuage envisage l'informatique en nuage souveraine et la manière dont il répond au marché et aux différentes exigences.

Impact sur le marché : Ce domaine examine la manière dont l'approche du fournisseur de services en nuage est perçue par les clients.

4 L'INTERET D'UN OBSERVATOIRE DE LA SOUVERAINETE NUMERIQUE

Cinq besoins à satisfaire pour amorcer le cercle vertueux

Le "cercle vertueux de la souveraineté numérique" est aujourd'hui trop faible, quand il n'est pas à l'arrêt. L'écosystème national, européen ou open source a moins de clients que l'écosystème américain ou chinois, et dispose donc de moins de revenus ou de fonds à investir dans l'amélioration de ses solutions. Les causes sont diverses et bien connues, qu'il s'agisse d'un départ plus tardif, d'un financement moins important, de pratiques anticoncurrentielles de la part des acteurs dominants, etc.

Où commencer pour amorcer ce cercle vertueux ? A quel endroit de la pile technologique, pour quel produit ? Où est-il indispensable d'avoir un appui ou une intervention publique ? Ce sont ces questions qui ont conduit à la création de l'observatoire de la souveraineté numérique.

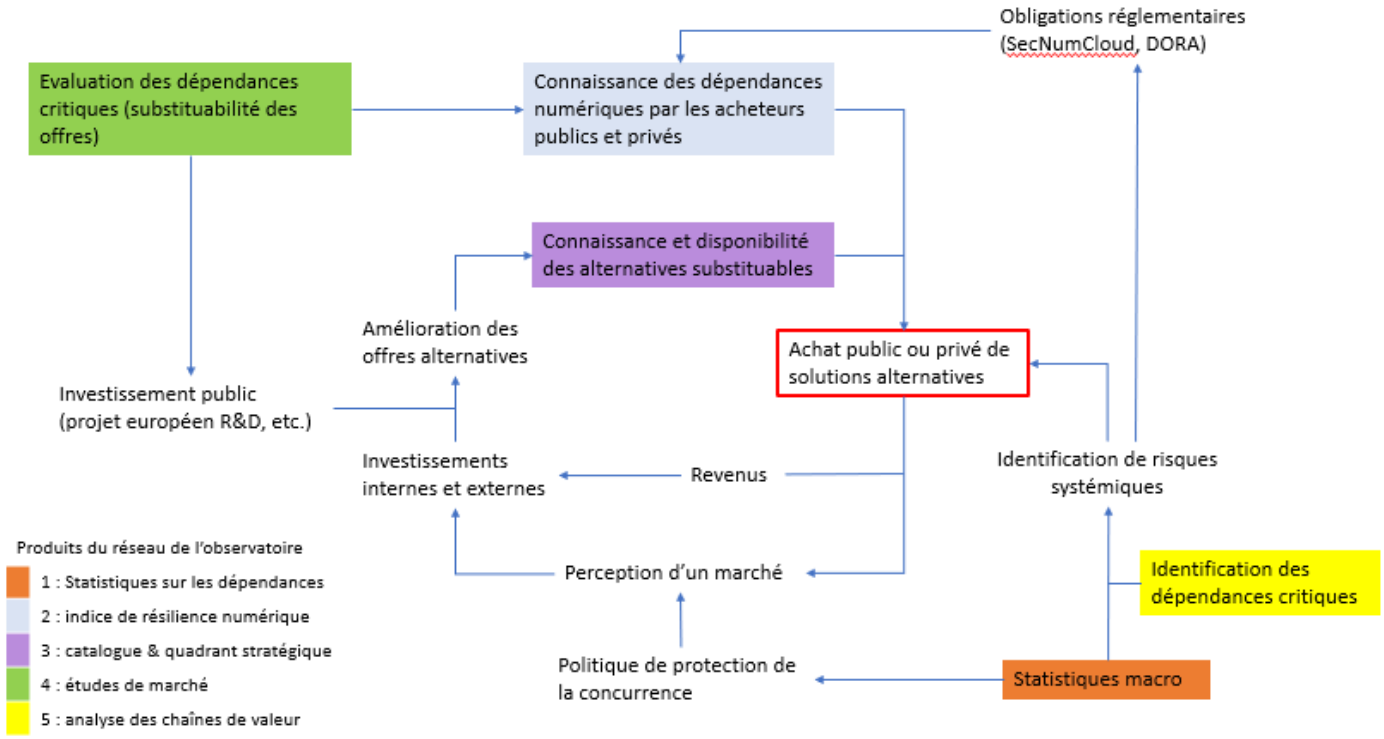
Dans le cadre de la préfiguration de l'observatoire, cinq besoins à satisfaire ont été identifiés :

