La souveraineté est une pile, pas un label

Sept strates, trois verdicts, une doctrine d'arbitrage pour l'IA en environnement régulé européen.

1. Introduction

L'article précédent posait que la souveraineté numérique n'est pas un débat politique mais une contrainte d'architecture, et qu'elle se distribue sur trois plans : la localisation des données, la qualification de l'infrastructure, l'immunité juridique de l'opérateur. Cette doctrine reste valide pour la couche IaaS-PaaS qualifiée SecNumCloud. Mais elle ne descend pas dans la pile matérielle qui rend cette infrastructure opérable.

Or la qualification SecNumCloud 3.2 délivrée à PREMI3NS de S3NS le 17 décembre 2025 [S1] et que Bleu, après validation du jalon J0 en avril 2025, vise toujours sans l'avoir obtenue à ce jour [S2], traite l'opérateur de service cloud, pas le silicium qu'il opère, ni la mémoire haute bande passante qui nourrit ses accélérateurs IA, ni les firmwares qui contrôlent ses serveurs, ni les infrastructures transcontinentales par lesquelles transitent ses données. Le silence doctrinal sur ces couches profondes produit un effet de simplification trompeur : il laisse croire qu'une qualification SecNumCloud résout l'intégralité du problème de souveraineté, alors qu'elle traite principalement une couche précise, l'immunité juridique extraterritoriale de l'opérateur.

L'accord politique européen du 7 mai 2026 sur le paquet Omnibus VII ne dispense pas de ce travail, il le déplace dans le temps. Le Parlement et le Conseil ont validé le décalage des obligations haut risque de l'Annexe III du 2 août 2026 au 2 décembre 2027, et de l'Annexe I au 2 août 2028 [S3]. La plupart des usages industriels embarqués ont été exemptés ; la santé ne l'a pas été. Pour les systèmes d'IA santé sous HDS, NIS2 et AI Act haut risque, la fenêtre de préparation s'allonge, mais le périmètre des contraintes structurelles reste intact. Une dépendance supply chain critique demeure une propriété architecturale du système, pas une date d'entrée en vigueur réglementaire.

La thèse de cette note est quadruple. *Premièrement*, la souveraineté n'est pas un label mais une pile composée de strates distinctes, chacune appelant un verdict autonome. *Deuxièmement*, la chaîne d'approvisionnement matérielle constitue désormais la couche profonde de la souveraineté effective, parce qu'elle conditionne la continuité opérationnelle, la maintenance, la disponibilité et la prévisibilité du système. *Troisièmement*, aucune offre commerciale, européenne ou non, ne ferme aujourd'hui la pile en souveraineté pure ; l'autarcie technologique est un fantasme industriel, et seule

une souveraineté composite et auditée est praticable. *Quatrièmement*, l'émergence de mécanismes d'attestation matérielle et de télémétrie d'usage sur les accélérateurs IA transforme progressivement certains composants en objets gouvernés à distance, et change la nature même du problème.

Domaine de validité. La thèse vaut pour les systèmes d'IA déployés en environnement régulé européen (RGPD, HDS, NIS2, AI Act haut risque) et dont la continuité opérationnelle fait partie des exigences fonctionnelles. Pour ces systèmes, l'arrêt brutal de la chaîne d'approvisionnement d'un composant critique n'est pas une nuisance contractuelle : c'est une rupture de service à enjeu réglementaire et clinique. La doctrine s'écrit sous cette contrainte.

La question doctrinale n'est donc plus seulement *où sont mes données ?* Elle devient : *quelles composantes de ma pile peuvent être interrompues, altérées, conditionnées ou rendues non défendables par une décision tierce extérieure à mon périmètre de gouvernance ?*

2. Sécuriser n'est pas internaliser

Les débats sur la souveraineté numérique mélangent souvent trois notions qui ne sont ni équivalentes ni substituables : *internaliser*, *diversifier*, *sécuriser*.

