HORS-SÉRIE °3

CYBER-IT MAGAZINE

LA CYBER EST UN MARATHON PAS UN SPRINT !

Maîtriser nos dépendances numériques

En partenariat avec Plumber

Une question ? Un besoin ?
cyberit.magazine@gmail.com

EDITO

L'Europe numérique se trouve à un carrefour historique, où chaque décision compte pour notre avenir collectif.

Alors que les géants de la tech extra-européens drainent des centaines de milliards d'euros des entreprises et administrations européennes, transformant nos data centers en extensions vulnérables, ce hors-série, spécialement conçu pour le Forum InCyber 2026, vous invite à plonger au cœur des enjeux d'une souveraineté numérique mise à mal, sans concessions ni résignation fataliste.

Vous y découvrirez comment notre dépendance croissante aux infrastructures étrangères expose nos données sensibles, personnelles, industrielles, souveraines, et nos secteurs vitaux comme la santé, l'énergie ou la défense à des risques systémiques profonds. Des cas concrets, récents, y sont analysés pour montrer comment une simple décision unilatérale outre-Atlantique peut renchérir brutalement les coûts, verrouiller des écosystèmes ou menacer l'accès à des services critiques.

Mais ce numéro ne s'arrête pas au diagnostic : il explore les leviers politiques et réglementaires qui émergent aujourd'hui pour inverser la tendance, de l'observatoire dédié à la cartographie des dépendances aux stratégies de relocalisation de productions stratégiques en passant par une réorientation ambitieuse de la commande publique à l'échelle du continent.

Vous y trouverez également les initiatives phares qui tracent une voie concrète vers l'autonomie, à l'image d'un projet cloud fédéré et interopérable porté par un vaste consortium d'acteurs européens, opérateurs télécoms, fournisseurs souverains, PME innovantes et communautés open source.

À l'occasion du FIC 2026, ce hors-série vous équipe pour saisir l'urgence. Il est temps de transformer les alertes en actions collectives, pour que nous reprenions les rênes de notre destin technologique et ne plus laisser nos ressources vitales s'évaporer au profit d'empires étrangers.

Arnaud LEROY

SOMMAIRE

L'Europe, otage numérique des géants de la tech ?

Le marché mondial du numérique reste une affaire d'oligopole dominé par trois géants américains, qui accaparent les deux tiers des parts de marché en infrastructure et plateformes, tandis que le reste du peloton peine à suivre la cadence effrénée de la croissance mondiale...

Le grand âge venant, chacun craint la dépendance physique ou mentale. Être tributaire des autres pour accomplir les actes les plus simples, être à la merci de leur défaillance, être impuissant face à la moindre difficulté, être victime de prédateurs faute de pouvoir se défendre, telles sont les craintes qui préoccupent les humains. La dépendance, c'est la perte de la maîtrise de son devenir.

Pour les personnes morales, les administrations, les entreprises, l'Etat, le risque de dépendance n'est pas lié au grand âge : il est le résultat d'une succession, d'une conjugaison d'abandons ou d'excès de confiance qui réduisent ou annihilent leurs degrés de liberté.

Ce glissement est souvent imperceptible, parce que les choix sont opérés par des acteurs multiples, à des moments différents, avec une approche technique et non stratégique. Le réveil peut être douloureux, notamment lorsque le contexte géopolitique connaît un changement profond, les amis d'hier pouvant être menaçants voire« écrasants » . La souveraineté numérique n'est pas synonyme d'indépendance, d'autarcie.

Elle repose sur les interdépendances, chacun ayant besoin de l'autre : « je te tiens, tu me tiens », la comptine des enfants devrait inspirer les décideurs politiques, économiques. Pour cela, il faut une approche globale, une gouvernance au sommet. Mais il faut aussi que chaque décision prise, à tous les échelons, prenne en compte la liberté d'action numérique.