1. Les gouvernements ont besoin de **statistiques macroéconomiques** pour évaluer la profondeur et le coût d'opportunité de leurs dépendances numériques, afin d'identifier les risques systémiques, d'établir des priorités et d'orienter leurs actions (obligations réglementaires, politique concurrentielle).
2. Les services publics et les entreprises ont besoin d'**outils, méthodes** pour évaluer leurs propres dépendances afin de gérer leurs risques et de suivre leurs progrès.
3. Les services publics et les entreprises ont besoin de **catalogues hiérarchisés** pour connaître les offres alternatives, évaluer leur qualité et réduire concrètement leurs dépendances.
4. Les gouvernements, les services publics et les investisseurs ont besoin d'une **analyse des écarts** pour évaluer objectivement la distance entre les offres dominantes actuelles et les alternatives européennes ou à source ouverte. Cela aidera à concevoir des politiques publiques et ne doit pas être exhaustif sur l'ensemble de la chaîne de valeur.
5. Les gouvernements, les entreprises et les services publics ont besoin d'**analyses de chaîne de valeur** pour identifier leurs dépendances critiques, y compris les plus difficiles à déceler. Ils doivent pouvoir le faire de façon prospective.

Certains de ces produits peuvent être mieux réalisés non pas par une entité publique mais par un fournisseur privé ou un consortium. Ils peuvent contenir des analyses sensibles et donc nécessiter une distribution limitée, soit pour des raisons de sécurité nationale, soit pour des raisons de protection commerciale.

Note : d'autres besoins sont (i) une meilleure coordination des stratégies au sein du gouvernement afin que (par exemple) la politique de soutien aux start-ups ne renforce pas involontairement les dépendances, (ii) l'aide aux services publics dans la conception de la stratégie de démarrage, (iii) la mise en place d'un système de gestion de l'information.

L'observatoire et son réseau visent à activer des leviers pour renforcer le cercle vertueux de la souveraineté



Quels produits pour répondre à ces besoins ?

Qu'est-ce qui a déjà été fait au niveau européen ?

Les travaux menés par la Commission européenne ces dernières années se sont concentrés sur :

- les dépendances dans des domaines d'importance stratégique pour l'UE (sécurité, sûreté, santé et transformation verte et numérique)
- la lutte contre les risques de point de défaillance unique et de dépendance technologique.

Au moyen du DMA et du DSA, la Commission européenne a mis en œuvre des outils de régulation visant à atténuer les risques de captation excessive de valeur et de perturbation politique, respectivement.

Le contexte géopolitique et l'accélération de l'IA ont eu deux effets :

- **L'intérêt des entreprises individuelles pour l'amélioration de leur résilience a augmenté**, car les coûts d'une captation excessive de valeur et le risque d'une pression géopolitique se sont accrus.
- **L'intérêt des gouvernements européens à renforcer leur souveraineté a augmenté**, car le coût de la dépendance technologique et le risque de perturbations politiques ont augmenté.

Des produits et des services concrets

Besoin 1 - Des statistiques macroéconomiques

- **Pourquoi ?** En l'absence de données sur le niveau de nos dépendances et le coût que cela représente, il nous est difficile de porter la réduction des dépendances au niveau politique, d'en assumer les coûts ou les contraintes, et d'en mesurer les progrès
- **Qu'est-ce qui existe ?** Les données disponibles sur les services numériques sont très parcellaires et ne permettent pas de produire ces statistiques, d'où des sondages sectoriels. A partir de 2029, les instituts statistiques européens et nationaux devraient intégrer des statistiques bien plus riches sur les échanges de services numériques
- **Quel rôle pour un observatoire public ?**
    - A partir de 2029, la production de ces statistiques doit être assurée par les instituts (Banque de France, INSEE) étant donné le savoir-faire nécessaire. L'observatoire n'aurait donc pas besoin de réaliser cette mission.
    - D'ici à 2029, l'observatoire pourrait dans son rôle de coordination aider la Banque de France et l'INSEE à réaliser avec des organismes professionnels des sondages permettant d'affiner les premières estimations et de les porter au niveau européen (en lien avec les acteurs d'Eurostack)

Besoin 2 - Des méthodes et des outils pour identifier ses dépendances et évaluer sa résilience

- **Pourquoi ?** Des entreprises et services publics souhaitent agir mais n'ont pas de repères sur le sujet de la résilience numérique. Comme il a fallu inventer une manière d'évaluer le bilan carbone, le travail est à faire pour la résilience.
- **Qu'est-ce qui existe ?** Un collectif d'entrepreneurs et think tank produit actuellement avec une dizaine de grandes entreprises partenaires une méthode pour un "indice de résilience numérique[5]" qui serait ouverte à toute entreprise souhaitant s'en saisir. Cet indice s'appuierait d'une part sur quatre critères quantitatifs qui mesurent factuellement l'indépendance du système d'information de l'organisation, à trois différentes échelles (nationale, européenne, extra-européenne), d'autre part sur quatre critères qualitatifs évaluant, quant à eux, la culture et l'organisation de l'entreprise vis-à-vis des enjeux numériques.
  Des entreprises comme societe.com préparent un service d'évaluation de la résilience numérique et pourraient se servir de ces méthodes.
- **Quel rôle pour un observatoire public ?** Les situations à prendre en compte seront très variées, et les débats seront nombreux autour de ces indicateurs. Il est préférable pour les premiers travaux de laisser une démarche ouverte se mettre en place dans l'écosystème, l'Etat pouvant être simplement associé, notamment pour aider à la convergence vers un référentiel unique. Les entreprises indiquent être prêtes à payer pour un « audit » de leur situation, mais ne pensent pas pertinent ou faisable que cette prestation vienne d un observatoire public.

