

Rapport d'orientation stratégique
2026

DE LA PROSPECTIVE **À L'ACTION**

Recommandations stratégiques pour 2040

Rapport d'orientation stratégique
2026

DE LA PROSPECTIVE À L'ACTION

Recommandations stratégiques pour 2040

Avant-propos

Depuis 2020, le Cigref conduit chaque année un exercice de prospective pour mieux comprendre les transformations à l'œuvre et éclairer les choix de long terme de ses membres. Six années de travaux nous ont conduits à explorer les grandes évolutions du numérique, à envisager différents futurs possibles, à identifier plusieurs futurs souhaitables, à discerner les ruptures susceptibles de les infléchir et à réfléchir à ce que pourrait devenir la fonction numérique elle-même. Au fil de ces travaux, notre regard s'est déplacé de l'observation des transformations vers leurs conséquences, puis vers les décisions qu'elles appellent.

Cette nouvelle édition est l'occasion de prendre du recul et de mettre en perspective ces six années de réflexion. Elle en propose une synthèse, avec l'ambition simple de faire ressortir ce qui nous paraît aujourd'hui essentiel pour les grandes organisations et pour ceux qui ont la responsabilité de leur fonction numérique.

Les **quatre scénarios de contexte** présentés dans ce rapport prolongent ceux que le Cigref avait construits à partir de 2021. Ils tiennent compte des bouleversements intervenus depuis. L'accélération de l'innovation, particulièrement de l'intelligence artificielle, est concomitante aux évolutions géopolitiques (tensions et constructions réglementaires des marchés) : la fragmentation des échanges et la concentration des capacités technologiques qui en résultent appellent une lecture stratégique encore plus exigeante pour trouver les chemins de croissance, adapter les capacités de l'organisation, et ne pas ignorer les impératifs environnementaux, sociaux et sociétaux. Ils décrivent des futurs possibles, mais ne prétendent pas dire lequel adviendra. Ils doivent nous permettre d'éprouver nos choix.

Cinq messages clés constituent le point d'aboutissement de cette démarche. Ils portent sur **cinq transformations qui nous paraissent déterminantes à l'horizon 2040**. La première concerne l'industrialisation de l'intelligence artificielle et ses effets sur les modèles opérationnels et le travail. La deuxième porte sur la place de la fonction numérique dans la gouvernance, la stratégie et la compétitivité. La troisième concerne la recomposition des chaînes de valeur. La quatrième porte sur la nécessité de renforcer l'autonomie stratégique technologique, pour innover comme pour gérer nos risques. Enfin, la cinquième concerne l'enjeu de l'accès aux ressources et de la soutenabilité.

Chacun de ces messages est décliné en deux principes d'action, et complété par des recommandations. Leur pertinence a été confrontée aux quatre scénarios afin de distinguer ce qui relève des circonstances de ce qui doit, au contraire, rester une constante dans les choix des organisations. Une conviction se dégage de ces six années de prospective, et s'illustre particulièrement dans la dernière partie d'analyse approfondie des transformations à l'œuvre. L'usage des technologies numériques par les grandes organisations, au service de leur performance et de leur compétitivité, reposera de manière croissante sur leur capacité à anticiper, à choisir, à adapter leurs trajectoires et, lorsque cela devient nécessaire, à reconstruire. Une telle dynamique impliquera de plus en plus de se construire des marges de manœuvre technologiques, économiques, de capital humain et d'écosystèmes.

C'est là que la fonction numérique au sein de nos grandes organisations prend une dimension nouvelle. Elle reste indubitablement responsable de la maîtrise des systèmes d'information et des technologies, et elle doit davantage éclairer proactivement les choix de croissance et de compétitivité des métiers. Pour l'innovation comme pour la résilience des processus de l'entreprise, son enjeu est de construire et préserver la liberté d'action.

Ce rapport ne cherche pas à prédire le monde de 2040, ce n'est pas l'objet de la prospective. Il propose des repères pour s'y préparer, en agissant dès maintenant. Ces actions prises aujourd'hui sont les marges de manœuvre de demain.

Emmanuel Sardet
Président du Cigref

Résumé exécutif

PARTIE 1 - Scénarios de contexte

Cette partie modélise l'échiquier stratégique à l'horizon 2040, en croisant la dynamique de fragmentation de l'espace numérique avec le niveau d'exposition à la conflictualité mondiale. Son ambition est de proposer un éclairage sur les futurs possibles dans lesquels les grandes organisations et leur fonction numérique pourraient être plongées, sous la forme de quatre trajectoires non prescriptives.

Scénario 1 - Formation d'un bloc multi-régional de coalitions entre puissances moyennes

Face au duopole sino-américain, une coalition d'États stratégiques instaure une troisième voie multilatérale pour préserver les biens communs stratégiques. En Europe, une avant-garde structure la « Communauté européenne du numérique et de l'énergie » (CENE), mutualisant les capacités critiques par coopérations renforcées. L'espace numérique, partiellement interopérable, demeure régi par la transparence, la portabilité et un certain État de droit. Dans cette configuration, les directions numériques évoluent au sein d'alliances interrégionales garantissant des corridors d'approvisionnement, ce qui permet de neutraliser l'influence hégémonique des géants technologiques et d'élaborer de nouvelles normes de marché.

Scénario 2 - Archipélisation des partenariats public-privé

Le multilatéralisme institutionnel s'effondre au profit d'une géopolitique polycentrique où prolifèrent des « archipels » d'alliances thématiques, bilatérales et opportunistes. Face aux vulnérabilités de tous ordres, la puissance et le pouvoir circulent en réseaux croisés et les frontières entre prérogatives publiques et privées s'estompent. L'Union européenne assumant une coopération à géométrie variable (généralisation de « l'opt-out »), le dirigeant numérique devient un diplomate technologique. Sa mission consiste à sécuriser les moyens de création de valeur, à commencer par l'accès aux ressources critiques (énergie, calcul, données) ou la mutualisation de capacités de cyberdéfense pour assurer la continuité d'activité au sein de consortiums industriels.

Scénario 3 - Colonisation numérique et techno-féodalisme

Le cyberspace se fracture sous la domination d'empires technologiques privés, agissant comme des quasi-États affranchis des régulations territoriales. Ces géants phagocytent peu à peu l'intégralité des briques technologiques et couches de valeur, des matières premières aux agents d'IA, imposant unilatéralement leurs standards. L'Europe, privée de relais, subit une vassalité économique où l'accès à la technologie est conditionné à des allégeances implicites. Face à ces stratégies prédatrices, la fonction numérique mène un combat principalement défensif et asymétrique pour survivre à l'extorsion tarifaire en sanctuarisant le plus possible la maîtrise locale des codes sources, des opérations et de la confidentialité des données.

Scénario 4 - Bipolarisation sino-américaine exclusive

Le monde subit un « second Yalta », scindé en deux blocs technologiques hermétiques et antagonistes, sous la coupe de Washington et de Pékin. L'Europe, reléguée au rang de terrain d'affrontement indirect, subit l'arsenalisation des dépendances réciproques. L'interopérabilité s'éteint (protocoles, modèles d'IA et câbles sous-marins « bifurquent ») transformant le moindre choix d'infrastructure en marqueur d'appartenance civilisationnelle. Les entreprises sont acculées à des arbitrages binaires et contraintes de découpler leurs systèmes d'information pour opérer dans un cyberspace devenu un champ de bataille global, permanent et total.

PARTIE 2 - Messages clés et principes d'action

Cette seconde partie traduit les conclusions de la recherche prospective en leviers stratégiques actionnables. Son but est d'aider les dirigeants, et tout particulièrement les dirigeants du numérique, dans leurs choix stratégiques de long terme pour piloter la valeur par les risques et gagner en compétitivité.

« D'ici 2040, l'industrialisation de l'IA s'accompagnera d'une mutation profonde des modèles opérationnels et de la nature même du travail. »

Principe d'action 1 - Mise en valeur des compétences numériques à l'ère de l'IA

Recommandations - Structurer des parcours d'acculturation et de formation continue axés sur l'orchestration globale des agents artificiels, des processus métiers et des flux de données. Développer la culture de l'esprit critique et de la primauté du jugement humain, combinant culture générale, curiosité intellectuelle, logique et éthique. Valoriser les compétences de supervision, en les promouvant dans les référentiels métiers et les fiches d'objectifs annuels.

Principe d'action 2 - Maîtrise et usage raisonné des technologies d'IA

Recommandations - Sanctuariser le patrimoine informationnel par des architectures *Zero Trust*, des garde-fous, une politique d'authentification forte et un cadre strict face à l'exfiltration de données induite par le *Shadow AI*. Qualifier les jeux de données d'entrée et approvisionner continuellement les IA en « données fraîches ». Déployer des architectures interopérables et redévelopper certains pans applicatifs pour renforcer l'autonomie stratégique.

« D'ici 2040, la proposition de valeur de la fonction numérique sera déterminante pour la gouvernance, la stratégie et la compétitivité des organisations. »

Principe d'action 3 - Réappropriation technologique et ingénierie d'architectures

Recommandations - Valoriser les données d'entreprise considérées comme un véritable avantage concurrentiel durable. Réinternaliser de façon ciblée et s'émanciper de certains logiciels face à l'inflation des coûts, à la contrainte d'accès durable aux ressources de calcul et à la hausse prévisible des tarifs des licences. Créer des entités internes dédiées à l'automatisation transversale.

Principe d'action 4 - Ancrage de la fonction numérique au Comex

Recommandations - Renforcer la posture de facilitateur d'affaires par l'exploitation industrielle de cas d'usages métiers. Se réappropriier l'ingénierie des systèmes pour maximiser l'avantage comparatif de l'IA, en favorisant la maîtrise technique au-delà des achats de commodité en solutions, services, intégration et maintenance. Favoriser l'acculturation technologique continue et immersive des instances de gouvernance. Partager clairement la responsabilité de la création de valeur et de la gouvernance des risques entre directions.

« D’ici 2040, le protectionnisme économique et les barrières réglementaires imposeront une reconfiguration globale des chaînes de valeur. »

Principe d'action 5 - Rééquilibrage des chaînes de valeur et d'approvisionnement

Recommandations - Concevoir des architectures découplables, afin d'absorber les divergences réglementaires et techniques entre plaques régionales. Orienter commande et co-développement en faveur de l'émergence d'alternatives technologiques crédibles. Sanctuariser les capacités d'ingénierie et l'ancrage territorial des compétences clés, pour préserver la maîtrise directe de la propriété intellectuelle et du patrimoine applicatif.

Principe d'action 6 - Pilotage contractuel et manoeuvrabilité économique

Recommandations - Séquencer proactivement les engagements contractuels et diversifier les fournisseurs. Exiger une « ingénierie de sortie » contractuelle effective et maintenir le rapport de force par la capacité à descendre opérationnellement dans les couches techniques. Maîtriser financièrement le TCO de l'IA et responsabiliser les métiers sur le plan budgétaire, par une extension de l'optimisation des factures cloud vers un *FinOps AI*.

« D’ici 2040, la conjonction de crises géopolitiques rendra les stratégies d'autonomie technologique indispensables. »

Principe d'action 7 - Gestion par les risques et garantie de la continuité d'activité

Recommandations - Mettre en place une gestion des vulnérabilités géopolitiques centrée sur les maillons faibles et l'exigence de preuves tangibles de continuité d'activité. Augmenter la maîtrise capacitaire par l'entraînement au mode dégradé et l'action collective. Se préparer aux crises en entraînant les instances de gouvernance.

Principe d'action 8 - Mutualisation des moyens de défense et alliances de confiance

Recommandations - Mutualiser les capacités d'anticipation et de défense et l'organisation d'exercices de crise inter-organisations. Co-construire des communs technologiques et une action juridique collective face aux pressions extérieures. Valoriser un marché européen dit de la « *sovereignty* » (NIS2) et encourager la création de normes européennes pour la confiance numérique.

« D’ici 2040, les arbitrages technologiques devront intégrer des critères discriminants en matière d'accès aux ressources et d'impact environnemental. »

Principe d'action 9 - Anticipation des tensions sur les accès aux ressources critiques

Recommandations - Mettre en place une gouvernance de l'IA en faveur d'un usage raisonné, pilotée par un Indice de robustesse. Adapter les architectures techniques et optimiser l'implantation territoriale des infrastructures, face aux contraintes foncières et énergétiques. Co-construire un cadre réglementaire pour réguler les barrières d'accès aux ressources.

Principe d'action 10 - Optimisation de la soutenabilité matérielle des modèles d'affaires

Recommandations - Privilégier la commande responsable et diversifier les architectures processeurs. Étendre méthodiquement les cycles de vie physiques et le remplacement de composants. Rechercher la frugalité applicative comme bouclier contre l'obsolescence matérielle forcée.

PARTIE 3 - Analyse prospective : les 5 champs de transformation

Cette partie propose une étude approfondie des transformations numériques en cours, sous la forme d'une cinquantaine de fiches. La finalité est de permettre aux dirigeants d'anticiper les tendances lourdes et émergentes, les incertitudes et ruptures afin de tirer des avantages compétitifs même des plus grandes vulnérabilités.