La souveraineté numérique ne se décrète pas ; elle est l'agrégat d'une multitude de choix qui, pris individuellement peuvent sembler sans importance, mais dont l'addition révèle l'ampleur de la subordination, de l'aliénation consciente ou non de son destin numérique.

L'heure n'est plus aux jérémiades, au constat de l'impuissance, au fatalisme. Il suffit de vouloir reconquérir le terrain, d'élargir sa sphère d'autonomie. Pour cela, il faut une vision, un discours, une volonté.

Après vient l'action ! Les décideurs ont aujourd'hui une immense responsabilité. S'ils faillissent, alors les citoyens seront les esclaves de la Big Tech, les zombies du numérique.

Le thème du Forum InCyber n'est pas le fruit d'un choix d'opportunité. Il est un appel à une reprise en main collective.

« Être ou ne plus être » libres dans un cyberespace qui dévore, telle est la question à laquelle nous devons apporter une réponse urgente !

Général d'armée (2S)
Martin Watin-Augouard
Fondateur du Forum InCyber

Dépendance numérique
constat économique et souveraineté fragilisée

Selon une étude du Cigref publiée en 2025, les entreprises européennes dépensent collectivement **265 milliards d'euros** par an pour des outils et services numériques contrôlés par des acteurs extra-européens

Cette somme colossale, équivalente au PIB de certains pays européens, ne finance pas seulement des abonnements ou des licences : elle représente un flux massif de capitaux vers l'extérieur, privant l'Europe de leviers économiques vitaux pour développer ses propres champions technologiques.

Une dépendance massive ne se limite pas aux aspects financiers. Elle touche les infrastructures jugées critiques, les logiciels d'entreprise, les plateformes cloud, et même les outils de productivité de notre quotidien.

Des géants comme Microsoft avec Office 365 et Azure, Amazon Web Service, Google G Suite et son Cloud, ou encore Salesforce dominent les marchés, imposant leurs standards et leurs architectures.

En France, par exemple, plus de 80% des grandes entreprises utilisent des suites SaaS américaines pour leurs messageries et collaborations, tandis que

les clouds publics hyperscalers captent 70% des déploiements critiques

Résultat : les data centers européens deviennent des succursales de la Silicon Valley, hébergeant des données soumises au Cloud Act américain ou à des régimes extraterritoriaux similaires.

Le rachat de VMware par Broadcom illustre parfaitement les risques inhérents à cette situation. Annoncé en 2023 et finalisé en 2024, ce deal a déclenché une tempête pour les utilisateurs : hausses tarifaires brutales (jusqu'à 300% sur certains contrats perpétuels), modifications des conditions contractuelles imposant des engagements annuels forcés, et incertitudes stratégiques pour les utilisateurs européens.

Des milliers d'entreprises, y compris des administrations publiques, se retrouvent piégées dans un écosystème verrouillé, contraints de migrer vers des alternatives coûteuses ou de renegocier dans l'urgence.

Les implications vont bien au-delà du simple coût d'acquisition. Elles incluent la perte de contrôle sur nos données sensibles, personnelles, industrielles ou souveraines, exposées à des juridictions étrangères et à des risques de transferts forcés. L'innovation européenne en pâtit également : enfermées dans des écosystèmes fermés, les startups et PME peinent à innover sans dépendre de roadmaps dictées par les US.

Face à cette hémorragie, les signaux d'alarme se multiplient. le Cigref alerte sur un "risque systémique", tandis que Bruxelles brandit Data Act, AI Act et Digital

Markets Act pour imposer interopérabilité et réciprocité.

Les 265 milliards annuels pourraient alors devenir la plus grosse subvention involontaire aux géants de la tech mondiale, au détriment de la renaissance numérique.