Internaliser consiste à produire soi-même, ou sous contrôle capitalistique direct, un composant critique de la chaîne. C'est l'ambition maximaliste de souveraineté technologique pure. Dans le domaine des semi-conducteurs avancés, elle se heurte à une réalité industrielle sévère. Produire un wafer leading-edge exige non seulement une fab mais un écosystème amont complet : lithographie EUV, photoresists, masques, gaz spéciaux, packaging avancé, bonding hybride, mémoire haute bande passante, chaîne logicielle EDA. Aucun acteur européen ne maîtrise aujourd'hui l'ensemble. ASML produit les machines EUV, mais Carl Zeiss SMT produit les optiques, JSR et Tokyo Ohka dominent les photoresists, Synopsys et Cadence dominent les outils EDA, TSMC concentre la fabrication leading-edge, Samsung et SK Hynix dominent la HBM. La fragmentation est par construction.

Diversifier consiste à répartir les dépendances afin qu'aucune rupture isolée ne provoque l'arrêt du système. C'est une stratégie de résilience, non de souveraineté. Une diversification réussie peut tout à fait reposer sur des fournisseurs non européens, du moment qu'ils ne sont pas tous exposés au même risque géopolitique, climatique ou logistique simultanément.

Sécuriser combine internalisation partielle, diversification, contrats stratégiques, stocks tampons, garanties de volume, clauses de continuité et trajectoires de substitution.

Sécuriser une dépendance, c'est en faire une propriété auditée du système plutôt qu'une vulnérabilité subie.

La distinction qui tranche : internaliser est une stratégie industrielle, diversifier est une stratégie de résilience, sécuriser est une stratégie de souveraineté. Les trois peuvent coexister. Aucun ne remplace les deux autres, et la souveraineté composite défendue ici suppose les trois activées simultanément, à des dosages différents selon les strates.

3. Le modèle « souveraineté par le contrôle » : ce qu'il résout, ce qu'il ne résout pas

Le modèle validé par l'ANSSI avec S3NS, et poursuivi par Bleu, repose sur une thèse : la souveraineté dépend moins de l'origine de la technologie que du contrôle effectif exercé sur son opération. La distinction est sérieuse, elle a été validée institutionnellement, mais sa portée doit être délimitée avec précision.

Ce que le modèle résout est réel : l'immunité juridique de l'opérateur cloud aux injonctions extraterritoriales directes. S3NS opère sous droit français, avec gouvernance française, personnel français, datacenters français, et séparation juridique vis-à-vis de Google Cloud par le contrôle capitalistique de Thales et un dispositif de quarantaine technologique[S1]. Bleu poursuit une architecture comparable autour des technologies Microsoft, à 100 % détenu par Capgemini et Orange[S2]. Le risque d'injonction directe au titre du CLOUD Act est ainsi significativement réduit et encadré, sans disparaître entièrement de l'analyse dès lors que la pile technologique reste licenciée auprès d'acteurs américains.

Ce que le modèle ne résout pas, et qu'il ne prétend pas résoudre, est la dépendance technologique structurelle aux fournisseurs américains pour les couches qu'il assemble. S3NS opère du Google Cloud sous licence ; Bleu opérera des briques Azure et Microsoft 365 sous licence. Les roadmaps produits, les mécanismes cryptographiques profonds, les chaînes de build, les microcodes CPU, les accélérateurs IA et les dépendances firmware restent sous contrôle technologique non européen. Le contrôle juridique a été acquis ; le contrôle de la production technologique n'a pas changé de main.

La formule doctrinale qui en découle est sobre. *Une certification SecNumCloud réduit fortement le risque juridique extraterritorial au niveau de l'opérateur. Elle ne transfère ni la propriété intellectuelle de la pile technologique, ni la maîtrise des roadmaps produits, ni le contrôle des composants matériels profonds. Elle qualifie une couche d'exploitation sous droit européen ; elle ne souverainise pas mécaniquement l'ensemble de la chaîne de production.*

La distinction qui tranche : contrôle et production ne sont pas la même chose. Le modèle résout une **souveraineté d'usage** ; il ne résout pas une **souveraineté de fabrique**. Cette nuance évite deux erreurs symétriques : considérer ces modèles comme fictivement souverains, ou les considérer comme inutiles parce que pas parfaitement souverains. Les deux postures sont intellectuellement faibles. La réalité est plus exigeante : ces modèles résolvent une strate critique de souveraineté sans résoudre les autres, et la doctrine doit nommer précisément quelles strates restent ouvertes.