Champ 1 - Économie du numérique

L'intelligence artificielle frappe d'obsolescence l'économie historique du logiciel et des ESN, impliquant une reconsidération des arbitrages « *make or buy* ». Par l'*hyper-capex*, les géants technologiques accaparent les infrastructures physiques générant une inflation tarifaire qui ampute les capacités d'investissement européennes. L'avènement du marché « *Business-to-Agent* » interroge la relation client, appelant les organisations à se prémunir contre la captation croissante de la valeur par les fournisseurs d'IA.

Champ 2 - Géopolitique du numérique

La confrontation sino-américaine structure l'ordre mondial, fusionnant puissance technologique et coercition d'État sur l'intégralité des chaînes de valeur. Le partenariat transatlantique subit une insécurité juridique chronique, exposant durablement les données européennes. Parallèlement, la militarisation des infrastructures civiles (IT/OT), l'état de la menace cyber, l'arsenalisation des monopoles, des monnaies numériques et de l'IA, imposent de rebâtir d'urgence une nouvelle architecture public-privé.

Champ 3 - Technologies et innovations

La compétition technologique reste subordonnée aux fondamentaux du cloud, centrée autour de la maîtrise du calcul, du stockage et des réseaux. L'IA franchit un cap vers l'exécution autonome, se spécialise pour gagner en efficacité et se retrouve embarquée dans des terminaux (*edge AI*) et des robots. La convergence des systèmes (IT/OT) et l'aube du quantique démultiplient les vulnérabilités cyber, tandis que les arbitrages entre modèles *open source* et propriétaires deviennent déterminants pour la maîtrise opérationnelle.

Champ 4 - Numérique responsable

L'illusion de l'immatérialité se heurte implacablement aux limites physiques : l'accaparement hydrique, énergétique et minéral interroge la soutenabilité du numérique. Parallèlement, l'intensification des chocs climatiques menace directement la continuité opérationnelle des infrastructures critiques. L'éco-efficacité (*Green IT* et *IT for Green*) devient, dès lors, un levier de rentabilité et de résilience sous contrainte, malgré la crainte que les gains offerts par la frugalité ne soient neutralisés par le paradoxe de « l'effet rebond » des usages.

Champ 5 - Travail et numérique

L'intégration de l'IA générative bouscule la matrice des périmètres et organisations des postes, substituant à la logique d'exécution une exigence de supervision à haute charge cognitive. Le marché fait face à une pénurie chronique de talents IT, une rupture de la transmission et une fracture de la capacité de jugement. Parallèlement, l'exfiltration des savoirs et savoir-faire *via* le *Shadow AI* et les cyberattaques ciblées font des collaborateurs un facteur de risque, tandis que l'IA agentique interroge le modèle historique d'externalisation *offshore*.

Table des matières

<i>Avant-Propos</i>	02
<i>Résumé exécutif</i>	04
<i>Table des matières</i>	08
<i>Objectifs et méthodologie du rapport</i>	10
<i>Membres du Conseil d'Orientation Stratégique</i>	128
<i>Membres du Conseil d'Orientation Stratégique Jeunes</i>	129
<i>Remerciements</i>	130

Partie 1. Scénarios de contexte **12**

Scénario 1 - Formation d'un bloc multi-régional de coalitions entre puissances moyennes	16
Scénario 2 - Archipélisation des partenariats public-privé	18
Scénario 3 - Colonisation numérique et techno-féodalisme	20
Scénario 4 - Bipolarisation sino-américaine exclusive	22

Partie 2. Messages clés et principes d'action **24**

Message clé 1 - « D'ici 2040, l'industrialisation de l'IA s'accompagnera d'une mutation profonde des modèles opérationnels et de la nature même du travail. »	28
Message clé 2 - « D'ici 2040, la proposition de valeur de la fonction numérique sera déterminante pour la gouvernance, la stratégie et la compétitivité des organisations. »	30
Message clé 3 - « D'ici 2040, le protectionnisme économique et les barrières réglementaires imposeront une reconfiguration globale des chaînes de valeur. »	32
Message clé 4 - « D'ici 2040, la conjonction de crises géopolitiques rendra les stratégies d'autonomie technologiques indispensables. »	34
Message clé 5 - « D'ici 2040, les arbitrages technologiques devront intégrer des critères discriminants en matière d'accès aux ressources et d'impact environnemental. »	36

Partie 3. Analyse prospective **44**

Tendances lourdes et émergentes, incertitudes et hypothèses de rupture à l'horizon 2040	
Champ 01 - Économie du numérique	48
Champ 02 - Géopolitique du numérique	66
Champ 03 - Technologies et innovations	82
Champ 04 - Numérique responsable	100
Champ 05 - Travail et numérique	116

Objectifs et méthodologie du rapport

Les Rapports d’Orientation Stratégique (ROS) ont pour ambition de servir les membres du Cigref dans leurs capacités à appréhender et préparer l’avenir. Cette mission nécessite d’acquérir une vision globale des enjeux numériques, replacés dans leur contexte. L’objectif est de proposer un outil capable d’accompagner les décideurs numériques dans leurs ambitions stratégiques, en appliquant des méthodes d’analyse prospective rigoureuse au sujet des principales transformations présentes et futures de leur écosystème afin d’en tirer des enseignements et d’identifier des leviers d’action.

L’édition 2026 du ROS, s’est nourrie des travaux de prospective stratégique portés par le Cigref ces 6 dernières années, en adoptant un regard critique afin de tirer les enseignements des évolutions observées depuis 2020, et d’en retenir les dynamiques susceptibles d’être structurantes à l’avenir ou de représenter de nouveaux champs des possibles.

Sur le plan de la gouvernance et de la comitologie, ce rapport s’est appuyé sur :

- Les travaux des six ROS précédents ;
- Les travaux menés en continu par l’équipe permanente du Cigref ;
- Le travail d’analyse prospective effectué par le groupe projet du Cigref et du cabinet de conseil en prospective Futuribles, construit sur une base méthodologique rigoureuse ;
- Les apports proposés par deux instances du Cigref sollicitées lors d’ateliers organisés entre janvier et juin 2026 :
 - **Le Conseil d’Orientation Stratégique (COS)** : composé de 5 administrateurs du Cigref et de 5 personnalités qualifiées, ce conseil définit chaque année les ambitions de la démarche de réflexion stratégique du Cigref, oriente ses travaux et apporte son expertise pour garantir leur qualité.
 - **Le Conseil d’Orientation Stratégique Jeunes (COS Jeunes)** : créé en 2023, ce conseil est composé de 75 collaborateurs de moins de 30 ans, issus de 40 organisations membres du Cigref. Il oriente les travaux de cette démarche en complément des positions du COS.

Le rapport est structuré en trois parties

La première partie a pour but d'interroger les évolutions possibles du contexte international à l'horizon 2040, au travers de quatre scénarios prospectifs explorant les futurs. Construits à partir des matériaux d'analyse rassemblés dans la troisième partie, ces scénarios prospectifs font se croiser deux grands axes structurants : l'évolution possible de l'espace numérique mondial (d'un modèle éclaté à un modèle interopérable) et l'évolution possible des jeux d'acteurs (allant de la construction proactive d'équilibres à l'exposition à la conflictualité). En déclinant ces scénarios selon le périmètre géographique mondial et européen et le périmètre sectoriel du numérique, cette approche méthodologique n'a pas de visée prescriptive, mais cherche plutôt à modéliser la complexité géostratégique pour offrir une base de réflexion permettant aux grandes organisations de se projeter.

La seconde partie propose des messages clés à l'horizon 2040 pour passer des trajectoires de contexte à l'action. Issus de l'analyse de fond développée en troisième partie, ces cinq messages clés transversaux constituent le résultat essentiel de cette réflexion. Pour assurer leur dimension pratique auprès des directions du numérique, chacun de ces messages est décliné en deux principes d'action assortis de bonnes pratiques. La clé de cette partie réside dans la confrontation de ces cinq messages aux quatre scénarios prospectifs de contexte. Ce "stress-test" a pour but de garantir la pertinence opérationnelle des 5 messages clés et de transformer des concepts théoriques en véritables outils de pilotage stratégique pour naviguer, se préparer et saisir des opportunités au sein de réalités fluctuantes.

La troisième partie représente la base de recherche et d'analyse fondamentale. Elle est structurée autour des cinq grands champs de transformations numériques identifiés par le Cigref dès le premier ROS de 2020, à savoir : géopolitique, économie, technologies, environnement et société. Sans prétention à l'exhaustivité, cette sélection entend offrir une approche la plus transversale possible à un objet d'étude aussi vaste, divers et changeant que le numérique.

Objectifs et méthodologie

Scénarios de contexte

Partie 1

Scénarios de contexte

Cette première partie propose un éclairage sur les futurs possibles dans lesquels les grandes organisations et leur fonction numérique pourraient être plongées, sous la forme de quatre trajectoires non prescriptives.

Méthodologie

L'édition 2021 du Rapport d'Orientation Stratégique (ROS) étudiait quatre scénarios sur les futurs possibles du numérique à horizon 2030-2035. Actualisés en 2022 afin d'intégrer les impacts des transformations géopolitiques, ces scénarios proposaient alors aux organisations membres du Cigref quatre trajectoires tendancielle pour se projeter dans la complexité du contexte géostratégique européen et mondial, avec un éclairage particulier donné au secteur numérique. Les multiples bouleversements du contexte international nous ont conduits, pour ce ROS de synthèse, à faire évoluer les scénarios prospectifs.

Les 4 scénarios de 2026 forment le substrat de tout le travail d'analyse prospective qui a été réalisé en profondeur dans la Partie 3 de ce rapport. Ils intègrent ainsi deux types de matériaux issus de l'étude des cinq champs de transformation du numérique :

- D'une part, de nouvelles tendances lourdes qui caractérisent par leur inertie et leur fort impact les grandes transformations en cours à l'horizon de 15 ans, viennent nourrir à des degrés divers les différents scénarios. Les acteurs numériques y seront exposés différemment selon leur nature et pourront y réagir selon leurs stratégies propres.
- D'autre part, un certain nombre d'hypothèses de rupture ont été introduites dans chaque scénario par le travail d'analyse prospective. Ces hypothèses peuvent être de nature aussi bien géopolitique, économique, technologique, environnementale que sociale.

Les deux premiers scénarios, intitulés « Colonisation numérique et technoféodalisme », et « Bipolarisation sino-américaine exclusive », sont, dans leur logique, identiques à ceux proposés en 2021 (« Une Chine conquérante dans un monde bipolaire » et « Far west, colonies digitales et cartels numériques »). En effet, l'évolution du contexte international observée va dans le sens d'une confirmation, et même d'une accélération de ces scénarios :

- Premièrement, la concentration actuelle de pouvoir et de richesses entre les mains de quelques empires privés, a internationalement consacré « l'heure des prédateurs » (Giuliano da Empoli). L'emprise commerciale et l'influence politique croissante de ces acteurs est tout particulièrement manifeste dans le secteur numérique, qui rassemble 90% du top 10 des plus grandes fortunes mondiales.
- Deuxièmement, le niveau de puissance acquis par la Chine confirme la compétition sino-américaine « à armes égales ». La politique américano-centrée du « *Make America Great Again* » et la capacité d'autosuffisance chinoise développée par la politique du « *Made in China 2025* » renforcent la logique de blocs qui se font face de manière exclusive.

En parallèle, deux nouveaux scénarios ont émergé, correspondant à deux réactions possibles des puissances publiques et privées face aux évolutions du contexte. Le scénario « **Formation d'un bloc multi-régional de coalitions entre puissances moyennes** » décrit une montée en puissance de coalitions régionales cherchant à mettre en place une nouvelle forme de multilatéralisme, en raison de la baisse d'influence des institutions internationales. Le scénario « **Archipélisation des partenariats publics-privés** » envisage la multiplication d'alliances thématiques et opportunistes conclues entre acteurs publics et privés, afin de répondre de manière pragmatique à leurs besoins. Ces deux scénarios traduisent à la fois l'émergence d'une logique de fragmentation globale et la recherche d'un meilleur équilibre dans les relations internationales.