L'heure n'est plus aux diagnostics, il est temps d'agir, ou de signer l'acte de vassalité numérique pour des décennies

La dépendance numérique extra-européenne ne constitue pas simplement un désavantage commercial, elle représente une vulnérabilité structurelle aux conséquences multiples et profondes pour notre continent.

l'Europe se retrouve pieds et poings liés à des géants technologiques étrangers, subissant leurs agendas sans pouvoir riposter. Cette emprise, loin d'être anecdotique, mine les fondations mêmes de notre souveraineté, transformant des outils censés nous libérer en chaînes invisibles.

Au-delà des chiffres, une emprise sur les infrastructures critiques

Les décisions unilatérales prises par des gouvernements étrangers ou des entreprises non-européennes peuvent brutalement affecter notre accès aux technologies critiques. Les lois extraterritoriales américaines comme le Cloud Act ou les restrictions d'exportation technologique illustrent parfaitement comment nos infrastructures peuvent devenir des instruments de pression politique.

Une simple décision du côté de Washington suffit à bloquer l'accès à des services vitaux pour les banques, les hôpitaux ou les armées européennes, tandis que les tensions sino-américaines risquent de couper les approvisionnements en puces ou logiciels.

L'Europe, simple consommatrice, paie le prix de ces bras de fer sans avoir son mot à dire, et se retrouve exposée à un véritable chantage technologique en permanence.

Nos données sensibles, qu'elles soient personnelles, industrielles ou gouvernementales transitent et sont stockées sur des infrastructures étrangères., souvent de l'autre côté de l'Atlantique.

Cette situation expose l'Europe à des risques d'espionnage économique, de surveillance de masse, et de non-respect de nos standards de protection des données, pourtant parmi les plus exigeants au monde avec notamment le RGPD.

Malgré les amendes record infligées, les flux de données continuent de s'écouler vers des serveurs californiens ou chinois, où la NSA ou des agences rivales peuvent y puiser à volonté.

Cette toile d'araignée de dépendances n'est pas forcément inéluctable. Des projets comme Gaia-X ou l'European Common Compute Power tracent la voie vers un cloud européen, tandis que des acteurs poussent pour prouver qu'une alternative européenne est viable.

Mais sans un volontarisme politique radical, quotas d'achat public EU, fonds d'investissement massif, et sanctions contre les lock-ins, l'Europe continuera de saigner ses ressources numériques au profit d'empires étrangers.

HAUT-COMMISSARIAT
À LA STRATÉGIE
ET AU PLAN
Liberté
Égalité
Fraternité

Les leviers pour reprendre le contrôle

1 - L'observatoire de la souveraineté numérique ?

" La souveraineté commence par la lucidité. Nous devons savoir d'où et de quoi nous dépendons : sur quelles briques technologiques ; dans quels secteurs et pour quels usages. C'est tout l'objectif de l'Observatoire de la souveraineté numérique, que j'ai décidé de confier au Haut-commissariat à la Stratégie et au Plan. »

Anne Le Hénanff
Ministre déléguée chargée de
l'Intelligence artificielle et du Numérique

Face à l'urgence de la situation, la France franchit une étape décisive en janvier 2026 avec le lancement de l'Observatoire de la souveraineté numérique.

Cette annonce interroge néanmoins : quel est l'intérêt de mettre en place une nouvelle entité alors que plusieurs structures poursuivent déjà des objectifs similaires ?

En 2014, **l'Observatoire des libertés et du numérique** voit le jour à l'initiative d'un regroupement d'associations et de syndicats, dont la LDH et le CECIL, avec pour mission de défendre les droits fondamentaux face aux mécanismes de surveillance.

L'année suivante, en 2015, **l'Institut de la Souveraineté Numérique** est créé afin de rassembler les acteurs économiques du secteur et de formuler des propositions concrètes.

En 2017, une mobilisation citoyenne conduit à la naissance de **l'Observatoire français de l'indépendance numérique**.

Puis, en 2021, Télécom Paris et Netexplo lancent à leur tour un **Observatoire Technologies & Souveraineté numérique** placé sous le patronage de Cédric O, alors secrétaire d'État chargé du Numérique.