4. Sept strates, instruites une à une

La souveraineté d'une architecture IA ne peut plus être évaluée globalement. Elle doit être instruite strate par strate, selon une grille uniforme : *Quelle question de souveraineté pose-t-elle ? Quel est le verdict européen actuel ? Quelle dépendance résiduelle subsiste ? Quelle décision CTO en découle ?* Sept strates apparaissent aujourd'hui structurantes.

Strate 1 : Silicium logique (CPU, GPU, accélérateurs IA). La question est de savoir qui conçoit, qui fabrique, qui peut conditionner l'opération. Le verdict européen 2026 est celui d'une conception partielle, avec la livraison du SiPearl Rhea1 attendue dans le courant 2026[S4], mais d'une fabrication leading-edge absente. Les dépendances résiduelles critiques portent sur TSMC pour la gravure, ARM pour l'architecture, et l'attestation cryptographique sous gouvernance hors UE. La décision CTO type est *compensable* dès lors qu'elle est couverte par des contrats long terme et une trajectoire de bascule datée vers les accélérateurs européens à mesure qu'ils arrivent à maturité.

Strate 2 : Mémoire avancée (HBM, DRAM, NAND). Qui produit la mémoire qui nourrit les GPU et les serveurs ? Le verdict européen est nul : aucun acteur, aucun projet d'industrialisation amorcé. Le marché reste concentré autour de SK Hynix, Samsung et Micron, avec des capacités 2026 largement préemptées par les hyperscalers et les grands acteurs IA américains [S5]. La décision CTO est *compensable* au cas par cas par engagement de volume pluriannuel, mais elle reste non substituable à court terme, c'est la dépendance la plus dure de la pile.

Strate 3 : Firmware et racines de confiance. Qui signe le microcode, le BMC, le secure boot ? Coreboot et LinuxBoot offrent des alternatives ouvertes, mais leur adoption en environnement serveur de production reste marginale. Les dépendances résiduelles portent sur Intel ME, AMD PSP et les BMC propriétaires (iLO, iDRAC, IPMI), non auditables intégralement. La décision CTO est *compensable* par audit indépendant, exigence de signature reproductible et zone de quarantaine pour les mises à jour.

Strate 4 : Réseau physique (backbone, fibre, câbles sous-marins). Qui produit, qui possède, qui exploite les routes du trafic ? Le verdict européen est fort sur la fabrication

des câbles (Alcatel Submarine Networks, nationalisée à 80 % par l'État français en novembre 2024 [S6]) et sur la fibre (Prysmian, Nexans), moyen sur le backbone (Nokia, Ericsson). Les dépendances résiduelles portent sur Cisco, Juniper et Arista pour les équipements de datacenter, et sur la propriété hyperscaler croissante des câbles transatlantiques. La décision CTO est *acceptable* dès lors que le trafic régulé reste sous contrôle européen vérifié.

Strate 5 : Système d'exploitation et hyperviseur. Qui contrôle le noyau et la couche de virtualisation ? Le verdict est fort techniquement, avec Linux, KVM, Xen, mais faible en gouvernance, avec une domination des fondations américaines (Linux Foundation, CNCF). Les dépendances résiduelles portent sur la maintenance noyau mondiale et la gouvernance projets hors UE. La décision CTO est *acceptable* sous condition d'auditabilité du build et de fork défensif documenté.

Strate 6 : Orchestration et plateforme. Qui gouverne Kubernetes, OpenShift, les outils de pilotage ? Le verdict est élevé techniquement, faible en gouvernance (la CNCF reste dominée par les acteurs américains). Le risque résiduel est celui d'un fork hostile ou d'un blocage de release. La décision CTO est *acceptable* si un fork interne est maintenu à coût raisonnable par les équipes ou un consortium européen.

Strate 7 : Cloud souverain qualifié. Qui opère, sous quel droit, avec quelle immunité extraterritoriale ? Le verdict européen est croissant, avec un paysage à deux philosophies coexistantes : la souveraineté technologique pure (OVHcloud, Outscale, Scaleway, NumSpot) et la souveraineté par le contrôle (S3NS qualifié, Bleu visant). Les dépendances résiduelles portent sur la stack technologique sous licence pour les modèles hybrides, ou sur l'écosystème logiciel pour les acteurs indigènes. La décision CTO devient *disqualifiante* en santé sensible si l'opérateur n'est pas qualifié SecNumCloud 3.2 ou en trajectoire vérifiable de qualification.