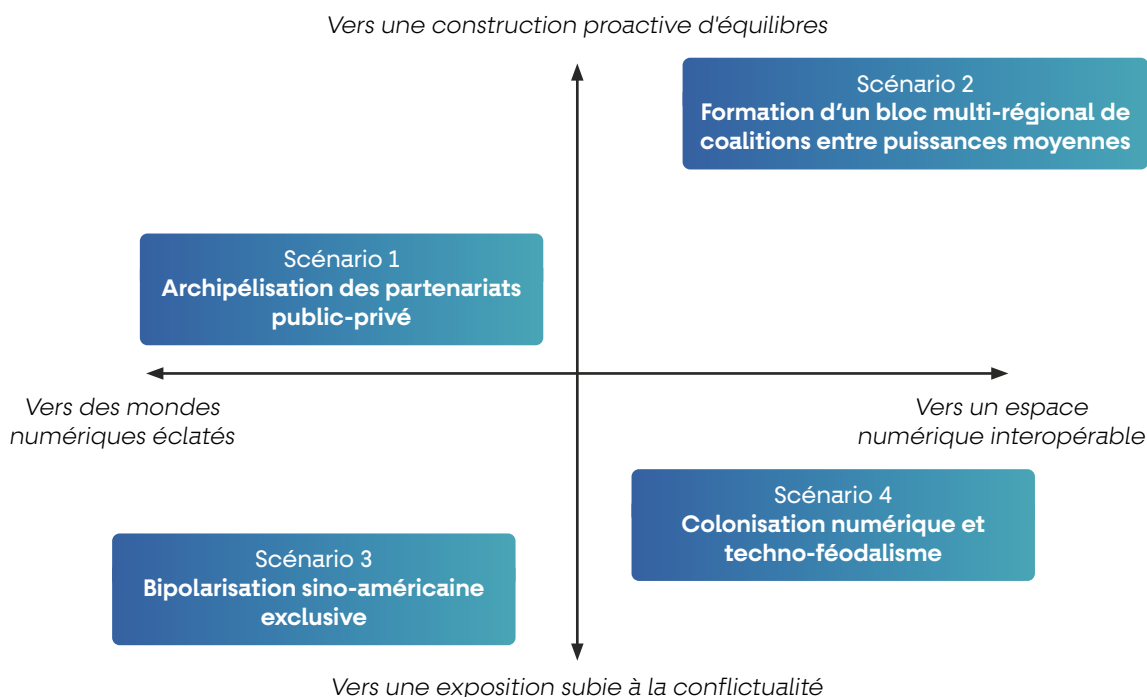
Ces quatre scénarios sont donc construits selon deux axes :

- L'évolution de la structure de l'espace numérique mondial, s'orientant vers des mondes éclatés ou, au contraire, vers un espace numérique interopérable ;
- L'évolution des jeux d'acteurs, visant une construction proactive d'équilibres ou, au contraire, subissant une plus grande exposition à la conflictualité.

Chaque scénario est décrit selon trois périmètres, en considérant tour à tour le périmètre géographique, mondial et européen, et le périmètre sectoriel du numérique.

Ces scénarios n'ont pas vocation à couvrir l'ensemble du champ des possibles, encore moins à être prescriptifs, mais à proposer des éclairages sur les futurs possibles dans lesquels les grandes organisations et leur fonction numérique pourraient être plongées. Ces scénarios constituent donc une base de réflexion pour les organisations et ont contribué à identifier les cinq messages clés à l'horizon 2040 présentés en deuxième partie de ce rapport et à élaborer les principes d'action qui en découlent.

4 scénarios prospectifs de contexte à l'horizon 2040



Scénario 01

Formation d'un bloc multi-régional de coalitions entre puissances moyennes

Face à la bi-polarité sino-américaine, des « puissances moyennes » s'allient pour trouver une troisième voie qui, malgré un périmètre plus restreint, offre un espace numérique interopérable, régi par le droit, au service de la résilience et de la compétitivité. Dans chaque région, des coalitions se forment et un bloc multi-régional se constitue, faisant naître une nouvelle forme de multilatéralisme.

Périmètre mondial

Le système international reste instable, mais les quelques « poches de coalitions régionales » entre puissances moyennes évitent une bipolarisation stricte, et si les tensions géopolitiques persistent, la conflictualité reste contenue. Ces coalitions parviennent à imposer, à leur niveau, ou à l'échelle mondiale lorsqu'elles sont rassemblées en un bloc multi-régional, plusieurs standards dans les secteurs essentiels des énergies, de la gestion des eaux, des infrastructures numériques, de la santé, des transports, de la banque et des marchés financiers. Elles soutiennent également des initiatives pour préserver les biens communs stratégiques comme l'espace extra-atmosphérique, l'espace numérique, le spectre électromagnétique, l'Antarctique, le vivant et le climat, ou les fonds marins. Le succès de ces initiatives repose sur la coopération d'États stratégiques déterminés à traiter un nombre restreint d'enjeux jugés prioritaires et à aborder leur caractère multifactoriel, avec cohérence et sur le temps long.

Périmètre européen

Une nouvelle dynamique à « 6 nations pionnières » s'instaure en Europe dans le but de concentrer forces et capitaux pour mutualiser des capacités critiques, et faire passer à l'échelle des partenariats ciblés. Un groupement sectoriel baptisé « Communauté européenne du numérique et de l'énergie » (CENE) est créé, basé sur un principe juridique européen de « coopération renforcée » devenu la norme en Europe, qui rend un acte applicable uniquement aux États membres qui le désirent. Cette communauté de réalisation parvient à préserver des marges de manœuvre grâce à des alliances industrielles équilibrées, des normes communes clarifiées, un droit de la concurrence vraiment appliqué, une diplomatie technologique active, des mécanismes anti-coercition crédibles. À l'échelon régional, le marché est plus ouvert à la concurrence et les produits et services sont plus nativement conformes aux standards européens, même si les risques de fragmentation interne de l'UE restent un défi.

Périmètre numérique

Le numérique devient un espace partiellement interopérable. Pour maintenir des standards ouverts et renforcer sa dynamique collective, la Communauté européenne du numérique et de l'énergie (CENE) s'associe à des initiatives d'autres coalitions régionales (Canada-Mexique-Brésil pour les Amériques, Japon-Inde-Singapour-Corée du Sud pour l'Asie, Egypte-Nigéria-Kenya-Afrique du Sud pour l'Afrique, Arabie saoudite-Qatar-Émirats-arabes-unis pour le Moyen-Orient). Le bloc multi-régional ainsi constitué construit des partenariats d'approvisionnement privilégiés (chaînes logistiques de matières premières, corridors d'énergie et de transfert de données, capacités de calcul) et défend une gouvernance du numérique fondée sur la transparence, l'explicabilité, la portabilité et la réversibilité. Les géants technologiques américains ou chinois conservent une influence majeure, mais sont contraints par des coalitions d'États capables de peser réellement sur les cadres normatifs et l'accès aux marchés. Le numérique demeure un champ intense de compétition et d'exercice de la puissance, mais non un instrument exclusif de domination.



Scénario

02

Archipélisation des partenariats public-privé

Les blocs régionaux arrimés aux grandes institutions internationales ne tiennent plus. À la place émergent des « archipels » d'alliances mouvantes, thématiques, opportunistes, où États, entreprises et organismes de recherche coopèrent selon leurs besoins. Des partenariats hybrides et principalement bilatéraux ou sectoriels se multiplient de façon inédite, dans une vision « constructualiste » et capacitaire de la puissance.

Périmètre mondial

Le multilatéralisme hérité des accords de Bretton Woods et de Marrakech s'efface au profit d'une géopolitique fragmentée et polycentrique. Les alliances se structurent autour des goulots d'étranglement et des maillons faibles des chaînes de valeur. Les États ne peuvent plus tout faire seuls, les entreprises non plus et la co-dépendance devient un moteur d'action. La conflictualité est diffuse, systémique, mais les interdépendances considérablement multipliées empêchent une rupture totale. La puissance circule entre acteurs publics et privés dans un réseau d'interactions mondiales plus dense, créant une géopolitique plus instable, mais fonctionnelle.

Périmètre européen

L'Union européenne devient un espace de coopération modulaire et à géométrie variable. Le principe « d'opt-out », permettant aux États membres qui refusent de participer à certaines politiques communes de négocier leur retrait, n'est plus une exception mais une règle de fonctionnement. Les nations confrontées de manière asymétrique aux ruptures d'approvisionnement, aux pressions extraterritoriales et à une conflictualité hybride croissante, développent des alliances public-privé différenciées, parfois concurrentes. Le socle commun, bien que réduit, se renforce et la résilience opérationnelle des États s'ajoute aux « critères de convergence » européens, avec des standards communs, des mécanismes d'alertes, des critères d'interopérabilité minimale et des obligations de transparence. Les directives DORA et NIS2 inspirent une modification du traité constitutif de l'UE (TFUE), dans le but d'instituer une « Communauté pour la résilience européenne » (ou CRE). Cette instance de coordination est chargée d'agréger les capacités nationales et d'orchestrer la supervision distribuée. La forte décentralisation des pouvoirs délégués *de facto* à l'UE par les États membres est compensée par la multiplication des partenariats public-privé.

Périmètre numérique

Le numérique se structure en « archipels » de confiance. États, consortiums sectoriels et organismes de recherche coopèrent de façon opportuniste, thématique et souvent bilatérale. Ces alliances se recomposent selon les besoins afférents à l'accès aux matières premières, aux GPU et clusters de calcul, aux corridors de données, à la sécurisation énergétique ou encore au partage de renseignements cyber. Les infrastructures critiques sont mutualisées au sein de coalitions *ad hoc* qui font naître des canaux de partage d'informations de crise, des *red teams* inter-organisations, des SOC ou des capacités anti-DDoS enrichies par l'IA communes. Les organisations naviguent dans un environnement où l'accès aux ressources critiques dépend de leur capacité à rejoindre ou à maintenir ces alliances. Les grands acteurs numériques, fournisseurs comme utilisateurs, deviennent en cela des acteurs diplomatiques à part entière. Les frontières public-privé deviennent poreuses, certaines entreprises participant activement à la sécurité nationale, tandis que les États cherchent à orchestrer les capacités industrielles privées avec volontarisme et planification pour maintenir la résilience de leurs tissus nationaux.



Scénario

03

Colonisation numérique et techno-féodalisme

Le numérique se fracture et dépend d'une poignée d'empires technologiques privés. La logique prédatrice absorbe peu à peu toutes les couches technologiques et chaînes de valeur.

Périmètre mondial

Bien qu'elles ne puissent pas disposer de souveraineté, les grandes multinationales deviennent nominalement des quasi-États dotés de capacités décisionnelles, financières, matérielles et informationnelles supérieures à pratiquement toutes les puissances intermédiaires. Les décisions unilatérales de ces acteurs systémiques peuvent déstabiliser des régions entières, provoquer des ruptures d'approvisionnement, reconfigurer des chaînes de valeur mondiales ou remplacer la médiation étatique dans des conflits intérieurs ou internationaux, rendant caducs le concept d'État-nation moderne et son ancrage territorial. Malgré les risques de déstabilisation que leurs stratégies prédatrices et apatrides impliquent, la régulation de ces acteurs est pratiquement devenue impossible, car ils contrôlent des nœuds essentiels pour les flux mondiaux et ont acquis localement de nombreux statuts d'opérateurs de prérogatives régaliennes. Leur démantèlement est également rendu inenvisageable, à cause de leur poids et des ramifications qu'ils possèdent sur les marchés financiers mondiaux.

Périmètre européen

La plupart des acteurs européens, États comme organisations, perdent en autonomie stratégique, hormis quelques-uns dont le poids économique ou le positionnement dans les chaînes de valeur mondiales bénéficient à ces grandes multinationales. Les marges de manœuvre réglementaires se réduisent et les initiatives dites de « *sovereignty* » (certifications de sécurité et politiques industrielles stratégiques) peinent à rivaliser avec la puissance financière et l'intégration verticale de ces géants. Les organisations européennes sont contraintes d'adopter des solutions extra-européennes « sur étagère », faute de capacités d'innovation en interne, de sources de financement public-privé suffisantes et d'alternatives crédibles et à l'échelle à des prix compétitifs.

Périmètre numérique

Le numérique se fracture en territoires contrôlés par des empires technologiques privés qui absorbent progressivement toutes les couches de la pile technologique et des chaînes de valeur, des matières premières aux agents IA, en passant par les puces, l'énergie, les data centers, les câbles, les plateformes, la distribution. Certains géants abusent de leur position dominante par des stratégies prédatrices visant à se débarrasser massivement et brutalement de tous les clients dont les dépenses en volume ou marge ne répondent pas à leurs attentes. Certains acteurs vont plus loin, en imposant leurs standards, leurs écosystèmes dominants et leurs règles contractuelles, au point de se priver volontairement de fournir leurs solutions à des régions entières par pure représaille envers certaines législations locales jugées défavorables. Dans ce contexte, les infrastructures deviennent captives, les données circulent sous contrainte, et les organisations évoluent dans des environnements fermés où l'accès aux technologies dépend d'allégeances implicites. La maîtrise locale des codes sources, de la confidentialité et de la disponibilité des données, des opérations (incluant les maintenances et les mises à jour), des infrastructures et des clauses contractuelles en est considérablement dégradée. Le numérique cesse d'être un espace ouvert pour devenir un système féodal, structuré par des suzerains technologiques et des vassaux économiques.



Scénario

04

Bipolarisation sino-américaine exclusive

Le monde forme à nouveau deux blocs exclusifs et deux États, la Chine et le États-Unis, s'accaparent ressources et territoires. Ces super-puissances usent du levier technologique pour s'affronter et profitent d'un alignement étroit entre leurs champions numériques nationaux et leurs administrations publiques.