Besoin 3 - Des catalogues hiérarchisés

- **Pourquoi ?** Les offres alternatives, qu'elles soient françaises, européennes, open source ou bénéficiant d'un label particulier (SecNumCloud), ne sont pas toujours connues. Surtout, les décideurs peuvent avoir du mal à identifier la meilleure des solutions alternatives.

[5] Voir le communiqué de presse : https://assets.rte-france.com/prod/public/2025-07/2025-07-04-cp-indice-resilence-numerique.pdf

- **Qu'est-ce qui existe ?** Les CSF produisent des catalogues de solutions, tandis que des acteurs américains (Gartner) ou européens (PAC/CXP) classent des offres, mais sans y introduire des critères liés à la résilience numérique. Des personnalités autour d Eurostack ont proposé des grilles d analyses des offres (cf. l'annexe 4).
- **Quel rôle pour un observatoire public ?**
    - Option 1 : l'observatoire laisse l'écosystème (CSF, prestataire privé de type Gartner) créer et distribuer un catalogue, afin d'éviter de subir des pressions de la part d'offreurs pour être inscrits dans le catalogue. Les entreprises s affirment prêtes à acheter ce genre de catalogue s il paraît crédible.
    - Option 2 : l'observatoire coordonne la création d'un label "souverain" ou "résilient" permettant d'identifier certaines offres. Les entreprises ne semblent pas prêtes à acheter un « catalogue d offres labellisées » à un observatoire public.

Besoin 4 - De l'analyse comparative des offres

- **Pourquoi ?** Plusieurs leviers publics existent pour agir sur les achats d'offres alternatives (subvention, action contre un abus de position dominante, programme de recherche, contrainte réglementaire ou achat public). Afin d'évaluer leur pertinence, il est crucial d'évaluer les raisons (techniques et commerciales) qui conduisent les acheteurs à acheter des offres dominantes.
- **Qu'est-ce qui existe ?** De façon ad hoc, la DGE ou l'Autorité de la Concurrence réalisent des études de marché pour comparer des offres.
- **Quel rôle pour un observatoire public ?** Dans les deux cas il s agit d'abord d'un besoin pour les décideurs publics, que les entreprises ne paraissent pas prêtes à financer.
    - Option 1 : l'observatoire acquiert les compétences afin de pouvoir réaliser ces analyses comparatives à la demande des décideurs publics
    - Option 2 : l'observatoire s'appuie sur un réseau d'observatoires "fils" et spécialisés

Besoin 5 - De la veille pour repérer les dépendances critiques profondes

- **Pourquoi ?** Certaines actions (protection du patrimoine, gestion du risque dans les services publics) nécessitent de repérer aussi tôt que possible des dépendances critiques, y compris en constituant des bases de données sur les différentes couches et briques
- **Qu'est-ce qui existe ?** De façon ad hoc, le ministère de l'économie ou le ministère de la défense et certaines fédérations professionnelles ou filières peuvent réaliser des analyses sur les chaînes de valeur
- **Quel rôle pour un observatoire public ?** Les options sont les mêmes que pour le besoin 4, mais les entreprises pourraient être prêtes à participer au financement de ces analyses. Toutefois, il est peu probable que cela couvre plus d un tiers du coût de fonctionnement de l observatoire.

5 LES CINQ SCENARIOS POSSIBLES POUR L'OBSERVATOIRE

5.1 Cadrage

L'Observatoire français des ressources minérales pour les filières industrielles (OFREMI), cité en exemple dans la lettre de mission, compte une quinzaine d'agents. Cependant, de l'avis de la mission, la "complexité" de l'activité de l'OFREMI (impliqué dans le suivi des minerais stratégiques dans leur cycle de vie) correspond à une seule couche de la pile technologique du numérique. Or, il y a au minimum une dizaine de couches pour appréhender l'industrie du numérique dans son ensemble. Et celles-ci peuvent être décomposées chacune en plusieurs sous-couches, pour certaines d'une grande complexité.

	Scénario 1 « BDD »	**Scénario 2 « Bureau d'étude »**	**Scénario 3 "Label"**	**Scénario 4 "Intégré"**	**Scénario 5 "Réseau"**	**Privé achèterait le produit ?**	**Privé achèterait à l'observatoire public ?**
1 - Statistiques	Instituts	Instituts	Instituts	Instituts	Instituts	Non (fédé ?)	Non
2 - Méthode & indicateur	Ecosystème	Ecosystème	Ecosystème	Ecosystème	Ecosystème	Evaluation dans son cas	Non
3 - Catalogue & radar	Ecosystème	Ecosystème	Label public	Label public	Ecosystème	Oui	Non
4 - Analyse comparative		Oui		Oui	Oui, via un réseau	Non	Non
5 - Analyse chaîne valeur	Avec base de données			Avec bases de données	Idem, en réseau	Oui	Faible
Veille & Com	Oui	Oui	?	Oui	Oui	Faible	Faible
ETP (hors veille)	10	11	2	27	2		
Budget presta	100 k€	5 M€	1 M€	6 M€	500 k€		

Tous les scénarios présentés ici intègrent deux activités considérées comme incontournables, en l'occurrence une activité "veille et alertes" ainsi qu'une activité "communication", sous la forme par exemple d'une lettre hebdomadaire envoyée par mail (aux abonnés) qui présenterait les événements marquants de la semaine dans le domaine du numérique en l'évaluant sur une échelle de 1 à 10 en termes d'impact. Ces deux activités représentent un coût fixe évalué à 3 ETP et 100 k€ de fonctionnement par an, en intégrant la dimension gouvernance de l'observatoire (préparation et animation des réunions du conseil d'administration).