Le verdict structurel est clair : la souveraineté européenne est forte aux deux extrémités de la pile (l'opérateur peut être qualifié SecNumCloud, le serveur peut être Eviden, le câble peut être ASN, le modèle peut être Mistral) mais fragile au milieu (silicium leading-edge, HBM, firmware, gouvernance des projets open source). Cette structure en sablier est une caractéristique historique : l'Europe a maintenu ses capacités d'intégration et ses compétences applicatives pendant que la production de composants critiques se déplaçait vers l'Asie et les États-Unis.

5. Le silicium change de nature politique

Le changement le plus important depuis deux ans ne réside pas uniquement dans la concentration industrielle des GPU IA. Il réside dans l'émergence progressive d'une infrastructure d'attestation matérielle, et le sujet doit être formulé avec précision.

À ce jour, aucun mécanisme public documenté ne constitue un *kill switch* opérationnel permettant la désactivation distante des GPU NVIDIA. La position de NVIDIA est explicite et répétée publiquement par sa direction : aucune backdoor, aucun *kill switch*, et la télémétrie utilisée pour le pilote de vérification de localisation reste *read-only* [S7]. Le mécanisme en pilote sur l'architecture Blackwell est un agent logiciel optionnel, installé par le client sur ses propres serveurs, qui exploite la télémétrie GPU, l'attestation cryptographique et la mesure de latence réseau pour estimer le pays d'opération du chip (précision comparable à une géolocalisation IP, pas un GPS embarqué) [S7] [S8]. L'extension à Hopper et Ampere est seulement à l'exploration ; rien n'a été annoncé sur ce périmètre.

Plusieurs briques convergent néanmoins, et c'est leur composition qui mérite l'attention doctrinale plutôt que chaque brique isolée. Côté politique export, la nouvelle politique de licences du BIS américain, publiée le 13 janvier 2026, encadre l'export du H200 vers la Chine par examen au cas par cas, vérification par laboratoire tiers indépendant aux États-Unis avant expédition, taxe de 25 % à l'importation, plafond de volume et exigences de conformité côté acheteur, dont des clauses d'absence d'accès distant[S9] [S10]. Côté hardware, l'architecture Blackwell embarque des capacités d'attestation cryptographique renforcées par rapport aux générations précédentes [S7]. Côté logiciel, le pilote de vérification de localisation est en cours de déploiement optionnel.

Pris isolément, aucun de ces éléments ne transforme un GPU en terminal contrôlé à distance. Pris ensemble, ils établissent un précédent doctrinal : *la possibilité que l'autorisation d'opérer un accélérateur IA devienne progressivement une propriété attestée, vérifiée et conditionnée par une autorité extérieure au propriétaire physique du matériel*. Le précédent porte sur l'infrastructure de contrôle, pas sur une capacité actuelle de coupure. La distinction est essentielle pour la rigueur du propos.

La distinction qui tranche : posséder un accélérateur IA ne signifie plus nécessairement contrôler intégralement l'attestation que cet accélérateur produit sur sa propre conformité. Le datacenter peut être français, l'opérateur peut être européen, le cluster peut être physiquement localisé sous juridiction nationale ; le référentiel d'attestation, la chaîne cryptographique et les mécanismes de conformité peuvent rester externes. La souveraineté juridique locale cesse alors d'être suffisante pour les classes de systèmes les plus régulés.

6. La HBM : le point de rupture réel

La mémoire haute bande passante constitue probablement la dépendance la plus critique et la moins compensable de la pile IA européenne actuelle. Le marché mondial est concentré autour de SK Hynix, Samsung et Micron, et les capacités 2026 sont largement préemptées par les hyperscalers et les grands acteurs IA américains [S5]. La

HBM3E est en pénurie structurelle ; la HBM4 entre en production en 2026 pour la plateforme NVIDIA Rubin.

Aucun acteur européen ne produit de HBM. Aucun projet européen public d'industrialisation HBM n'est annoncé à ce jour. La concentration géographique est extrême : production essentiellement en Corée du Sud et capacité Micron américaine secondaire ; le base die HBM est produit chez TSMC. Toute la chaîne, pour les GPU IA mondiaux, repose sur trois fournisseurs asiatiques et un trio géographique (Corée du Sud, Taïwan, États-Unis pour Micron) qui ne contient pas l'Europe.