Périmètre mondial

Le monde se recompose en deux sphères d'influence exclusives, rappelant un second moment Yalta. Les États-Unis verrouillent l'Amérique du Nord au Sud par néo-isolationnisme, n'hésitant plus à recourir à des démonstrations de force militaires ou technologiques, tandis que la Chine consolide son influence en Asie et en Afrique et propose des initiatives de coopération mondiale. Les zones intermédiaires deviennent des terrains de confrontation indirecte, où sanctions, contrôles et restrictions à l'export, menaces de « *kill switch* » et pressions diplomatiques redessinent les chaînes de valeur mondiales. Les alliances traditionnelles s'effritent, les institutions internationales perdent leurs capacités d'arbitrage, et la conflictualité devient si permanente et habituelle que la neutralité devient impossible. Dans le nouveau paradigme stratégique de « compétition, contestation, affrontement », chaque choix d'architecture ou de fournisseur est interprété comme un acte d'alignement géopolitique ou de « mise sous parapluie », comme dans le cas des États non dotés qui se placent sous la protection d'une puissance nucléaire pour assurer leur propre survie.

Périmètre européen

Dans la guerre économique que se livrent les deux super-puissances, l'Europe est un terrain d'affrontement indirect et subit l'arsenalisation de leurs dépendances réciproques. Les pressions politiques, économiques et réglementaires s'intensifient, notamment à travers l'incompatibilité volontaire de certains standards, l'exclusion ciblée de certains fournisseurs jugés « à risque », et des alignements diplomatiques imposés par les circonstances. L'UE tente de préserver une autonomie relative, mais ses marges de manœuvre et son poids sur la scène internationale se réduisent, au point de la reléguer dans la catégorie « tiers-monde ».

Périmètre numérique

Le numérique se structure autour de deux écosystèmes incompatibles et qui se font face : le bloc américain dominé par les *hyperscalers* et le bloc chinois fondé sur l'intégration État-entreprises. Le découplage s'étend des infrastructures physiques aux couches logicielles, et les standards, les infrastructures énergétiques, les modèles d'IA, les câbles, les satellites et même les solutions de sécurité numérique bifurquent et se dupliquent en deux sphères distinctes. Les organisations doivent choisir un camp, car l'interopérabilité se restreint et s'avère politiquement sensible. Les technologies, les protocoles et les fournisseurs s'imposent comme des marqueurs d'appartenance civilisationnelle. Les infrastructures clés de l'espace numérique (énergie, cloud-IA, réseaux) deviennent des enjeux de sécurité nationale, et les organisations européennes, dans un champ bien plus vaste que celui des secteurs critiques de NIS2, se trouvent *de facto* incorporées aux arbitrages étatiques en matière de souveraineté, d'accès aux technologies et de continuité d'opération. L'espace numérique cesse d'être un commun stratégique et se transforme en un véritable champ de bataille énergétique, financier, normatif, informationnel, où la moindre dépendance peut être instrumentalisée dans la rivalité sino-américaine, comme un levier de coercition, voire d'humiliation stratégique.



Messages clés et principes d'action

Partie 2

Messages clés et principes d'action

Cette seconde partie traduit les conclusions de la recherche prospective en leviers stratégiques actionnables.

Méthodologie

Chaque année, le Rapport d'Orientation Stratégique (ROS) identifie une série de messages clés et principes d'action dans le but de traduire les conclusions de la recherche prospective en leviers stratégiques actionnables.

Cette édition de synthèse fixe le cap à l'horizon 2040 à partir de « **messages clés** » transversaux portant sur **cinq transformations qui nous paraissent déterminantes**. Ces messages sont le fruit du travail d'analyse prospective réalisé en profondeur et présenté dans la Partie III de ce rapport.

Sans prétention à l'exhaustivité, ces messages clés sont déclinés en **dix principes d'action** qui font l'objet d'une description détaillée et sont complétés par une liste de **recommandations**. Ces éléments ont pour ambition d'aider les organisations, et tout particulièrement leurs directions du numérique, dans leurs choix stratégiques de long terme pour :

- **Se préparer** aux transformations en cours et à venir ;
- **Naviguer** dans un monde en perte de repères et aux multiples perturbations ;
- **Saisir les opportunités** ouvertes par les nouvelles trajectoires numériques.



Les messages clés et principes d'action

« D'ici 2040, l'industrialisation de l'IA s'accompagnera d'une mutation profonde des modèles opérationnels et de la nature même du travail. »

Principe d'action 1. Mise en valeur des compétences numériques à l'ère de l'IA

Principe d'action 2. Maîtrise et usage raisonné des technologies d'IA

« D'ici 2040, la proposition de valeur de la fonction numérique sera déterminante pour la gouvernance, la stratégie et la compétitivité des organisations. »

Principe d'action 3. Réappropriation technologique et ingénierie d'architectures

Principe d'action 4. Ancrage de la fonction numérique au Comex

« D'ici 2040, le protectionnisme économique et les barrières réglementaires imposeront une reconfiguration globale des chaînes de valeur. »

Principe d'action 5. Pilotage contractuel et manoeuvrabilité économique

Principe d'action 6. Rééquilibrage des chaînes de valeur et d'approvisionnement

« D'ici 2040, la conjonction de crises géopolitiques rendra les stratégies d'autonomie technologiques indispensables. »

Principe d'action 7. Gestion par les risques et garantie de la continuité d'activité

Principe d'action 8. Mutualisation des moyens de défense et alliances de confiance

« D'ici 2040, les arbitrages technologiques devront intégrer des critères discriminants en matière d'accès aux ressources et d'impact environnemental. »

Principe d'action 9. Anticipation des tensions sur les accès aux ressources critiques

Principe d'action 10. Optimisation de la soutenabilité matérielle des modèles d'affaires

« D'ici 2040, l'industrialisation de l'IA s'accompagnera d'une mutation profonde des modèles opérationnels et de la nature même du travail. »

Principe d'action 1. Mise en valeur des compétences numériques à l'ère de l'IA

La recomposition du marché du travail, sous le double effet de la transition démographique et de l'accélération technologique, accentue les tensions quantitatives et qualitatives sur les métiers du numérique. Dans un paysage concurrentiel marqué par une « guerre des talents » exacerbée et une quête de sens accrue des collaborateurs, la nature du travail futur pourrait dépasser la simple maîtrise technique individuelle au profit d'une synergie globale entre l'humain et la machine, valorisant réellement celui-ci. L'enjeu pour les directions numériques consisterait à faire de l'IA, si cela est nécessaire et justifié, un catalyseur de compétences et un vecteur d'émancipation professionnelle, plutôt qu'un outil de substitution. Pour manager cette nouvelle force de travail hybride (*Hybrid Workforce*), mêlant collaborateurs et agents autonomes, un alignement stratégique des instances de gouvernance s'impose, du Conseil d'administration à la Direction des ressources humaines. Le rôle de la fonction numérique, facilitatrice d'affaires (*business enabler*) des usages et garante éthique et technique des systèmes, pourrait s'en trouver renforcé.

Recommandations

- **Structurer des parcours d'acculturation et de formation continue**, axés sur l'orchestration globale des agents artificiels, des processus métiers et des flux de données. Cette dynamique d'apprentissage (*upskilling, reskilling*) permettrait de répondre à l'évolution rapide des fiches de poste et d'endiguer le recours à des solutions non validées.
- **Développer la culture de l'esprit critique et de la primauté du jugement humain**, combinant culture générale, curiosité intellectuelle, logique et éthique. Face aux risques d'appauvrissement cognitif, les organisations de pointe pourraient se positionner comme des « orchestrateurs du développement humain », en valorisant les tâches les plus humainement formatrices pour l'esprit, stimulantes pour les qualités propres des individus et créatrices de valeur.
- **Valoriser les compétences de supervision**, en promouvant dans les référentiels métiers et les fiches d'objectifs annuels le temps consacré au paramétrage, à la supervision, à la vérification et à l'actualisation des modèles d'IA. Cette reconnaissance, à engager avec le soutien du département RH, est un prérequis indispensable pour pérenniser l'engagement des équipes et garantir l'efficacité des investissements technologiques.

À l'horizon 2040, la résilience RH et l'innovation managériale pourraient devenir les véritables signatures des organisations matures, capables de transformer une rupture technologique prometteuse en un véritable progrès organisationnel légitime, durable et socialement responsable.

Principe d'action 2. Maîtrise et usage raisonné des technologies d'IA

L'industrialisation de l'IA au profit des besoins humains et de l'économie réelle devrait impliquer de reconfigurer les modèles organisationnels et opérationnels des entreprises et administrations. L'intégration fine, adaptée et maîtrisée des différents maillons de l'IA pourrait devenir un atout différenciant pour certaines organisations, et un enjeu de survie des modèles d'affaires pour d'autres. À l'échelle industrielle, ces technologies requièrent un écosystème propre à leur bon fonctionnement et à leur bon usage. Si l'intégration d'agents avancés offre un potentiel de productivité local inédit, le besoin d'accès élargi aux systèmes d'information concentre des risques technologiques majeurs de perte de maîtrise des données, des connaissances métiers et des usages.

Recommandations

- **Sanctuariser le patrimoine informationnel.** Face aux usages non validés (*Shadow AI*), les directions numériques doivent pouvoir segmenter les différents stocks de données et maîtriser leurs flux en temps réel. Le déploiement d'architectures globales *Zero Trust*, de garde-fous (*AI Gateways & Guardrails*), de politique d'authentification forte (IAM), et de cadres d'usage stricts pourrait prévenir l'exfiltration de données sensibles et protégerait la valeur stratégique des processus internes.
- **Qualifier les jeux de données d'entrée** en lien avec les métiers (*Data Stewards, Business Owners*), passant par le marquage actif des données (*watermarking*), garantissant la traçabilité, en complément d'audit des interactions d'agent, avec explicabilité continue des algorithmes sous-jacents pour les IA à « haut risque » soumis à l'*AI Act*.
- **Approvisionner continuellement les IA en données « fraîches »**, avec une validation déterministe et humaine en sortie, condition essentielle pour garder un ancrage dans le réel et éviter l'appauvrissement cognitif et la dégradation de l'information en circuit fermé.
- **Déployer des architectures interopérables**, misant sur des protocoles d'échange standardisés (type MCP) pour offrir un cadre strictement cloisonné d'accès des IA aux bases de données internes. L'utilisation de protocoles ouverts (type UCP) pourrait favoriser la transparence des algorithmes de recommandation IA et limiter les potentielles rentes d'interface des grands fournisseurs, tout au long des parcours transactionnels intégrés aux agents.
- **Redévelopper certains pans applicatifs pour renforcer l'autonomie stratégique**, malgré la hausse des coûts d'inférence et la contrainte des ressources de calcul. Les décideurs pourraient gagner à substituer l'achat de certains logiciels critiques « sur étagère » par des redéveloppements ciblés. La création d'un pôle d'excellence (*AI Factory*) ou d'une filiale dédiée à l'automatisation transversale permettrait d'éviter les risques de disruption induits par le transfert à l'externe des connaissances métiers.

À l'horizon 2040, ce processus de maîtrise technologique et de contrôle effectif des interactions d'agent à agent pourrait être renforcé par des alliances stratégiques. La coopération entre organisations et États européens, conjuguée à une contractualisation stricte sur la conservation et l'entraînement des données, permettrait d'imposer ces pratiques éthiques et opérationnelles comme de véritables prérequis de marché, au-delà des simples positions de principe.

« D'ici 2040, la proposition de valeur de la fonction numérique sera déterminante pour la gouvernance, la stratégie et la compétitivité des organisations. »

Principe d'action 3. Réappropriation technologique et ingénierie d'architectures

La rupture technologique induite par l'émergence de l'IA, notamment agentique, devrait placer les directions numériques devant des arbitrages hautement structurants. D'un côté, l'intégration de *plug-ins* et d'agents avancés ouvre des perspectives de productivité inédites, en réduisant les frictions entre données, outils et utilisateurs. De l'autre, le besoin d'accès très large des IA pour opérer automatiquement concentre des risques majeurs de dépendance technologique, d'exfiltration des données, et de perte de maîtrise des usages et des coûts, tout particulièrement lorsque les salariés contournent les solutions métiers validées pour adopter des agents plus rapides, plus souples et plus personnalisables (*Shadow AI*). La création de valeur et les contraintes qui y sont associées pourraient se déplacer vers la conception d'architectures globales, robustes et explicables. Le goulot d'étranglement des organisations se situerait alors moins dans la capacité à générer des lignes de code que dans l'adaptation stratégique et dans la manoeuvrabilité des gouvernances numériques.

Recommandations

- **Valoriser en priorité les données d'entreprise considérées comme un véritable avantage concurrentiel durable**, les entités devant pour cela être capables de structurer et d'exploiter leurs propres « gisements internes », en complément d'une modélisation précise de leurs processus métiers et industriels spécifiques.
- **Réinternaliser de façon ciblée et s'émanciper des progiciels**, face à l'inflation des coûts, à la contrainte d'accès durable aux ressources de calcul et à la hausse prévisible des tarifs des licences. Les décideurs pourraient tirer bénéfice à ne plus acheter certains logiciels critiques « sur étagère », au profit d'appels d'offres de redéveloppement de tout ou partie de ces actifs.
- **Créer des entités internes d'automatisation**. La structuration volontaire d'une filiale ou d'un pôle interne dédié à l'automatisation transversale pourrait constituer un levier d'indépendance opérationnelle majeur, assurant la rétention des connaissances métiers au sein de l'organisation sans transfert à des tiers ou risque de désintermédiation forcée.