Comme le montrent les deux dernières colonnes du tableau de synthèse des scénarios, il y a peu de produits que les entreprises seraient prêtes à payer s'ils étaient réalisés par un observatoire public.

L'observatoire devrait avoir deux modes de fonctionnement :

- Mode 1 : il s'agit d'un mode permanent d'enrichissement de la connaissance. La question de savoir si l'observatoire doit gérer des bases de données est entière. Sans doute devrait-il le faire sur des sujets qui ne sont pas documentés dans des bases de données existantes (Banque de France / INSEE / etc.).

- Mode 2 : il s'agit d'un mode projet dans lequel un sujet est identifié (par exemple décrire la chaîne de valeur du cloud et analyser les dépendances) et traité par l'observatoire dans une logique de mobilisation d'experts du sujet. Un chef de projet est nommé au sein de l'observatoire ; il est responsable d'un ou plusieurs sujets et gère tous les aspects capitalisation de connaissance. Nous envisageons qu'une dizaine de sujets puissent être traités en parallèle chaque année, représentant un coût prévisionnel d'environ 10 ETP. Les sujets sont choisis par la gouvernance mais des sujets "urgents" (peu nombreux) peuvent être traités en "circuits courts".

5.2 Scénario 1 – « Base de données »

Idée principale

Dans ce scénario, l'observatoire, outre son activité de veille, développe une compétence pour analyser les chaînes de valeur. Dans la durée, l'observatoire a une connaissance fine des chaînes de valeur numériques de l'industrie. L'observatoire comprend les rapports de force, les lock-in existants ou à venir.

Deux niveaux d'analyse pourraient être réalisés.

- Une analyse « macro » de la chaîne de valeur qui permet d'identifier les acteurs (en particulier français). Une base de données pourra être construite à cette fin pour chaque chaîne de valeur et maintenue au profit des entreprises cherchant des solutions proposées par des entreprises françaises ou européennes. Ce niveau d'analyse pourra être public.
- Des analyses fines permettant d'analyser les rapports de force et les jeux de dépendances des acteurs. Ce travail étant stratégique, il serait prudent de le classifier (secret) et d alimenter les décideurs ministériels et des entités du type SISSE (pour protéger les entreprises considérées comme stratégiques dans la chaîne de valeur)

Ces travaux se feraient avec les filières dans une démarche projet (1 projet = 1 analyse de chaîne de valeur). A noter qu''il faudra un certain niveau de maturité et une méthodologie pour réaliser ces travaux. L'observatoire pourrait apporter la méthodologie.

Avantages du scénario

Cette activité de représentation des chaînes de valeur et de leur analyse devrait permettre de mieux comprendre les flux de valeurs, les dépendances, les stratégies d'acteurs et l'émergence des lock-ins.

Difficultés éventuelles

Ces travaux sont difficiles à réaliser et supposent la mobilisation d'experts du sujet (la chaîne de valeur de la cybersécurité n'a rien à voir avec la chaîne de valeur des composants).

Il existe déjà des travaux de ce type qui sont répartis dans différentes entités en France (ex : DGE, Banque de France, SISSE, Comités stratégiques de filières …). Il ne s'agit pas de refaire ce qui existe.

Il sera difficile de traiter l'univers numérique rapidement. Il faudra faire un choix de priorité sur quelles chaînes de valeur se concentrer dans un premier temps. La roadmap des analyses à mener pourrait se faire via la gouvernance de l'observatoire.

Coût prévisionnel

- 3 ETP pour l'activité de veille et alerte
- Le coût de construction d'une base de données (sur un étage de la pile technologique) est estimé à 1 homme-an. La maintenance d'une telle base à 1 homme-mois.
- Il y aura des dépenses de fonctionnement informatique à prendre en compte.
- Si l'on part sur une activité correspondant à une analyse de la pile technologique, sur la base d'une pile technologique de 10 étages, il faut compter 10 ETP (1 personne par étage). La description des chaînes de valeur se ferait par animation de groupes de travail impliquant d'autres entités (ex : CEA LETI sur le Hardware), dont la force de travail est considérée comme "gratuite" dans cette présentation.
- 2 ETP supplémentaires permettront de faire des analyses "transverses" c'est-à-dire prenant en compte plusieurs étages de la pile.