Lancé en début d'année avec l'ambition évidente de s'étendre rapidement à toute l'Europe, l'observatoire passe au crible, point par point, tout ce qui nous rend vulnérables.

L'observatoire s'intéresse à l'origine géographique des composants matériels (par exemple les semi-conducteurs, les équipements réseaux, les matériels de sécurité) et à la structure des chaînes d'approvisionnement, en identifiant les zones de concentration (dépendance à un petit nombre de pays ou de fournisseurs).

Il documente en outre l'exposition aux régimes juridiques extraterritoriaux, en recensant les technologies et services soumis à des législations étrangères pouvant influencer l'accès aux données ou aux infrastructures. Sur cette base, l'observatoire produit des indicateurs synthétiques, des cartographies des dépendances par secteur (santé, énergie, finance, administration, etc.) et par type de technologie, ainsi que des séries temporelles permettant de suivre l'évolution de ces dépendances.

Ces travaux donneront lieu à des rapports périodiques, des tableaux de bord et parfois des alertes thématiques lorsqu'un risque spécifique est identifié (par exemple une concentration accrue sur un fournisseur unique). Ils peuvent être utilisés par les pouvoirs publics pour prioriser les politiques d'investissement, pour cibler des programmes de soutien à certains segments industriels ou pour adapter le cadre réglementaire.

Les données produites peuvent également servir aux grandes entreprises et opérateurs d'importance vitale pour évaluer leur propre exposition et orienter leurs stratégies d'achats.

Enfin, lorsqu'il existe une coopération entre plusieurs pays, l'observatoire peut adopter une dimension multinationale (par exemple à l'échelle européenne), en harmonisant les méthodologies de mesure et en facilitant la comparaison des situations entre États membres.

Cette initiative stratégique, portée par le Haut-commissariat à la Stratégie et au Plan sous l'impulsion de la Ministre **Anne Le Hénanff**, marque une volonté politique forte de reprendre le contrôle de notre destin numérique.

UNE TRIPLE MISSION

1
Dresser un diagnostic partagé des dépendances critiques

2
Fournir des outils d'aide à la décision pour les acheteurs publics et privés

3
Contribuer à l'orientation des politiques publiques en matière de souveraineté numérique

Les premières analyses et restitutions auront lieu au printemps 2026

Les leviers pour reprendre le contrôle

2 - Relocaliser la production de matériels stratégiques ?

" L'Europe se trouve à un carrefour stratégique en matière de technologies, où sa dépendance excessive aux acteurs extra-européens, hyperscalers américains pour le cloud, fonderies asiatiques pour les semi-conducteurs, constitue à la fois une vulnérabilité économique massive et un risque existentiel pour sa souveraineté. »

Si nous essayons de donner une définition concrète de ce levier, voici ce que nous pourrions en dire :

la relocalisation de la production de matériels stratégiques numériques désigne l'ensemble des politiques et initiatives visant à développer ou renforcer, sur un territoire donné, des capacités industrielles dans des domaines considérés comme essentiels au fonctionnement du numérique.

Parmi ces domaines figurent notamment **les semi-conducteurs**, que ce soit les puces, mémoires ainsi que les composants plus spécifiques.

Les équipements de réseau, routeurs, commutateurs, antennes, **certains matériels de cybersécurité** (modules matériels de sécurité, équipements de chiffrement) et, plus largement, les infrastructures physiques des **centres de données**.

L'enjeu est d'augmenter la part de ces composants produits localement ou dans une zone jugée de confiance, afin de limiter la vulnérabilité aux aléas extérieurs.

Concrètement, cette relocalisation passe par plusieurs types de mesures.

D'abord, des dispositifs de **soutien public** peuvent être mis en place : subventions à l'investissement, garanties de prêts, crédits d'impôt pour la recherche et le développement, programmes de co-financement avec des partenaires privés.