À l'horizon 2040, la réappropriation technologique et l'ingénierie d'architecture pourraient s'imposer comme des voies d'autonomie stratégique et de manoeuvrabilité commerciale des organisations face aux monopoles technologiques.

Principe d'action 4. Ancrage de la fonction numérique au Comex

L'adoption des technologies d'IA à une échelle industrielle et la régionalisation croissante des enjeux numériques devraient achever de faire de la fonction numérique la colonne vertébrale des modèles d'affaires et de la résilience des organisations. Ce changement d'échelle induit durablement une évolution déjà engagée de son positionnement au sein des entreprises et des administrations. Longtemps considérée comme un centre de coûts ou une fonction technique de support, la direction numérique a toutes les chances de s'imposer comme un partenaire d'affaires à haute valeur ajoutée et un copilote stratégique de la trajectoire globale. Quels que soient le secteur, l'intensité numérique des activités et leur exposition géographique à la réglementation et aux tiers, les choix numériques conditionnent de manière croissante la résilience opérationnelle, la compétitivité économique, l'agilité organisationnelle et l'innovation productive. L'éparpillement de la représentation des différentes prérogatives numériques au sein des instances décisionnelles constituerait une vulnérabilité majeure.

Recommandations

- **Renforcer la posture de facilitateur d'affaires**, permettant à la fonction numérique d'accentuer son rôle de conseil et de stratège. Ce positionnement exige d'outiller et d'accompagner les directions métiers dans l'exploitation industrielle de leurs cas d'usages, tout en garantissant la cohérence et la sécurité des architectures systèmes et leur alignement avec la chaîne de valeur.
- **Se réappropriier l'ingénierie des systèmes pour maximiser l'avantage comparatif de l'IA**, en favorisant la maîtrise technique au-delà des achats de commodité en solutions, services, intégration et maintenance. La différenciation de la fonction numérique compétitive pourrait se faire par la conception d'architectures holistiques, modulaires et interopérables, la structuration rigoureuse des bases de données pour leur exploitation par des agents autonomes, et l'optimisation fine des modèles d'IA spécialisés et de leurs empreintes financière et humaine.
- **Favoriser l'acculturation technologique continue et immersive des instances de gouvernance**, pour combler l'éventuel déficit de compréhension stratégique au plus haut niveau. La création d'un « passeport numérique » ou la réalisation de travaux prospectifs réguliers permettrait aux membres du Comex et du Conseil d'administration d'arbitrer de manière éclairée et cohérente, sur le temps long, les stratégies d'investissement, de maîtrise des dépendances et d'évaluation de la soutenabilité environnementale et financière des modèles automatisés.
- **Partager la responsabilité de la création de valeur et de la gouvernance des risques** entre la fonction numérique, la direction financière et juridique, la direction des ressources humaines, des achats, de la communication et des opérations. Cette approche conjointe ferait du numérique un projet d'entreprise transversal, garantissant le pilotage fin des coûts structurants, la protection du patrimoine informationnel et la convergence réelle entre opportunités business et gestion des perturbations du numérique, de quelque nature qu'elles soient.

À l'horizon 2040, l'ancrage de la fonction numérique au plus haut niveau décisionnel pourrait s'imposer comme une condition *sine qua non* de performance et de compétitivité durable pour une part considérable des organisations.

« D'ici 2040, le protectionnisme économique et les barrières réglementaires imposeront une reconfiguration globale des chaînes de valeur. »

Principe d'action 5. Rééquilibrage des chaînes de valeur et d'approvisionnement

La fragmentation normative concomitante à la montée des protectionnismes économiques devrait conduire à une reconfiguration durable de la géographie du numérique. L'idéal d'un marché mondial et unifié s'efface au profit d'un monde plutôt structuré en « plaques régionales » autonomes, chacune porteuse de ses propres régulations, standards techniques et exigences de souveraineté. Pour les organisations opérant à l'international, le maintien des opérations sur différentes zones géographiques devrait exiger une capacité d'adaptation fine aux spécificités locales, les contraignant parfois à des arbitrages d'ancrage, de sélection de marché ou de désengagement au gré des alliances géoéconomiques. Face à ces incertitudes, la résilience des organisations ne pourra pas dépendre exclusivement du soutien ou de l'intervention des pouvoirs publics

Recommandations

- **Concevoir des architectures découplables et veiller à la modularité de l'urbanisation**, afin d'absorber les divergences réglementaires et techniques entre plaques régionales. En concevant des systèmes d'information nativement agiles, hautement cloisonnés et intrinsèquement interopérables, les organisations garantiraient la flexibilité nécessaire pour opérer simultanément sur des marchés morcelés, sans subir de blocages à l'entrée, ni de ruptures d'approvisionnement.
- **Orienter commande et co-développement régional** en faveur de la masse critique indispensable à l'émergence d'alternatives technologiques crédibles. Afin d'éviter les pièges de l'entente ou du cartel, cette convergence de la commande privée pourrait être tirée par la co-innovation sur des briques pré-concurrentielles neutres (solutions *open source* génériques). Par la constitution de consortiums industriels ou la mutualisation des fonds pour accompagner la maturation industrielle des entreprises jusqu'à leur mise en bourse (capital risque, private equity, fonds de dotation), l'offre régionale pourrait également être structurée dans le but de sécuriser les approvisionnements des organisations en composants critiques tout au long de leurs chaînes de valeur, sans attendre l'introduction de politiques publiques plus volontaristes.
- **Sanctuariser les capacités d'ingénierie et l'ancrage territorial des compétences clés**, pour préserver la maîtrise directe de la propriété intellectuelle et du patrimoine applicatif. Ce levier repose sur la réinternalisation de l'assemblage de certaines briques stratégiques prioritaires et sur le maintien d'écosystèmes régionaux de savoir-faire. Avoir une démarche proactive concrète et à la portée des organisations permettrait de prévenir la fuite des talents et de contrer les risques de désintermédiation forcée par des acteurs hégémoniques.

À l'horizon 2040, seules la rigueur d'architecture, l'alliance industrielle entre grands donneurs d'ordres et la maîtrise locale des compétences d'ingénierie permettront de sécuriser la résilience des chaînes d'approvisionnement numériques au sein d'un espace économique mondial plus morcelé.

Principe d'action 6. Pilotage contractuel et manoeuvrabilité économique

Le pilotage par les risques devrait s'imposer comme un chantier majeur pour la maîtrise des dépendances technologiques et leur impact sur les modèles d'affaires. Sous l'effet de l'absorption des infrastructures stratégiques par un nombre restreint d'acteurs hégémoniques, le périmètre des vulnérabilités s'élargit au-delà du logiciel, touchant à la puissance des modèles d'IA et à leurs capacités de calcul, au stockage et aux réseaux, à l'énergie et aux matières premières. Sous l'effet de la pression induite par les investissements technologiques sans précédents, la fonction numérique pourrait s'affirmer comme un acteur incontournable de la manoeuvrabilité économique des organisations.

Recommandations

- **Séquencer les engagements contractuels et diversifier les fournisseurs**, en distinguant fonctions applicatives génériques et services critiques ou données à forte sensibilité ("*minimum viable company*"). Outre les renégociations proactives de contrat avant leur échéance, les organisations pourraient arbitrer entre des engagements courts (24-36 mois) prévenant le *vendor lock-in* et des partenariats de long terme assurant la stabilité des actifs socles. Cette autonomie décisionnelle exigerait de généraliser la diversification des fournisseurs (stratégies multi *cloud&IA*, avec options *on-premise*, *edge computing* et *open source*). Ce pilotage pourrait s'appuyer sur des outils de qualification des capacités de résilience, à l'image de l'IRN, ou la construction collective d'un cadran d'aide à la décision stratégique à l'échelle européenne, complémentaire à ceux des cabinets d'analyse anglo-saxons.
- **Exiger une « ingénierie de sortie » contractuelle effective et maintenir le rapport de force par la capacité à descendre opérationnellement dans les couches techniques**. La réversibilité *de droit*, assortie de clauses juridiques illusoires si l'architecture reste captive, peut être dépassée par une ingénierie de sortie garantissant la portabilité technique *de fait*, appuyée par des plans de sortie chiffrés et des lignes rouges financières fixées avant la signature des contrats. Face aux mutations des modèles commerciaux (ESN vendant des résultats outillés, fournisseurs cloud intégrant des IA, éditeurs opérant des agents autonomes), la fonction numérique doit pouvoir opposer un rapport de forces contractuel pour endiguer l'inflation des coûts et sécuriser la création et la capture de valeur. Selon les stratégies et les moyens alloués, cette fermeté peut passer par une redescente progressive et ciblée dans les couches techniques, pour regagner en autonomie capacitaire *via* le *System Design*.
- **Maîtriser financièrement le TCO et responsabiliser les métiers sur le plan budgétaire**, par une extension de l'optimisation des factures cloud vers un FinOps AI. L'intégration des coûts cachés de l'IA (*tokenomics*) pourrait devenir un facteur clé pour éclairer les arbitrages *make or buy* au prisme des besoins réels et des volumes d'usage. En complément de dispositifs d'innovation et d'intrapreneurs robustes, la refacturation interne « au réel » des directions métiers pourrait les responsabiliser sur leurs consommations et garantir un usage efficient des ressources (réservation des modèles les plus coûteux aux cas d'usage à forte valeur ajoutée).

À l'horizon 2040, le pilotage contractuel, la rigueur d'ingénierie et la manoeuvrabilité économique s'imposeront comme les garants indispensables de la soutenabilité financière, de l'agilité budgétaire et de la liberté d'action des organisations face à la volatilité des marchés technologiques.

« D'ici 2040, la conjonction de crises géopolitiques rendra les stratégies d'autonomie technologique indispensables. »

Principe d'action 7. Gestion par les risques et garantie de la continuité d'activité

L'aggravation des tensions géopolitiques et la multiplication des conflits internationaux imposent aux organisations d'affronter l'enchaînement, la concomitance et la superposition de chocs majeurs (guerres conventionnelles et hybrides, cyberattaques étatiques et ingérences cognitives, crises logistiques, énergétiques, sanitaires). Le numérique étant devenu aussi bien le théâtre que le moyen d'affrontement entre États, la puissance qui lui est associée dépasse le cadre des opérations support et fait de la continuité d'activité un actif stratégique. L'intégration des risques géopolitiques au plus haut niveau de la gouvernance doit permettre de bâtir une résilience globale transformant les dépendances critiques subies en interdépendances choisies et maîtrisées.

Recommandations

- **Mettre en place une gestion des vulnérabilités géopolitiques centrée sur les maillons faibles (SPOF) et l'exigence de preuves tangibles de continuité d'activité.** Ce levier repose sur l'évaluation dynamique des risques de rupture liés aux tensions internationales (accès aux services critiques ou à leurs sous-jacents matériels, exploitation et mise à jour des logiciels, gestion des codes sources ou stockage et traitement des données par des fournisseurs étrangers). Outre la cartographie des vulnérabilités et l'approche *multi-sourcing*, les organisations pourraient imposer à leurs partenaires des tests de résilience en conditions réelles, sur site, et des mécanismes de réversibilité opérationnelle activables en cas de crise majeure.
- **Augmenter la maîtrise capacitaire par l'entraînement au mode dégradé et l'action collective.** Pour se prémunir contre les décisions unilatérales d'États ou le verrouillage indirect par des fournisseurs étrangers, les directions numériques gagneraient à coupler leur modularité technique à une préparation au fonctionnement en mode dégradé durable. Cette autonomie opérationnelle pourrait s'adosser à une participation aux coalitions françaises et européennes, garantissant de manière cohérente et ciblée la liberté de décision et le maintien des activités prioritaires lors de déstabilisations internationales sous le seuil de la conflictualité ouverte.
- **Se préparer aux crises en entraînant les instances de gouvernance.** La préparation conjointe du triptyque Conseil d'administration, Comité Exécutif et Direction numérique, permettrait un alignement au plus haut niveau de décision sur les enjeux stratégiques, psychologiques, communicationnels et opérationnels des crises hybrides. Une cellule de risques prospectifs pourrait également être dédiée à la modélisation des ruptures en cascade, avec analyses d'impact métier (*Business Impact Analysis*). L'identification des interdépendances entre plans de continuité et l'étude des corrélations de vulnérabilité inter-filiales, permettrait de hiérarchiser les scénarios d'attaques, tout en érigeant le facteur humain en rempart stratégique face au *continuum* de la menace (cyberattaques, désinformation et guerre cognitive).

À l'horizon 2040, le pilotage par les risques géopolitiques et l'anticipation des crises pourraient devenir essentiels pour garantir l'autonomie et la résilience des organisations dans un monde instable.