Cette absence n'est pas accidentelle. La HBM exige des compétences en empilement vertical (TSV, *through-silicon vias*), en bonding hybride et en thermique de précision que l'Europe n'a pas développées au niveau industriel. Le Chips Act 2 en discussion pour 2026 pourrait identifier la HBM comme priorité, mais aucun projet d'industrialisation n'est aujourd'hui à l'état de planification opérationnelle. Le projet phare Intel Magdeburg, annoncé en 2022, a été annulé en juillet 2025 [S11]. ESMC Dresden, qui doit démarrer la production en 2027, cible les nœuds 28/22 nm CMOS et 16/12 nm FinFET pour les marchés automobile et industriel, et n'est pas une fab leading-edge IA [12].

Le constat touche directement le facteur limitant principal des GPU IA modernes : la bande passante mémoire. Sans HBM, les accélérateurs IA modernes perdent une part essentielle de leur valeur opérationnelle. Même un accélérateur européen hypothétique dépendrait encore aujourd'hui d'une chaîne HBM non européenne (Rhea1 lui-même embarque quatre piles HBM2E Samsung) [S4] [S13].

La HBM est le caillou dans la chaussure de la souveraineté IA européenne. Tant qu'il est là, la pile complète ne peut être qualifiée de souveraine sans qualification d'usage. Ce constat n'appelle pas le fatalisme ; il appelle la hiérarchisation.

7. Trois verdicts : acceptable, compensable, disqualifiante

Une doctrine utile ne peut pas rester descriptive ; elle doit produire des règles d'arbitrage opérationnelles. Une dépendance devient problématique lorsqu'elle cumule quatre propriétés : elle est critique, elle est non substituable, elle n'est pas contractualisée, et elle est exposée à une décision tierce non maîtrisable.

Une dépendance n'est pas un échec de souveraineté. Elle le devient lorsqu'elle est à la fois critique, non substituable, non contractualisée et exposée à une décision tierce non maîtrisable. La doctrine ne doit donc pas demander : *cette strate est-elle européenne ?*

Elle doit demander : *cette strate peut-elle interrompre, altérer ou rendre non défendable le service régulé, et quelles contre-mesures vérifiables existent ?*

Trois verdicts en découlent.

1. **Acceptable.** La dépendance existe mais reste techniquement substituable à coût et délai raisonnables, sans capacité de coupure asymétrique par l'acteur tiers. Exemple typique : un orchestrateur Kubernetes maintenu par la CNCF, dont un fork défensif documenté est techniquement maintenable par les équipes internes ou par un consortium européen. La dépendance existe, mais elle n'est pas asymétrique : la rupture serait coûteuse pour les deux parties, et l'effort de substitution est borné.
2. **Compensable.** La dépendance n'est pas substituable à court terme mais peut être couverte par un mécanisme contractuel ou opérationnel vérifiable : stock stratégique, contrat long terme avec garantie d'approvisionnement et clauses d'isolation politique, redondance multi-fournisseurs, ou trajectoire de migration datée et financée. La HBM Samsung embarquée dans un Rhea1 entre dans cette catégorie tant qu'un contrat avec engagement de volume couvre la durée de vie du cluster et qu'une trajectoire de bascule existe pour la génération suivante. La compensation est l'aveu lucide d'une dépendance, pas son ignorance.
3. **Disqualifiante.** La dépendance peut interrompre ou altérer un système critique sans recours réaliste. Exemple typique : un mécanisme externe d'attestation conditionnant l'usage d'un accélérateur déployé dans un système clinique vital, sans clause d'isolation contre l'évolution réglementaire de la juridiction émettrice et sans trajectoire alternative documentée. Si la dépendance est disqualifiante, l'architecture doit être revue — pas adoucie par un discours.

Cette taxonomie n'est pas une grille de notation. C'est un schéma d'arbitrage qui transforme la doctrine de *constat* en doctrine de *gouvernance*. Sans ce passage, la souveraineté composite reste un exercice descriptif. Avec lui, elle devient un instrument de décision.

8. Pourquoi le paradigme « Made in Europe » est insuffisant

Le débat public glisse progressivement vers une logique binaire : européen ou non européen. Cette grille est insuffisante pour deux raisons symétriques.