5.3 Scénario 2 – « Bureau d'étude »

Idée principale

Outre son activité de veille (générique à tous les scénarios), les sujets que traite l'observatoire sous forme de projets dans ce scénario sont des analyses comparatives de produits, permettant de mieux positionner les produits français ou européens par rapport à leurs concurrents.

L'idée de départ est que si l'on compare brutalement les produits de Microsoft aux autres, les produits Microsoft sont supérieurs car offrant plus de fonctionnalités. De plus, si un produit concurrent de Microsoft se positionne pour offrir une différenciation, Microsoft va utiliser une "stratégie de bundle" pour forcer l'achat de SA solution à ses clients plutôt que l'achat de la solution concurrente (cas d'école de l'entreprise Jalios dans sa concurrence avec Sharepoint, Microsoft faisant un bundle avec Office365)

Mais est-ce cela dont ont besoin les entreprises ?

Ici l'observatoire développe une démarche marketing (la question n'étant pas que technique) pour mieux identifier les outils dont les entreprises ont besoin, montrer que les produits étrangers ne sont pas forcément les mieux placés et développer des actions pour faire migrer les utilisateurs des entreprises françaises vers des produits français.

Avantages du scénario

Ce scénario permet de bien positionner l'observatoire par rapport à la DGE qui souhaite garder l'activité de l'analyse des chaînes de valeur pour elle.

L'idée serait, une fois l'identification produit/entreprise française réalisée, de rentrer dans une dynamique d'adoption par l'Etat avec l'appui de la DINUM. Un indicateur de mesure des efforts d'accompagnement de l'Etat pourrait être mis en place.

L'Etat donnant l'exemple, d'autres entreprises devraient suivre.

Cette méthodologie, si elle avait été mise en place plus tôt, aurait permis de mieux choisir les entreprises pouvant répondre aux problématiques posées par le Health DataHub.

Difficultés éventuelles

L'analyse comparative des produits n'est pas facile, d'autant qu'il faut avoir accès aux fiches techniques desdits produits. Une entreprise comme Yole en France s'est spécialisée sur ce sujet sur la niche des composants électroniques et fait un travail remarquable, basé sur du retro-engineering.

L'acquisition de compétences sur ce sujet sera un challenge pour l observatoire.

L'activité est proportionnelle aux ressources dont disposera l'observatoire. On peut penser à utiliser de la sous-traitance pour augmenter le nombre d'analyses.

Coûts prévisionnels

- Coût fixe de 3 ETP pour assurer la veille et les alertes.
- Le traitement d'une analyse produit et de stimulation de son usage est évaluée à 1 ETP et 500 k€ de sous-traitance a minima.
- Pour 10 sujets par an, il faut donc compter 10 ETP et 5 M€ de fonctionnement.

5.4 Scénario 3 – « Label »

Idée principale

L'observatoire, outre son activité de veille, essaie dans ce scénario de redonner un sens au mot "souveraineté" et des repères pour les entreprises qui souhaiteraient construire ou utiliser des solutions souveraines dans le monde numérique. En effet, le constat est que le mot souveraineté est devenu un mot valise et utilisé aujourd'hui dans une large acception, tout le monde devenant "souverain by design", y compris des acteurs comme AWS ou Microsoft…

L'observatoire dans ce scénario, a autant de compétences marketing que technologiques.

L'observatoire a donc un rôle très important à jouer dans le narratif pour accroître la confiance.

Dans ce scénario, outre son activité de veille, l'observatoire pourrait être à l'origine de différents produits visant à améliorer la confiance en la souveraineté française (et européenne).

Un produit possible pourrait être la mise en place d'un label de confiance (complémentaire de SecNumCloud) dans une démarche identique à une démarche qualité pour obtenir un label ISO9000. Il s'agirait de développer un label « Sovereign French Tech » promouvant la filière française.

Un radar des entreprises labellisées souveraines serait également produit.

D'autres produits pourraient être imaginés pour renforcer cette dynamique souveraineté.

Avantages du scénario

Dans ce scénario, une grande partie de l'activité est portée par le secteur privé, qui, via le processus de labellisation permettra de "garantir" le fait que les composants d'une solution ne dépendent pas d'acteurs étrangers.

Ne pourront utiliser le label que les sociétés labellisées, ce qui renforcera le concept de souveraineté.

Difficultés éventuelles

S'il faut développer ce label, cela peut prendre plusieurs mois/années. Il faudra de plus être en capacité de développer un écosystème d'entreprises capables de labelliser les entreprises qui le souhaiteront.

Coûts prévisionnels

- L'activité de veille est évaluée à 3 ETP
- La mise en place d'un tel observatoire est évaluée à 2 ETP supplémentaires et 1 M€ de fonctionnement par an.

5.5 Scénario 4 – « Intégré »

Idée principale

Dans ce scénario, on considère que les trois activités précédentes présentées dans les scénarios 1,2 et 3 sont éligibles comme activités de l'observatoire et que l'observatoire est dimensionné pour les assurer.

Avantages du scénario

Une plus grande capacité de production, avec une panoplie de produits et services pour l'écosystème français.

Difficultés éventuelles

La construction de l'observatoire peut être difficile.