Ces mesures sont souvent associées à des engagements formalisés de la part des industriels : **implantation d'usines** dans certains pays, volume minimal de production sur place, transfert ou maintien de compétences de conception et d'ingénierie, **création d'emplois qualifiés**.

Ensuite, des cadres de coopération peuvent être établis entre États ou au sein d'ensembles régionaux pour coordonner les implantations, **éviter les doublons et répartir les spécialisations** (par exemple certains pays concentrés sur la gravure, d'autres sur le packaging ou les tests).

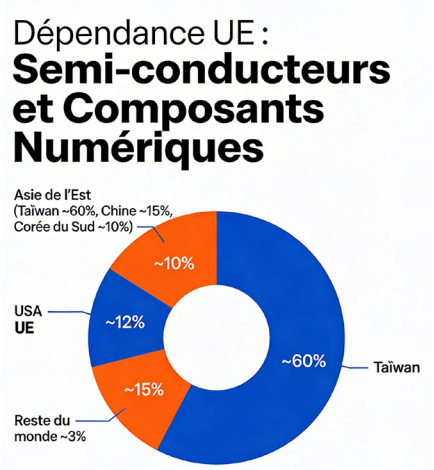
Vision à l'échelle de la souveraineté numérique

L'objectif est d'ancrer sur le territoire une partie significative de la base matérielle sur laquelle reposent le cloud, les systèmes d'information critiques, les réseaux de communication et les infrastructures de cybersécurité.

Le Chips Act européen fixe par exemple une cible de doublement de la part de production mondiale de semi-conducteurs de l'Union Européenne, de 10% à 20% à l'horizon 2030, avec un effort financier public estimé à 43 milliards d'euros pour soutenir l'écosystème.

La relocalisation s'appuie aussi sur des infrastructures connexes : disponibilité d'énergie, de réseaux de transport, de main-d'œuvre qualifiée, d'écosystèmes de sous-traitants et de centres de recherche.

Elle s'inscrit donc dans une logique de politique industrielle de long terme. D'un point de vue opérationnel, le développement de ces capacités locales permet de réduire la dépendance à un nombre restreint de pays ou de régions pour les composants clés, de mieux maîtriser les délais et les conditions d'approvisionnement et de disposer de marges de manœuvre en cas de tensions géopolitiques, de restrictions à l'exportation ou de perturbations logistiques.



Les leviers pour reprendre le contrôle

3 - Commande publique et nouveau cadre réglementaire ?

" La réforme de la commande publique numérique vise à réorienter les 2 000 milliards d'euros annuels dépensés par les administrations européennes vers des solutions souveraines. Un principe de préférence UE, avantageraient les offres garantissant localisation des données, contrôle opérationnel local et usage prioritaire de l'open source »

La commande publique, lorsqu'elle s'appuie sur un cadre réglementaire adapté, devient l'un des leviers les plus puissants pour orienter concrètement le marché numérique européen vers une véritable souveraineté technologique.

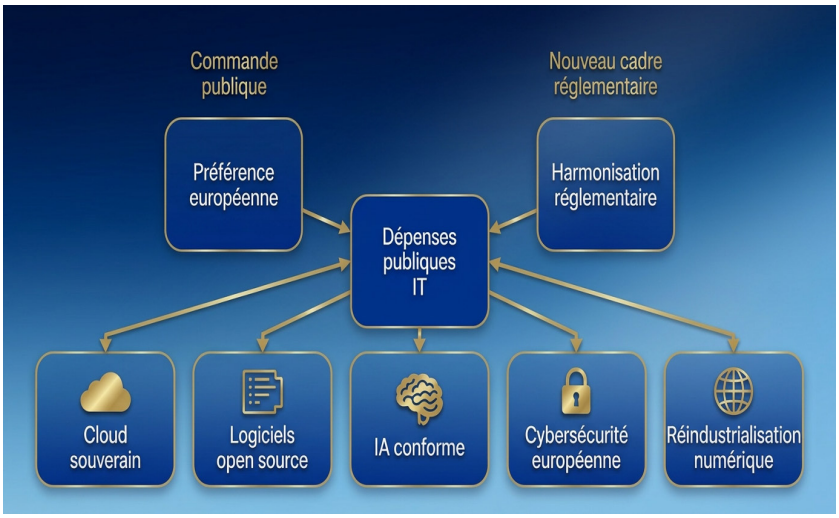
Autrement dit, les milliards d'euros dépensés chaque année par les administrations publiques peuvent se transformer en un outil stratégique de réindustrialisation, à condition d'être mieux orientés.