Principe d'action 8. Mutualisation des moyens de défense et alliances de confiance

Dans un contexte mondial marqué par le rapport de force, la désinstitutionnalisation des alliances et la vision transactionnelle des relations internationales, la sécurité numérique apparaît comme un domaine d'exercice privilégié de la souveraineté des États, en miroir de la sécurité physique. Face à la décomplexion des offensives étatiques, la capacité régaliennne de protection de l'ensemble du tissu social se trouve contrainte par l'urgence opérationnelle. L'ampleur des investissements nécessaires au développement de capacités de défense ne peut être supportée par les seuls acteurs publics et ne peut tenir de la seule responsabilité des entreprises. Le besoin d'autonomie exige de structurer des coalitions réunissant entreprises, opérateurs d'infrastructures critiques, administrations et académiques.

Recommandations

- **Mutualiser les capacités d'anticipation et de défense et l'organisation d'exercices de crise inter-organisations.** Pour réduire l'asymétrie face aux attaques sophistiquées et enrichies à l'IA, les organisations doivent travailler à ériger un bouclier défensif collectif. Cette mutualisation pourrait passer par l'amélioration de l'interconnexion des CERT, la transformation du signal faible de crise en une alerte stratégique pour dirigeant, le co-développement de modèles d'IA spécialisés à certains cas d'usage de sécurité numérique ou encore l'entraînement aux crises systémiques intra-sectorielles ou inter-OIV/OSE, incluant les ministères de tutelle.
- **Co-construire des communs technologiques et une action juridique collective face aux pressions extérieures.** L'investissement conjoint dans des fondations neutres et des architectures *open source* permettrait de garantir la continuité des approvisionnements indépendamment des embargos, sanctions ou politiques d'exportation d'États tiers. Une marge de manœuvre pourrait être dégagée par l'organisation d'une force de frappe juridique B2B mutualisée (« *sueing machine* »). L'union des moyens et des expériences en contentieux dissuaderait certaines pratiques contractuelles abusives induites par le contexte géopolitique, et opposerait une résistance collective aux injonctions extraterritoriales sans suspendre les actifs stratégiques à la seule application du droit de la concurrence français et européen.
- **Valoriser un marché européen dit de la « *sovereignty* » et encourager la création de normes européennes pour la confiance numérique.** La multiplication des exigences réglementaires (NIS2, DORA, CADA, CSA2, CRA, IA Act notamment) doit pouvoir être convertie en un levier d'entraînement, en complément d'incitations fiscales, pour favoriser la résilience européenne. Les donneurs d'ordres des entités importantes et essentielles devraient pouvoir flécher les achats vers des acteurs locaux, *via* un dispositif de préférence européenne pragmatique (*Buy European Act* proposé par [Eurostack](#)). En parallèle, les acteurs économiques doivent obtenir des pouvoirs publics une harmonisation et une simplification des référentiels, pour lever les contradictions normatives, obtenir des critères d'immunité extraterritoriale opérants et responsabiliser les tiers en cascade, pour une conception et une configuration native de la sécurité de leurs solutions.

À l'horizon 2040, la capacité à faire écosystème, à coproduire la sécurité numérique et à animer des alliances de confiance modulaires pourrait constituer le fondement de la pérennité stratégique des organisations.

« D'ici 2040, les arbitrages technologiques devront intégrer des critères discriminants en matière d'accès aux ressources et d'impact environnemental. »

Principe d'action 9. Anticipation des tensions sur les accès aux ressources critiques

Dans un contexte d'exacerbation des contraintes énergétiques et de plus grande imprévisibilité climatique (canicules, inondations, stress hydrique, feux, tempêtes), la soutenabilité environnementale du numérique dépasse la seule démarche de responsabilité sociétale pour constituer un paramètre de viabilité opérationnelle à part entière. Face à l'explosion des besoins induits par les data centers dédiés au cloud et à l'IA (consommation électrique, refroidissement, métaux critiques), l'enjeu ne réside plus dans une course effrénée à la consommation, mais dans un arbitrage rigoureux entre utilité réelle, confort technologique, performance et accès stable aux ressources critiques.

Recommandations

- **Mettre en place une gouvernance de l'IA en faveur d'un usage raisonné, et pilotée par un Indice de robustesse.** Pour rompre avec la logique de surconsommation de ressources, les déploiements technologiques pourraient être soumis à un filtrage strict fondé sur le juste besoin et l'utilité réelle. L'adoption d'un Indice de robustesse permettrait d'évaluer la contribution métier et le ROI complet sous un double angle *FinOps* et *GreenOps*. En renforçant le dialogue avec les métiers et en appliquant un référentiel d'éco-conception partagé avec les fournisseurs, les organisations pourraient orienter l'innovation (ultrapersonnalisation, interfaces conversationnelles, agents autonomes) vers un modèle créateur de valeur signifiante et plus sobre.
- **Adapter les architectures techniques et optimiser l'implantation territoriale des infrastructures, face aux contraintes foncières et énergétiques.** Les directions numériques gagneraient à évaluer l'exposition physique de leurs sites et de leurs prestataires. Ce pilotage pourrait s'appuyer sur des *stress-tests* et l'expérimentation en conditions réelles des plans de continuité face à des scénarios de rupture majeure (accès à l'eau, crise électrique, perte de site), tout en inscrivant l'empreinte foncière dans une logique de circularité (valorisation de la chaleur fatale, reconversion de friches et respect du Zéro Artificialisation Nette).
- **Co-construire un cadre réglementaire pour réguler les barrières d'accès aux ressources.** Face à la convergence des exigences européennes (directives CER, NIS2, CSRD) et au risque d'accaparement de l'énergie décarbonée, les organisations auraient intérêt à dépasser la conformité subie pour devenir architectes du cadre opérationnel et s'assurer des garanties d'exploitation en période de crise. L'établissement d'un dialogue entre acteurs économiques et pouvoirs publics permettrait de planifier l'attribution des capacités de calcul et d'énergie sur le territoire, prévenant ainsi les rentes par préemption et les ruptures d'attribution. Ce cadre concerté transformerait les contraintes de sobriété en un levier d'attractivité et de politique industrielle, réalignant le progrès numérique sur sa contribution au bien-être social et à l'économie réelle.

À l'horizon 2040, l'anticipation des tensions sur les ressources, en dialogue avec les pouvoirs publics, et l'intégration des critères de soutenabilité dans la gouvernance numérique représenteront des conditions essentielles pour une performance légitime et résiliente.

Principe d'action 10. Optimisation de la soutenabilité matérielle des modèles d'affaires

La pénurie de semi-conducteurs et l'envolée des prix des composants obligent les organisations à repenser leurs stratégies d'achat et de renouvellement de leur matériel informatique. Sous l'effet de la compétition pour les capacités de production, de l'effet d'éviction de la mémoire standard au profit des puces IA et des tensions sur les métaux critiques, la dépendance matérielle devient un risque financier et opérationnel majeur. Face au renouvellement forcé des parcs induit par l'inflation logicielle et aux besoins croissants d'autres industries comme l'automobile, les organisations ne peuvent plus considérer la gestion des équipements comme un simple achat récurrent. Alignant vision stratégique et passage à l'échelle, la fonction numérique aurait intérêt à faire de l'économie circulaire et de la sobriété matérielle les piliers de la résilience de son organisation.

Recommandations

- **Privilégier la commande responsable et diversifier les architectures processeurs.** Faute de pouvoir agir directement sur la production des semi-conducteurs, les directions numériques pourraient orienter leurs achats vers l'éco-conception, plus pérenne. La diversification des familles d'architectures matérielles (x86, ARM, architectures ouvertes type RISC-V) permettrait également de contourner ce goulot d'étranglement. La spécification fine des besoins réels permettrait, enfin, d'éviter le surdimensionnement et de contourner la compétition intersectorielle sur les composants passifs.
- **Étendre méthodiquement les cycles de vie physiques et le remplacement de composants.** Face à l'explosion des coûts d'acquisition et aux risques de pénurie sur les serveurs et PC haut de gamme, la soutenabilité des modèles d'affaires exige de faire de la réparabilité, de la modularité et du reconditionnement des priorités d'exploitation. Les directions numériques gagneraient à systématiser la mise à niveau ciblée des composants (extension de mémoire, remplacement modulaire) et à nouer des partenariats avec des acteurs du réemploi. L'allongement proactif de la durée de vie des actifs physiques, couplé à la constitution de stocks de réserve stratégiques, permettrait de préserver la capacité opérationnelle, tout en lissant les investissements matériels (CAPEX).
- **Rechercher la frugalité applicative comme bouclier contre l'obsolescence matérielle forcée.** L'optimisation de la couche matérielle exige de maîtriser les couches hautes pour éviter qu'un logiciel gourmand ne rende inefficace une infrastructure existante. Pour rompre ce cercle vicieux, les directions numériques auraient intérêt à favoriser la frugalité dans le choix des solutions, le recours à des modèles d'IA spécialisés et sobres (SLM, *open source*). En ajoutant l'acculturation des collaborateurs à l'auto-régulation des usages, cette gouvernance garantirait la soutenabilité financière et la continuité opérationnelle des systèmes déployés.

À l'horizon 2040, la soutenabilité matérielle, articulée autour d'achats responsables, de remplacement des composants et d'arbitrages applicatifs, pourrait accompagner la compétitivité des organisations, en garantissant la soutenabilité financière des systèmes numériques face aux chocs d'approvisionnement.

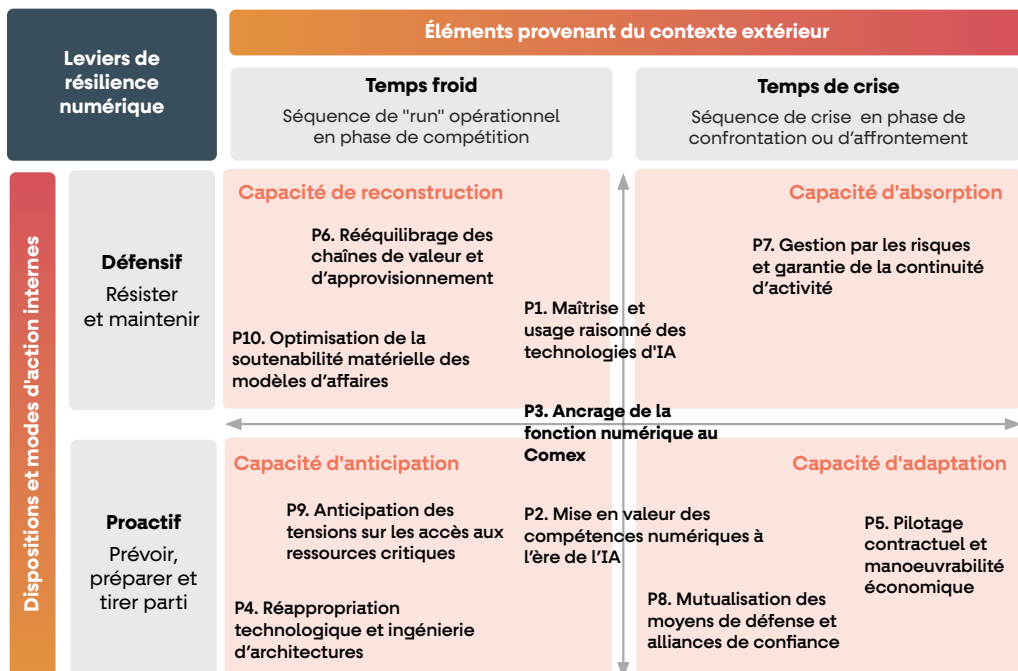
Matrice de positionnement des principes d'action stratégique

Pour faciliter les arbitrages et le pilotage par les risques au niveau stratégique, la matrice ci-dessous positionne les 10 principes d'action au croisement des deux axes fondamentaux de la résilience numérique :

- **Le contexte extérieur**, qui met en regard le temps froid (séquence de compétition, en activité normale) et le temps de crise (séquence de confrontation ou d'affrontement) ;
- **Les dispositions internes de l'organisation**, qui articulent la posture défensive (résister et maintenir les actifs) avec la posture proactive (prévoir, préparer et tirer parti).

Cette grille d'analyse permet de positionner chaque principe au cœur de l'une des **quatre capacités dynamiques** de l'organisation : l'anticipation, l'absorption, l'adaptation et la reconstruction.

En position centrale, les principes P1 (Maîtrise de l'IA), P2 (Compétences) et P3 (Ancrage Comex) constituent le pivot de gouvernance transversal. Ils incarnent la colonne vertébrale stratégique et humaine indispensable pour orchestrer le passage du *run* opérationnel à la gestion des perturbations.





Scénario 01

Formation d'un bloc multi régional de coalitions entre puissances moyennes

Principe d'action 1
Mise en valeur des compétences numériques à l'ère de l'IA

Partenariats entre parcours de formation (*upskilling* et *reskilling*) et fluidification de la mobilité des talents au sein du bloc multi-régional. Harmonisation des certifications et des fiches métiers de l'IA, pour une *Hybrid Workforce* au service des hommes et de l'économie réelle.

Principe d'action 2
Maîtrise et usage raisonné de l'IA

Conception d'architectures modulaires et ouvertes à l'échelle du bloc. Structuration rigoureuse des bases de données internes pour garantir la réversibilité et l'interopérabilité des agents autonomes.