Coûts prévisionnels

Il faudrait imaginer un observatoire de l'ordre d'une trentaine de personnes avec des moyens financiers importants (plusieurs millions d'euros) et une capacité informatique dédiée.

5.6 Scénario 5 – « Réseau »

Idée principale

Dans ce scénario, il n'y a pas UN observatoire mais un ensemble d'observatoires (dont le nombre peut varier au cours du temps) qui sont organisés autour d'une tête de réseau, qui gère l'animation des différents observatoires, les aspects gouvernance et le suivi des projets.

Le choix des observatoires pourrait se faire suivant une logique "technologique", c'est-à-dire un observatoire positionné sur chaque étage de la pile technologique (par ex : CEA-LETI sur l'étage Hardware).

Avantages du scénario
Les dossiers sont maîtrisés par des équipes spécialistes du sujet et sont donc plus facilement mobilisables.

Il est possible de traiter des sujets de type "analyse de chaîne de valeur" aussi bien que des sujets "analyse comparative de produits", voire d'autres sujets plus "ésotériques"…

Chaque observatoire gère les bases de données sur le périmètre qui le concerne (ce qui peut faire des économies par mutualisation du SI de l'observatoire avec celui de l'entité qui l'héberge).

Le modèle d'organisation est facilement "scalable". Dans l'hypothèse où il faudrait dans le futur faire un zoom sur un nouveau domaine (par exemple : robots humanoïdes), la désignation d'un nouvel observatoire permet de mobiliser rapidement des ressources sur le sujet.
On peut imaginer de traiter de façon parallèle une dizaine de sujets dans chaque observatoire. S'il y a 10 observatoires fils, cela permet de traiter 100 sujets par an. Les sujets "transverses à la pile technologique" sont pris par la tête de réseau.

Difficultés éventuelles
Ce scénario présuppose qu'il n'y a pas ou peu d'interdépendance entre les différents étages de la pile technologique, ce qui n'est pas évident. Par ailleurs, la désignation d'un observatoire pour un étage particulier peut être délicat. Par exemple dans le cas de la désignation du CEA-LETI sur l'étage hardware pourrait être contesté par le CNRS.

La gouvernance serait assurée via un conseil d'administration auquel participeraient les différents observatoires fils. C'est lors de ce CA que seraient fixés les sujets à traiter.

Coûts prévisionnels
La tête de réseau est évaluée à 5 ETP (3 ETP fixe + 2 ETP animation de réseau et projets transverses) + 500 k€.

Il faudra décider d'abonder chaque observatoire fils. Une dotation de 2 ETP semble un bon compromis. Sachant que chaque observatoire devra "abonder" de façon complémentaire avec des ressources en propre pour gérer la dizaine de sujets qui lui sera commandée. Soit pour une dizaine d'observatoires, 20 ETP supplémentaires à prévoir.

ANNEXES

Annexe 1 : Lettre de mission

MINISTÈRE
CHARGÉ DE L'INTELLIGENCE
ARTIFICIELLE
ET DU NUMÉRIQUE
Liberté
Égalité
Fraternité

Paris, le 14 avril 2025

Monsieur le Vice-Président,

La succession des crises récentes – pandémie de la Covid-19, guerre en Ukraine, tensions géopolitiques affectant les chaînes de valeur mondiales – a mis en lumière la nécessité d'intégrer pleinement les enjeux de résilience et de souveraineté dans notre stratégie économique. Ces événements ont révélé, parfois avec brutalité, la profondeur de certaines dépendances stratégiques, qu'elles soient industrielles, énergétiques ou numériques.

Dans un contexte où les technologies numériques sont devenues des infrastructures critiques de nos sociétés, la France, comme l'ensemble de l'Union européenne, doit se doter des moyens d'identifier, de comprendre et de maîtriser ses vulnérabilités. La concentration des capacités de production manufacturière en Asie, et le rôle prépondérant d'acteurs extra-européens dans nos systèmes numériques, interrogent directement notre autonomie stratégique.

La souveraineté numérique, entendue comme la capacité à faire des choix technologiques libres, éclairés et réversibles, constitue dès lors un pilier essentiel de notre sécurité économique, de la protection de nos données, et de la défense de nos valeurs démocratiques. La panne massive survenue en juillet 2024, causée par un prestataire de Microsoft, a illustré de manière spectaculaire notre degré de dépendance à des solutions que nous ne maîtrisons pas.

Face à ces constats, la France a engagé depuis plusieurs années des actions concrètes pour renforcer sa résilience numérique : référentiel SecNumCloud porté par l'ANSSI, promotion des logiciels libres dans l'administration, soutien à des filières industrielles européennes via le plan d'investissement France 2030. À l'échelle européenne, les textes fondateurs que sont le RGPD, le DSA et le DMA participent à la construction d'un espace numérique plus souverain et plus équilibré. Ces initiatives s'inscrivent dans le cadre d'une stratégie industrielle européenne renforcée, visant à accroître la résilience et la compétitivité de l'Union, tout en préservant une économie ouverte. Elles reflètent l'engagement de l'UE en faveur d'une autonomie stratégique ouverte, qui concilie souveraineté économique et coopération internationale.