Un système assemblé en Europe avec GPU NVIDIA, HBM coréenne, firmware Intel ME, dépendances EDA américaines et gravure TSMC ne devient pas souverain parce que son intégration finale est européenne. La nationalité du dernier assembleur ne résume pas la

souveraineté de la chaîne. Acheter *Made in Europe* ne fabrique pas *Made in Europe*, et cette confusion produit des arbitrages contre-productifs où l'organisation paie une prime pour un assemblage local sans réduire substantiellement ses dépendances.

Inversement, une pile composite utilisant certaines briques non européennes mais disposant d'une gouvernance locale, d'une auditabilité forte, d'une trajectoire de migration, d'une isolation juridique et d'une résilience supply chain documentée peut être beaucoup plus défendable qu'un assemblage « européen » opaque dont aucune des dépendances n'est instruite.

La distinction qui tranche : Made in Europe est une catégorie commerciale, souveraineté composite auditée est une catégorie d'ingénierie. Ce ne sont pas les mêmes objets, et les confondre dégrade la qualité des décisions architecturales prises sur cette base.

9. Conclusion

Le problème contemporain de souveraineté numérique n'est plus seulement un problème de cloud. C'est un problème de continuité opérationnelle gouvernée sous dépendances multiples. Les modèles comme S3NS et Bleu résolvent une partie réelle du problème (l'immunité juridique de l'opérateur) sans résoudre la souveraineté du silicium qu'ils opèrent, ni celle de la HBM qui nourrit leurs accélérateurs IA, ni celle des mécanismes profonds de firmware et d'attestation. Cela ne les invalide pas ; cela fixe leur périmètre réel.

La souveraineté n'est pas un état pur. C'est une discipline d'arbitrage qui consiste à identifier, strate par strate, quelles dépendances sont tolérables, lesquelles sont compensables, lesquelles deviennent disqualifiantes au regard du modèle de menace du système considéré.

Une certification SecNumCloud immunise l'opérateur, pas le silicium qu'il opère ; le CLOUD Act lit les organigrammes, les régimes export lisent les *bills of materials*, et les accélérateurs IA commencent désormais à apprendre à attester de leurs propres conditions d'opération. Dans ce contexte, la souveraineté composite n'est pas une concession pragmatique à l'imperfection du réel — c'est la seule doctrine techniquement défendable pour construire des systèmes d'IA régulés sans sombrer ni dans l'illusion d'autarcie, ni dans le renoncement stratégique.

Sources et références

Footnotes

1. S3NS, *S3NS annonce la qualification SecNumCloud 3.2 délivrée par l'ANSSI pour PREMI3NS*, communiqué du 19 décembre 2025 (visa ANSSI délivré le 17 décembre 2025). https://www.s3ns.io/actualite/s3ns-annonce-qualification-sec-num-cloud

2. Bleu, *Bleu valide le J0 de la qualification SecNumCloud 3.2*, communiqué du 17 avril 2025. La qualification, visée pour le premier semestre 2026, n'est pas obtenue à ce jour. https://www.bleucloud.fr/bleu-valide-le-j0-de-la-qualification-secnumcloud-3-2/

3. Conseil de l'Union européenne, *Artificial Intelligence: Council and Parliament agree to simplify and streamline rules*, communiqué officiel du 7 mai 2026 ; Commission européenne, communiqué IP/26/1024 du 7 mai 2026. Accord politique provisoire dans le cadre du paquet Omnibus VII : décalage des obligations Annexe III au 2 décembre 2027 et Annexe I au 2 août 2028 ; exemption de la plupart des usages industriels embarqués ; les dispositifs médicaux restent dans le scope. Adoption formelle attendue avant le 2 août 2026. https://www.consilium.europa.eu/en/press/press-releases/2026/05/07/artificial-intelligence-council-and-parliament-agree-to-simplify-and-streamline-rules/ ; https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1024

4. SiPearl, page produit *Rhea1 pour HPC et inférence d'IA* : architecture 80 cœurs ARM Neoverse V1, fabrication TSMC en N6 (7 nm), quatre piles HBM2E embarquées, premiers échantillons commerciaux disponibles début 2026, déploiement dans le module Cluster du supercalculateur exascale JUPITER (Forschungszentrum Jülich) prévu mi-2026. Tape-out confirmé en juillet 2025. https://sipearl.com/fr/rhea1