En mettant en place un principe clair et solide de préférence européenne dans tous les achats numériques, qu'il s'agisse de l'État, des collectivités, des hôpitaux, des universités ou encore des opérateurs jugés essentiels comme les fournisseurs d'énergie ou les banques publiques, les pouvoirs publics peuvent créer une demande durable et prévisible au bénéfice des acteurs européens.

Cela profiterait directement aux fournisseurs de cloud souverain, aux éditeurs de logiciels open source certifiés, aux plateformes d'intelligence artificielle conformes et aux solutions européennes de cybersécurité.

Ce mouvement structurant, ne peut produire ses effets que s'il s'accompagne d'un cadre réglementaire clair, unifié et adapté à la réalité du terrain. L'Union européenne et ses États membres doivent travailler à la mise en place d'une architecture juridique cohérente, à la fois protectrice et opérationnelle, afin que les acteurs économiques évoluent dans un environnement lisible, prévisible et équitable.

Cela suppose une harmonisation stricte et homogène des règles relatives à la souveraineté des données et des métadonnées, de manière à garantir la sécurité juridique des échanges transfrontaliers tout en évitant les divergences d'interprétation entre législations nationales.



Cette harmonisation doit aller de pair avec une adaptation pragmatique et non punitive des textes existants portant sur l'intelligence artificielle, le numérique et la protection des données personnelles, en particulier l'AI Act, le RGPD et le DSA.

Le cadre réglementaire doit également clarifier progressivement et de façon méthodique les exigences de certification applicables aux infrastructures numériques critiques.

Une telle clarification est essentielle pour garantir un niveau homogène de sécurité et de conformité à travers toute l'Union, tout en évitant les doublons, les contradictions et les surcharges administratives qui freinent l'innovation.

Elle permettrait aux entreprises européennes d'évoluer dans un contexte de confiance mutuelle, réduisant les barrières à l'entrée sur les marchés publics et simplifiant les démarches nécessaires à la qualification de leurs solutions.

Ce cadre commun offrirait par ailleurs une base solide pour la reconnaissance mutuelle des certifications, facilitant la collaboration transnationale et la création d'un espace numérique réellement intégré.

En articulant dans la durée ces deux leviers, la commande publique et le cadre réglementaire, les États européens disposent de la capacité de transformer ce qui, jusqu'ici, relevait d'un ensemble de dépenses dispersées en un moteur stratégique de réindustrialisation numérique.

Nous y voyons une façon de bâtir un espace numérique unifié, basé sur la confiance et la transparence, avec une meilleure maîtrise des technologies clés pour tous les citoyens et entreprises.

EURO-3C, le Projet Phare pour un cloud souverain en Europe

L'Union européenne vient de lancer EURO-3C, un projet stratégique financé à hauteur de 75 millions d'euros dans le cadre du programme Horizon Europe.

Annoncé au Mobile World Congress 2026 à Barcelone, ce consortium réunit 87 organisations européennes pour construire la première infrastructure fédérée Telco-Edge-Cloud à grande échelle sur le continent, réduisant ainsi la dépendance aux fournisseurs américains du cloud.

Ce projet phare mettra en évidence la capacité de l'Europe à fournir des services numériques de pointe entièrement au moyen de sa propre infrastructure.