Principe d'action 3
Réappropriation technologique et ingénierie d'architectures

Déploiement d'IA nativement interopérables (protocoles ouverts type MCP, UCP et *Guardrails* communs) et conformes aux standards de transparence, d'explicabilité et de traçabilité des données (*watermarking*) édictés par les coalitions régionales.

Principe d'action 4
Ancrage de la fonction numérique au Comex

Positionnement du CIO au Comex en copilote stratégique de la résilience. Acculturation des différentes instances de gouvernance aux enjeux numériques via un « passeport numérique » pour piloter la valeur de manière transversale et différenciante.

Principe d'action 5
Pilotage contractuel et manoeuvrabilité économique

Structuration d'un cadran d'aide à la décision stratégique à l'échelle du bloc et qualification de la résilience via un Indice de Résilience Numérique. Séquençage des engagements et pilotage proactif des arbitrages *make or buy* au sein d'un marché régional régulé.

Principe d'action 6
Rééquilibrage des chaînes de valeur et d'approvisionnement

Orientation stratégique de la commande privée et co-développement régional de briques pré-concurrentielles neutres (*open source*). Ancrage territorial des compétences pour consolider l'offre industrielle au sein du bloc.

Principe d'action 7
Gestion par les risques et garantie de la continuité d'activité

Participation active aux coalitions et réseaux de partage d'informations stratégiques du bloc (ex. PIIEC). Évaluation dynamique des vulnérabilités géopolitiques et alignement des instances décisionnelles sur un cadre de résilience partagé.

Principe d'action 8
Mutualisation des moyens de défense et alliances de confiance

Valorisation d'un marché régional de la "sovereignty" appuyé sur un alignement normatif (ex. NIS2, DORA) et un *Buy European Act*. Investissement dans des fondations neutres et architectures open source à l'échelle de la coalition.

Principe d'action 9
Anticipation des tensions sur les accès aux ressources critiques

Co-construction d'un cadre réglementaire régional et planification concertée de l'attribution de l'énergie et des capacités de calcul avec les pouvoirs publics du bloc, prévenant les rentes par préemption.

Principe d'action 10
Optimisation de la soutenabilité matérielle des modèles d'affaires

Commande publique et privée responsable orientée vers les architectures ouvertes (RISC-V, ARM) et l'éco-conception à l'échelle régionale pour contourner les monopoles de production de puces.

Scénario 02 Archipélisation des partenariats public-privé

Principe d'action 1
Mise en valeur
des compétences
numériques à l'ère de l'IA

Création de chaires industrielles et de parcours de formation co-construits entre entreprises, organismes de recherche et acteurs publics pour pallier les tensions chroniques sur les compétences clés.

Principe d'action 2
Maîtrise et usage raisonné
de l'IA

Co-développement de modèles d'IA *ad hoc* et déclinaison aux besoins sectoriels. Réinternalisation d'actifs et intégration verticale ciblées. Endiguement du *Shadow AI* par des politiques d'accès IAM et de gouvernance négociées au sein d'îlots de confiance.

Principe d'action 3
Réappropriation
technologique et
ingénierie d'architectures

Création de pôles d'excellence internes ou d'entités dédiées à l'automatisation transversale. Valorisation des processus métiers spécifiques et des données propriétaires au sein de consortiums et de plateformes mutualisées.

Principe d'action 4
Ancrage de la fonction
numérique au Comex

Posture de facilitateur d'affaires et « diplomate technologique » de la fonction numérique au Comex. Partage de la gouvernance des risques (DAF, DRH, Juridique) pour co-construire des alliances et adapter agilement le numérique aux besoins des archipels.

Principe d'action 5
Pilotage contractuel
et manoeuvrabilité
économique

Généralisation d'une « ingénierie de sortie » et d'une portabilité technique effective *via* des contrats modulaires à engagements courts (24-36 mois). Responsabilisation budgétaire des métiers (*FinOps*, refacturation au réel) adaptée aux alliances *ad hoc*.

Principe d'action 6
Rééquilibrage des
chaînes de valeur et
d'approvisionnement

Constitution de consortiums industriels et mutualisation de fonds (capital-risque, *private equity*) pour structurer l'offre régionale. Co-innovation ciblée pour sécuriser les approvisionnements en composants critiques.

Principe d'action 7
Gestion par les risques et
garantie de la continuité
d'activité

Co-construction de la résilience au sein d'îlots de confiance. Réalisation croisée de scénarios de perturbation en conditions réelles, intégration de mécanismes de secours communs et entraînement conjoint des gouvernances au fonctionnement en mode dégradé.

Principe d'action 8
Mutualisation des moyens
de défense et
alliances de confiance

Structuration « d'archipels de confiance » hybrides (entreprises, OIV/OSE, CERTs, organismes de recherche). Mutualisation des capacités d'anticipation, co-développement d'IA de sécurité et exercices de crise inter-organisations.

Principe d'action 9
Anticipation des tensions
sur les accès aux
ressources critiques

Négociation d'accords territoriaux d'optimisation des infrastructures (valorisation de la chaleur fatale, calcul différé sur énergie décarbonée). Évaluation de l'exposition physique *via* des stress-tests partagés.

Principe d'action 10
Optimisation de la
soutenabilité matérielle
des modèles d'affaires

Partenariats stratégiques territoriaux avec des acteurs du réemploi. Extension méthodique du cycle de vie des parcs matériels (reconditionnement, mise à niveau modulaire) et constitution de stocks de réserve.

Scénario 03

Colonisation numérique et techno-féodalisme

Principe d'action 1

Mise en valeur des compétences numériques à l'ère de l'IA

Exode des talents hautement qualifiés vers les géants de la tech qui captent la valeur. Risque d'appauvrissement économique et cognitif sur le long terme, pression sur les salaires et précarisation des rôles d'exécution.

Principe d'action 2

Maîtrise et usage raisonné de l'IA

Dépendance technologique subie face aux modèles propriétaires opaques imposés par les géants du secteur. Diversification partielle et forcée, face à la perte de contrôle sur les jeux de données d'entraînement et sur la réversibilité des flux opérationnels des IA.

Principe d'action 3

Réappropriation technologique et ingénierie d'architectures

Ingénierie sous forte contrainte. Tentatives de contournement des rentes d'interface et de l'inflation des coûts par du redéveloppement localisé sur les modules les plus critiques pour limiter la captivité.

Principe d'action 4

Ancrage de la fonction numérique au Comex

Posture défensive et sécuritaire de la fonction numérique au Comex, en tant que garant des arbitrages de dépendances face aux géants tech et de minimisation de la captivité tarifaire.

Principe d'action 5

Pilotage contractuel et manoeuvrabilité économique

Rapport de force contractuel défensif appuyé par la redescende dans le *System Design* pour endiguer l'inflation des dépenses et la captivité (*vendor lock-in*). Maîtrise financière du TCO et intégration de la tokenomics face aux rentes des monopoles.

Principe d'action 6

Rééquilibrage des chaînes de valeur et d'approvisionnement

Sanctuarisation des capacités d'ingénierie et réinternalisation de l'assemblage des briques applicatives stratégiques pour prévenir la désintermédiation forcée et l'absorption des chaînes de valeur par les géants privés.

Principe d'action 7

Gestion par les risques et garantie de la continuité d'activité

Cartographie interne des dépendances et maillons faibles face à l'asymétrie des géants de la tech. Développement autonome de la réversibilité technique et préparation au mode dégradé pour pallier les ruptures de service unilatérales.

Principe d'action 8

Mutualisation des moyens de défense et alliances de confiance

Réalisation d'actions juridiques et d'influence collectives (« *sueing machine* ») pour contrecarrer les pratiques contractuelles abusives, opposer une résistance aux injonctions extraterritoriales et faire appliquer le droit de la concurrence.

Principe d'action 9

Anticipation des tensions sur les accès aux ressources critiques

Filtrage des usages par un Indice de robustesse (ROI *FinOps*/ *GreenOps*) et arbitrage par les différentes composantes de la valeur créée pour minimiser l'impact des déploiements énergivores des géants de la tech.

Principe d'action 10

Optimisation de la soutenabilité matérielle des modèles d'affaires

Frugalité applicative et recours prioritaire aux modèles spécialisés sobres (SLM) comme boucliers d'auto-défense face à l'obsolescence matérielle forcée et à l'inflation logicielle imposées par les géants de la tech.

Scénario 04

Bipolarisation sino-américaine exclusive

Principe d'action 1
Mise en valeur
des compétences
numériques à l'ère de l'IA

Exacerbation de la compétition mondiale des talents en IA, par des restrictions administratives strictes selon les nationalités. Besoin de promouvoir une culture de l'esprit critique et du jugement humain pour maintenir une liberté d'arbitrage technologique.

Principe d'action 2
Maîtrise et usage raisonné
de l'IA

Alignement contraint de la pile technologique d'IA sur le bloc géopolitique d'appartenance. Tentative de sanctuarisation du patrimoine informationnel face au risque de restriction à l'export des superpuissances.

Principe d'action 3
Réappropriation
technologique et
ingénierie d'architectures

Piles technologiques imposées par le bloc géopolitique. L'ingénierie se réduit au cloisonnement défensif des systèmes et bases de données métiers pour parer les risques de rupture d'activité (*kill switch*).

Principe d'action 4
Ancrage de la fonction
numérique au Comex

Posture de gestion des risques et des crises de la fonction numérique au Comex. Forte coloration géopolitique des activités et attention portée à la continuité d'activité en mode dégradée.

Principe d'action 5
Pilotage contractuel
et manoeuvrabilité
économique

Diversification maximale des infrastructures (*multi-cloud, multi-AI, on-premise, edge*) et engagements courts pour obtenir la plus grande autonomie décisionnelle relative possible.

Principe d'action 6
Rééquilibrage des
chaînes de valeur et
d'approvisionnement

Conception d'architectures découplées et modularité de l'urbanisation du SI pour opérer de manière cloisonnée sur des plaques régionales étanches, sans subir de blocages à l'entrée ni de ruptures d'approvisionnement.

Principe d'action 7
Gestion par les risques et
garantie de la continuité
d'activité

Instauration d'une cellule de prospective géopolitique au Comex/CA pour modéliser les ruptures en cascade (*Business Impact Analysis*). Valorisation des PCA métiers face aux incidences des cyberattaques étatiques et à la guerre cognitive.

Principe d'action 8
Mutualisation des moyens
de défense et
alliances de confiance

Exposition totale au droit extraterritorial et aux sanctions unilatérales. La mutualisation se limite au maintien de briques *open source* de secours et à la sécurisation d'urgence des approvisionnements.

Principe d'action 9
Anticipation des tensions
sur les accès aux
ressources critiques

Arbitrage strict de l'utilité métier réelle face au rationnement étatique des ressources énergétiques et minérales. Généralisation d'arbitrages en faveur de l'efficacité *low-tech* pour garantir la viabilité opérationnelle.

Principe d'action 10
Optimisation de la
soutenabilité matérielle
des modèles d'affaires

Sobriété matérielle stricte et diversification des familles de processeurs pour sécuriser l'approvisionnement face au rationnement des composants et à la préemption des puces IA par les superpuissances.

Analyse prospective

Partie 3

Analyse prospective

Cette troisième partie propose une étude des cinq grands champs de transformation du numérique à l'horizon 2040.

Méthodologie

Cette troisième partie du rapport est construite selon les **principes de l'analyse prospective**, qui a pour objectif de distinguer, parmi la multitude de phénomènes à l'œuvre, ceux qui sont véritablement structurants pour l'avenir et ceux dont les perspectives sont plus ouvertes.

En tirant les enseignements des évolutions observées depuis 2020, l'analyse n'a retenu que les dynamiques d'avenir, sélectionnées selon leur impact et leur probabilité d'occurrence. Pour favoriser le format de synthèse, toutes les tendances n'ont pas fait l'objet d'une rédaction, certaines étant déjà détaillées dans les rapports précédents. Pour chacun des 5 champs thématiques, **quatre familles de transformations ont été distinguées** :

- **Des tendances lourdes**, dynamiques à fort impact et forte inertie, appelées à se pérenniser à l'horizon 2040. L'enjeu est d'en qualifier la portée pour permettre aux organisations d'en absorber les conséquences et de s'y adapter proactivement.
- **Des tendances émergentes**, phénomènes aujourd'hui émergents mais susceptibles de s'amplifier sous 15 ans. L'enjeu est d'en identifier les moteurs afin d'anticiper leurs opportunités et leur éventuelle mue en dynamiques structurantes.
- **Des incertitudes majeures**, interrogations dans les champs desquelles de multiples trajectoires sont possibles. L'enjeu est de dessiner les variables de ces incertitudes pour que les organisations puissent se forger une vision et des convictions pour y répondre.
- **Des hypothèses de rupture**, événements de probabilité plus faibles mais dont la survenue engendrerait un impact majeur. L'enjeu est de se plonger dans ces cas limites pour anticiper les risques de rupture, tout en se tenant prêt à en exploiter le potentiel positif.