5. Sur la concentration HBM autour de SK Hynix, Samsung et Micron et la préemption des capacités 2026 par les hyperscalers et acteurs IA américains, cf. analyses TrendForce et Astute Group 2025-2026 ; Bird & Bird, *Digital Omnibus on AI Provisional Agreement Reached at the May Trilogue*, 8 mai 2026. https://www.twobirds.com/en/insights/2026/digital-omnibus-on-ai-provisional-agreement-reached-at-the-may-trilogue

6. Sur la nationalisation d'Alcatel Submarine Networks par l'État français en novembre 2024 (prise de participation à 80 % pour environ 100 millions d'euros), cf. communications de l'Agence des participations de l'État et audition d'ASN au

Sénat français, février 2026. ASN reste l'un des trois acteurs mondiaux majeurs des câbles sous-marins, aux côtés de TE SubCom (États-Unis) et NEC (Japon).

7. Reuters, *Exclusive: Nvidia Builds Location Verification Tech That Could Help Fight Chip Smuggling*, 9-10 décembre 2025 (republication intégrale via U.S. News). Position publique répétée de NVIDIA : aucune backdoor, aucun *kill switch*, aucune capacité de désactivation distante (déclaration de David Reber Jr., chief security officer NVIDIA, août 2025 : « No Backdoors. No Kill Switches. No Spyware. »). Pilote initialement déployé sur Blackwell ; extension à Hopper et Ampere à l'exploration. https://www.usnews.com/news/top-news/articles/2025-12-09/exclusive-nvidia-builds-location-verification-tech-that-could-help-fight-chip-smuggling

8. Sur le mécanisme technique sous-jacent (Hardware-Enabled Mechanisms, attestation cryptographique, *landmark servers* à latence calibrée, équivalence de précision avec la géolocalisation IP), cf. Tom's Hardware, *Nvidia develops software-based tracking for AI GPUs*, 10 décembre 2025. https://www.tomshardware.com/pc-components/gpus/nvidia-develops-software-based-tracking-for-ai-gpus-to-quash-smuggling-concerns-solution-devised-to-prevent-shipments-to-nations-with-export-controls-in-place

9. Bureau of Industry and Security (BIS, Département du Commerce des États-Unis), *Department of Commerce Revises License Review Policy on Semiconductors Exported to China*, communiqué du 13 janvier 2026. Examen au cas par cas pour les NVIDIA H200, AMD MI325X et chips équivalents ; vérification par laboratoire tiers indépendant aux États-Unis avant expédition ; exigences de conformité côté acheteur ; clauses d'absence d'accès distant. https://www.bis.gov/press-release/department-commerce-revises-license-review-policy-semiconductors-exported-china

10. Sur les modalités économiques de l'export H200 vers la Chine (taxe de 25 % à l'importation aux États-Unis comme mécanisme constitutionnel de contournement de l'interdiction de taxe à l'export, plafond de volume, déclarations Jensen Huang du 17 mars 2026), cf. Bloomberg, *Nvidia Gets US License for Small Amount of H200 Exports to China*, 26 février 2026. https://www.bloomberg.com/news/articles/2026-02-26/nvidia-gets-us-license-for-small-amount-of-h200-exports-to-china

11. Sur l'annulation du projet Intel Magdeburg en juillet 2025, annoncé en 2022 avec 30 milliards d'euros d'investissement et 9,9 milliards d'euros de subventions allemandes engagées dans le cadre du Chips Act européen, cf. communications Intel et ministère allemand de l'Économie, juillet 2025.

12. Sur ESMC Dresden (coentreprise TSMC + Bosch + Infineon + NXP) : démarrage de production prévu en 2027, nœuds 28/22 nm CMOS et 16/12 nm FinFET, marchés

automobile et industriel, capacité cible de 480 000 wafers annuels en 2029. Cf. communiqué TSMC et partenaires, mises à jour 2025.

13. Sur le détail mémoire de Rhea1 (quatre piles HBM2E Samsung dans le boîtier), cf. *The Register*, *SiPearl finally tapes out Rhea1 supercomputer chip*, 9 juillet 2025. https://www.theregister.com/2025/07/09/sipearl_rhea1_tape_out/