Dans cette perspective, il devient nécessaire de structurer davantage notre action, de valoriser et de mutualiser les expertises existantes, et de doter l'État d'un dispositif pérenne de suivi et d'analyse systémique des dépendances technologiques et numériques. De nombreuses institutions – telles que l'INRIA, le CEA, la DGE, la DGT, l'ANSSI, la CNIL, l'ARCOM, l'ADEME, la DINUM, le SGDSN, France Stratégie ou encore le CNRS– contribuent d'ores et déjà à l'identification et à l'évaluation des dépendances numériques de l'État et de l'économie français. Il est désormais temps de leur donner un cadre lisible, fédérateur et pérenne.

C'est pourquoi j'ai décidé de vous confier une mission de préfiguration d'un Observatoire de la souveraineté numérique, chargé à terme d'objectiver nos dépendances critiques, d'identifier les leviers d'action, et de contribuer à l'élaboration de politiques publiques fondées sur une expertise transversale, structurée et opérationnelle. Cet observatoire pourrait s'inspirer de la mise en place de l'OFREMI sur le sujet des ressources minérales.

Cette mission devra aboutir à des propositions concernant :

- Le périmètre pertinent de l'Observatoire (enjeux technologiques couverts, articulation avec les organismes existants) ;
- Sa gouvernance et ses modalités de coordination interministérielle ;
- Les outils d'analyse, de cartographie, de veille et de prospective qu'il conviendrait de mettre en œuvre ;
- Les modalités d'ouverture vers les écosystèmes industriels, académiques et européens.

À cette fin, l'étude devra notamment répondre aux questions suivantes :

- Quels critères permettent de définir une dépendance technologique ou numérique critique ?
- Quelles sont aujourd'hui les principales vulnérabilités françaises et européennes en matière de logiciels, matériels, données, infrastructures, compétences et gouvernance ?
- Quelles méthodologies et quelles sources de données publiques et privées peuvent être mobilisées pour assurer une vision exhaustive et dynamique des chaînes de dépendance ?
- Comment garantir la complémentarité de l'Observatoire avec les missions assurées par l'ANSSI, la DINUM, la CNIL, France Stratégie ou encore le SGDSN ?
- Quels sont les leviers permettant de favoriser l'émergence de solutions européennes ou souveraines, dans une logique de codépendances maîtrisées et de compétitivité industrielle ?

Je vous invite à inscrire pleinement cette démarche dans le cadre des initiatives européennes en matière de résilience technologique et d'autonomie stratégique, en assurant une cohérence avec les travaux portés par la Commission européenne, les alliances industrielles (cloud, semi-conducteurs, IA) et les coopérations bilatérales et multilatérales.

La mission sera conduite sur une période de trois mois. Vous rendrez compte de manière régulière à mon cabinet de l'avancement des travaux.

Vous pourrez vous appuyez sur les services de la DGE, de la DG Trésor, de l'INRIA et de la DINUM, et pourrez vous rapprocher de tout acteur public ou privé intéressé au projet.

Vous veillerez à associer étroitement les organismes publics, les acteurs académiques, les représentants des entreprises stratégiques et les partenaires européens, dans une logique de co-construction rigoureuse, ouverte et tournée vers l'action.

Je vous remercie par avance de votre engagement dans cette mission stratégique pour la France et l'Europe, et vous prie d'agréer, Monsieur, l'expression de ma haute considération.

Clara Chappaz
Ministre Déléguée en charge de
l'Intelligence Artificielle et du numérique

Annexe 2 : Liste des acronymes utilisés

ANSSI	Agence nationale de la sécurité des systèmes d'information
CGE	Conseil général de l'économie
CEPII	Centre d'études prospectives et d'informations internationales
CIGREF	Club informatique des grandes entreprises françaises
CSF	Comité stratégique de filière
DAE	Direction des achats de l'Etat
DGE	Direction générale des entreprises
DGT	Direction générale du trésor
DINUM	Direction interministérielle du numérique
DMA	*Digital Markets Act* (règlement sur les marchés numériques)
DSA	*Digital Services Act* (règlement sur les services numériques)
DSI	Directeur des systèmes d'information
ETP	Equivalent temps plein
IMT	Institut Mines-Télécom
INRIA	Institut national de recherche en informatique et en automatique
INSEE	Institut national de la statistique et des études économiques
OFREMI	Observatoire français des ressources minérales pour les filières industrielles
SISSE	Service de l'information stratégique et de la sécurité économiques