Le cloud computing est devenu la colonne vertébrale de l'économie numérique européenne. Messageries professionnelles, outils collaboratifs, applications d'intelligence artificielle, stockage de documents, sauvegarde de données, réseaux sociaux reposent tous sur ces infrastructures distribuées. Pourtant, une très large majorité des dépenses cloud européennes profite aux hyperscalers américains : Amazon Web Services, Microsoft Azure et Google Cloud captent entre 60 et 70% du marché.

Cette domination s'explique par plusieurs atouts structurants : une puissance financière considérable permettant des investissements massifs dans les infrastructures mondiales, des écosystèmes logiciels extrêmement riches et intégrés, une rapidité de déploiement qui séduit les entreprises européennes, ainsi qu'une capacité à intégrer une multitude de services dans un environnement unique.

Le Cloud Act américain, entré en vigueur en 2018, permet aux autorités américaines d'exiger l'accès à des données hébergées par des entreprises sous juridiction américaine, même si ces données sont stockées sur des serveurs européens. Cette réalité juridique alimente depuis plusieurs années le débat sur la véritable maîtrise des données critiques santé, défense, finance, énergie par les organisations européennes.

Le projet EURO-3C ambitionne de déployer plus de 70 nœuds edge et cloud répartis dans 13 pays européens. Cette architecture combine trois technologies complémentaires comme les réseaux télécoms pour une connectivité 5G et préparatoire à la 6G.

Mais aussi l'informatique de périphérie, ce que l'on nomme edge computing, qui rapproche la puissance de calcul des utilisateurs finaux, réduisant la latence.

L'europe veut construire un cloud fédéré pour une infrastructure cloud souveraine et interopérable.

La localisation physique des data centers en Europe ne garantit pas la souveraineté des données

Le consortium EURO-3C réunit une diversité d'acteurs complémentaires, cette collaboration multi-opérateurs et multi-fournisseurs garantit l'interopérabilité et évite la création de silos technologiques nationaux.

Des acteurs européens reconnus comme OVHcloud (leader français du cloud souverain) et IONOS (spécialiste allemand) fournissent l'infrastructure physique, tandis que des PME technologiques spécialisées comme Scille (cybersécurité) et Krateo (ingénierie de plateformes) apportent agilité et expertise pointue.

Le consortium intègre des acteurs majeurs de l'open source et du cloud souverain tels que SUSE, éditeur de solutions Linux et Kubernetes, ainsi qu'OpenNebula, spécialisé dans la gestion de cloud orchestré.

En recyclant une partie des 264 milliards d'euros annuels actuellement exportés vers les États-Unis, EURO-3C pourrait créer des centaines de milliers d'emplois qualifiés et financer la R&D européenne. Le projet vise une part de marché cloud souverain de 15 à 20% d'ici 2030, un objectif réaliste si l'adoption par les PME suit celle des grands comptes.

Les défis restent importants : préssion concurentielle face à des concurrents bien établis, coûts initiaux de migration, coordination entre 13 pays.

Avec l'EURO-3C, l'Europe passera du statut de consommateur passif à celui d'architecte de son avenir numérique

Une ambition sans fonds ...

EURO-3C s'inscrit davantage dans une logique de test et d'expérimentation que dans celle d'un déploiement industriel destiné au marché. Le projet ne vise donc pas, à ce stade, la création d'une infrastructure cloud de grande ampleur.

Pourquoi ? Simplement car la construction de plateformes capables de rivaliser avec les hyperscalers nécessite habituellement des investissements se comptant en dizaines de milliards d'euros, un ordre de grandeur très éloigné de l'enveloppe annoncée de 75 millions d'euros.

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'ESPACE
Liberté
Égalité
Fraternité
horizon europe

CREDITS

Rédacteur : Arnaud LEROY
Design Graphique : Arnaud LEROY
Traduction Anglaise : Maëva ASTORGA
Parrain du magazine : Guillaume POUPARD

Avril 2026