Annexe 3 : Liste des personnes rencontrées ou interrogées

Organismes publics et parapublics

ORGANISME	NOM	PRENOM	Fonction
Cabinet de la ministre déléguée chargée de l'IA et du numérique	CABANNES	Théophile	Conseiller intelligence artificielle
	REVOL	Marc	Conseiller innovation
MEFSIN/DGE	COURBE	Thomas	Directeur général
	GAUQUELIN	Gustave	Chef du SISSE
	CLOPT	Baptiste	Adjoint au chef du bureau de l'intelligence artificielle
	DAHMANI	Sarah	Chargée de mission
	LEDUC-MORIN	Shanna	Chargée de mission
MEFSIN/DGT	MARINET	Vincent	Conseiller du directeur général
	CHARDON-BOUCAUD	Solal	Adjoint au chef du bureau Concurrence, numérique et économie du logement
MEFSIN/DAE	TUFFERY	Paul	
DINUM	PEZZIARDI	Pierre	Conseiller de la directrice
ANSSI	STRUBEL	Vincent	Directeur général
Bpifrance	FOURNIER	Paul-François	Directeur Exécutif, direction Innovation
	REMONT	Sophie	Directrice de l'expertise et des programmes
CEPII	BOUËT	Antoine	Directeur
Banque de France	SEDILLOT	Franck	Directeur de la balance des paiements
IMT	DUBARRY	Cécile	Directrice générale
	LECOQ	Laurence	Directrice déléguée à la recherche et au développement économique
	CHAOUCHI	Hakima	Responsable du domaine Souveraineté numérique et sobriété
INRIA	SPORTISSE	Bruno	Président-directeur général
	MAZETIER	Sandrine	Directrice générale déléguée à l'appui aux politiques publiques
	DENES	Maxime	
Institut polytechnique de Paris	COULHON	Thierry	Président
	RAPP	Vincent	Directeur exécutif du Hi! Paris Center
OFREMI	POINSSOT	Christophe	Directeur général délégué

Organisations professionnelles

ORGANISME	NOM	PRENOM	Fonction
CIGREF	d'AGRAIN	Henri	Délégué général
	de SURY	Marine	Directrice de mission
CSF Logiciels et solutions numériques de confiance	PAULIN	Michel	Président
CSF Industries de sécurité	ROUJANSKY	Jacques	Délégué permanent
Hexatrust	de GALZAIN	Jean-Noël	Président
	DECROP	Dorothée	Déléguée Générale
Numeum	LATOUR	Nicolas	
	MARSILLI	Constance	Déléguée aux affaires économiques et à l'Inclusion

Entreprises

ORGANISME	NOM	PRENOM	Fonction
Alliancy	FIEVET	Sylvain	Directeur de publication
Criteo	LANERET	Nathalie	Vice-Présidente en charge des affaires gouvernementales et des politiques publiques
Docaposte	POUPARD	Guillaume	Directeur général adjoint
	LUNGU	Smara	Directrice Stratégie, marketing, communication et relations institutionnelles
	DENYS	Séverine	Directrice des affaires institutionnelles et réglementaires
	LANNOY	Fanny	Responsable relations institutionnelles et normalisation
Jalios	BOUTHORS	Vincent	Président-directeur général
Michelin	CASEAU	Yves	Directeur du digital et des systèmes d'information
Orange	BERGER	Jérôme	Directeur de la stratégie
	MAINVILLE	Elsa	Vice-présidente chargée du développement corporate
OVH Cloud	REVCOLESCHI	Benjamin	Directeur général
	EGGRICKX	Blandine	Responsable des affaires publiques
Scality	LECAT	Jérôme	Président-directeur général
Total Energies	CHORIER	Julien	Chef de service

Annexe 4 : Critères de classification des offres

Modèle « LOTEC » pour une offre souveraine :

- **Souveraineté légale** : résidence des données, juridiction de ressort, conformité à la protection européenne des données, résilience à des pénalités juridiques extra-européennes, gestion de l'IP en Europe ou libre
- **Souveraineté opérationnelle** : contrôle opérationnel en Europe, communauté d'utilisateurs, réversibilité et portabilité des données, contrôle de version, encryptage, procédures de sécurité
- **Souveraineté technologique** : ouverture des standards, code auditable, licence ouverte, enregistrement des logs d'accès, rapports de transparence, audits tiers, contribution et capacité à attirer et maintenir les compétences
- **Souveraineté économique** : actionnariat européen, licences compatibles avec l'Europe, collaboration commerciales et académiques en Europe, réduction des dépendances extra-européennes, audit régulier
- **Souveraineté culturelle** : multilinguisme adapté aux langues et dialectes européens, compatibilité avec le système métrique et les fuseaux horaires européens, utilisation des normes européennes en UX design, entraînement sur des données européennes alignées avec les principes éthiques européens, régulation et modération compatibles

Qualification d'une offre « européenne » pour certains membres d'Eurostack

- Siège social en Europe
- Majorité de la R&D en Europe
- Majorité des droits de votes finaux par des entités européennes ou des individus ; ou absence de contrôle extra-européen
- Pas de restriction extra-européenne (IP, contrôle à l'export) sur la solution
- Soumission au droit européen et pas à des lois internationales
- Résidence fiscale en Europe, paiement de la majorité de son impôt sur les sociétés en Europe

« Quadrant stratégique européen » proposé par des membres du CIGREF avec deux axes :

- L'autonomie stratégique : notre capacité à utiliser une solution sans dépendre d'acteurs soumis à des législations extraterritoriales (Cloud Act, FISA, FCTA, etc.).
- La résilience numérique : la capacité du fournisseur à garantir la continuité, la sécurité et la conformité de ses services dans un environnement instable.