Cette structuration permet aux organisations de mieux se repérer et de se préparer aux grandes transformations en cours et à venir. Par ailleurs, elle permet de disposer de matériaux solides pour la construction des scénarios (Partie 1) et l'identification des principes d'action (Partie 2).

Les 5 champs de transformation

Tendances lourdes et émergentes, incertitudes et hypothèses de rupture à l'horizon 2040

Champ 01 - **Économie du numérique**

Champ 02 - **Géopolitique du numérique**

Champ 03 - **Technologies et innovations**

Champ 04 - **Numérique responsable**

Champ 05 - **Travail et numérique**

Analyse
prospective

Champ

01

Économie du numérique



Tendances lourdes

Tendance lourde 1. Le marché de l'intelligence artificielle tend à se substituer à celui du logiciel et des ESN, tout en renforçant celui du cloud

Tendance lourde 2. Le périmètre des dépendances numériques s'élargit sous l'effet de l'absorption des infrastructures stratégiques par les géants du numérique

Tendance lourde 3. L'avènement du marché « *Business-to-Agent* » amorce une reconfiguration substantielle des modèles d'affaires et de la relation client

Tendance lourde 4. Les conséquences économiques des dépendances technologiques pèsent de plus en plus sur la compétitivité européenne

Tendances émergentes

Tendance émergente 1. De nouvelles alternatives numériques européennes, crédibles et à l'échelle, renforcent la résilience du continent

Tendance émergente 2. Le modèle de facturation IA « à l'usage » vient s'ajouter au modèle « à la licence » intensifiant l'opacité des tarifications technologiques

Tendance émergente 3. L'exploitabilité des données devient un critère de valorisation des entreprises

Incertitudes majeures

Incertitude 1. La « mise en données du monde » pourrait conduire à une captation croissante de la valeur par les fournisseurs d'IA

Incertitude 2. L'intégration croissante de l'IA dans les processus métiers interroge ses capacités réelles d'effet de levier sur la compétitivité à long-terme

Hypothèses de rupture

Hypothèse 1. Le décalage entre investissements, obsolescence technologique et revenus de l'IA provoque une crise financière

Hypothèse 2. L'aboutissement du marché unique des services numériques consacre l'émergence de champions européens sur certaines briques technologiques critiques

Tendance lourde 1. Le marché de l'intelligence artificielle tend à se substituer à celui du logiciel et des ESN, tout en renforçant celui du cloud

DE QUOI S'AGIT-IL ?

Les solutions d'intelligence artificielle permettent à présent de produire massivement des lignes de code. Malgré la possible volatilité des prix du *token* d'IA, cette capacité de redéveloppement en interne remet en question le coût total de possession de logiciel propriétaire et d'intégration par les entreprises de services numérique (ESN). D'une part, les arbitrages de « *make or buy* » qui prévalaient depuis près de 30 ans se trouvent réinterrogés. D'autre part, la proposition de valeur des éditeurs et ESN traditionnels doit se réinventer.

LES DYNAMIQUES À L'ŒUVRE

L'irruption d'agents autonomes connectés et le déploiement des protocoles MCP (*Model Context Protocol*) ont provoqué une telle contraction du marché des éditeurs, que Wall Street a inventé le terme de « *SaaSocalypse* ». La correction boursière de février 2026 a été historique, effaçant environ 285 milliards de dollars de capitalisation en 48 heures, à la suite des annonces d'Anthropic visant à enrichir son environnement *Claude Cowork*. Le mouvement baissier a touché des acteurs de place comme Salesforce (-12%), ServiceNow (-11%), Accenture (-8%), Capgemini (-7%) et même Microsoft, qui a perdu entre 360 et 450 milliards de dollars de capitalisation en un mois. La même chute a eu lieu pour les acteurs technologiques de la verticale juridique (-18% pour Thomson Reuters, -20% pour LegalZoom) lors de la sortie, début mai, de Claude for Legal.

La division par trois, en moyenne, des multiples de valorisation boursière des éditeurs et ESN s'explique par le déploiement d'IA capables, pour la première fois, d'exécuter des flux de travail complets de bout en bout en accédant instantanément, universellement et de manière standardisée aux bases de données, APIs et fichiers de l'entreprise, pour exécuter des requêtes ou actions. Cette évolution, tantôt qualifiée de « désintermédiation des fournisseurs », de « levée des barrières à l'entrée du marché technologique », de « fin de la tarification *jours-homme* pour les ESN » ou encore « d'effondrement du modèle d'abonnement SaaS par utilisateur (*per seat*) », a été interprétée par le marché comme une rupture structurelle. En ce sens, la chaîne de développement étant devenue aujourd'hui le « *golden use-case* », les IA génératives comme agentiques, ne sont plus envisagées comme des outils venant enrichir des logiciels existants mais elles tendent plutôt à se substituer aux logiciels eux-mêmes. Les éditeurs de progiciels et fournisseurs d'information professionnelle, jusqu'alors considérés comme les principaux bénéficiaires de l'avènement de l'IA, en viennent même à être, pour certains, en danger quasi-existential.

L'ingénierie logicielle semble entrer dans une phase d'industrialisation dans laquelle le rôle du développeur est appelé à évoluer de la production directe de code vers la validation, l'orchestration et la supervision de portefeuilles produits. Les entreprises les plus avancées dans ces usages, notamment à travers le *vibe coding* - qui permet de décrire à une IA, en langage naturel, l'objet à développer - ne visent plus des gains de productivité incrémentaux de 10 à 30 %¹. À chaque étape du SDLC (*Software Development Life Cycle*), ces organisations ambitionnent de bénéficier, à l'échelle d'un processus, d'une multiplication de sa productivité allant de deux jusqu'à dix, grâce à la « fluidification » des rythmes de production par les agents sur les segments clés des chaînes de valeur. Cette vélocité ne se traduit toutefois pas par une réduction immédiate de l'emploi technologique, le nombre de développeurs actifs ayant paradoxalement progressé de 13 % au premier trimestre 2026. Le gain de temps offert par l'automatisation n'est pas uniquement converti en réduction d'effectifs, mais permet aux organisations de lancer des chantiers techniques qu'elles n'auraient jamais pu imaginer auparavant.

PERSPECTIVES À L'HORIZON 2040

Alors que par la puissance des IA génératives spécialisées le code devient un matériau qualifié par certains de « jetable », la création de valeur pourrait se déplacer vers des actions plus abstraites de conception d'architectures robustes et explicables. À l'heure où le « contenu logiciel » devient moins différenciant, la mise en place et l'utilisation pérennes d'agents spécialisés et de boucles de travail automatisée (*workflow*) pourraient faire apparaître de nouvelles poches de valeur ajoutée. La capacité d'adaptation des gouvernances numériques deviendrait alors le chantier d'attention principal des organisations. L'enjeu serait de parvenir à piloter finement la maîtrise des architectures et le maintien en compétence, la sécurité du code et la gestion des accès, les clauses juridiques de responsabilité et d'utilisation des données d'entraînement, le contrôle de la qualité et de la propriété intellectuelle, la gestion des coûts et de la dette technique. Sans stratégie, cette tendance pourrait cependant engendrer un double « *lock-in* », vis à vis des modèles fondateurs (OpenAI, Anthropic, Google) et vis à vis des acteurs du cloud qui disposent des capacités massives en calcul, stockage et réseaux nécessaires au passage à l'échelle de l'agentique.

D'ici 2040, l'industrie du logiciel pourrait subir les conséquences d'un déclassé définitif des actuelles solutions SaaS, vouées à devenir l'équivalent fonctionnel du « *mainframe* », c'est-à-dire de simples systèmes d'enregistrement confinés dans les « couches basses » de la pile numérique. L'IA agentique pourrait supplanter le SaaS en tant que nouvelle couche applicative à forte valeur ajoutée, dialoguant en direct avec les bases de données pour orchestrer l'ensemble de la chaîne de valeur. Un écosystème applicatif plus ouvert, distribué, interopérable et *de facto* orienté *open source* pourrait émerger de la brèche ouverte par les protocoles MCP, sans pour autant s'affranchir, par ailleurs, des enclaves propriétaires fortement intégrées au cloud.

Pour réaliser la rotation de leurs modèles d'affaires, les ESN pourraient recentrer leurs activités sur la gestion du changement et des risques (interaction homme-machine, délégation de responsabilité, audit et certification des systèmes autonomes, maîtrise des boucles de rétroaction etc.). Ces acteurs pourraient également se transformer en fournisseurs d'agents, c'est-à-dire en vendeurs d'actifs d'IA spécialisées capables de produire des gains de productivité tangibles et globaux, et plus seulement locaux et diffus.

¹ Rupture structurelle dans l'ingénierie logicielle avec l'IA générative et l'arrivée de l'IA agentique : travaux du Do Tank Cast & Cigref, Cigref, 3 février 2026.

Tendance lourde 2. Le périmètre des dépendances numériques s'élargit sous l'effet de l'absorption des infrastructures stratégiques par les géants du numérique

DE QUOI S'AGIT-IL ?

La vague d'investissements et d'emprunts destinés à financer les infrastructures du seul secteur numérique témoigne d'une intensité capitalistique digne de la première révolution industrielle par sa contribution au PIB mondial. La singularité tient surtout à la concentration de ces investissements entre les mains d'une dizaine d'acteurs privés, dont les capacités financières et industrielles rivalisent désormais avec celles de nombreux États. Leurs investissements s'étendent bien au-delà des seules infrastructures de calcul et de stockage, pour englober l'approvisionnement en énergie décarbonée, les réseaux optiques, les constellations satellitaires ou encore les chaînes logistiques nécessaires à leur fonctionnement. En ce sens, les géants du numérique étendent massivement leur emprise sur les couches physiques et captent des positions structurantes et stratégiques dans l'économie réelle. Cette dynamique élargit le périmètre des dépendances numériques, en transformant des infrastructures, autrefois publiques ou mutualisées pour la plupart, en actifs privés intégrés à des stratégies globales.

LES DYNAMIQUES À L'ŒUVRE

Le retour de l'hyper-capex marque une rupture d'échelle pour les modèles d'affaires des fournisseurs de solutions et produits numériques. Pour la seule année 2026, les principaux acteurs américains annoncent 725 Mds\$ d'investissements (Amazon 200 Mds\$, Microsoft 190 Mds\$, Google 190 Mds\$, Meta 145 Mds\$), auxquels s'ajoutent 662 Mds\$ d'engagements hors-bilan pour la location future de capacités de calcul, portant l'effort total à près de 1400 Mds\$. Le foisonnement et l'accélération des projets en IA sont tels que les montants doivent être financés pour plus de la moitié par de la dette ou de l'augmentation de capital. Le seul exemple du conglomérat Alphabet suffit à faire comprendre cette tendance de manière archétypale. Son émission de dettes, déjà inédite, début 2026, n'a pas suffi à couvrir ses annonces d'investissements pour les deux années à venir (500 Mds\$). Pendant près de dix ans l'entreprise disposait de liquidités considérables, après réinvestissement. Ce *free cash-flow* servait, d'une part, à obtenir des licences sur les technologies d'acteurs d'infrastructure alternatifs, en siphonnant leurs talents et leur propriété intellectuelle sans déclencher d'alertes auprès des autorités de la concurrence. D'autre part, il permettait de racheter les propres actions du groupe afin d'en bonifier la valeur pour ses actionnaires. Cette année, Alphabet s'est vu dans l'obligation de capter les liquidités du marché privé, en créant des actions pour 85 Mds\$, dans le but de financer son projet de construction d'une chaîne de valeur complète. Cette stratégie va de l'innovation sur les puces propriétaires (TPU v6, alternatives aux GPU Nvidia) aux canaux de distribution (environnement Google intégré, ou plateforme Hugging Face rachetée par Nvidia en tant que carrefour mondial des modèles *open source*), en passant par les câbles sous-marins et corridors de données (*Marea et Sol, Nuvem*), les centrales énergétiques (réacteurs à sels fondus de *Kairos Power, Power Purchase Agreements* combinant nucléaire SMR et stockage par batteries longue durée) et les modèles de pointe (Gemini et DeepMind).

Au-delà des stratégies d'intégration verticale des géants du numérique, la concentration inouïe des investissements de ces acteurs crée un choc de demande qui sature les chaînes d'approvisionnement mondiales. En témoigne la réorganisation brutale du marché des semi-conducteurs et l'effet d'éviction induit par les fondeurs de puces électroniques qui, pour répondre à la demande massive de l'IA, dédient prioritairement leurs lignes de production à la mémoire IA (HBM) à très forte marge. Ce choix sacrifie mécaniquement les volumes de mémoire RAM standard, provoquant une pénurie structurelle et une inflation de +40 % à +60 % en un an. Cette asymétrie de marché, pilotée par les besoins capacitaires d'une poignée de géants fragilise et appauvrit l'ensemble de la chaîne de valeur numérique des organisations européennes.

PERSPECTIVES À L'HORIZON 2040

Dans la continuité de la cloudification du numérique, la course à l'innovation devrait être de plus en plus contrainte par le coût d'accès à la puissance de calcul. L'accès à l'énergie et la maîtrise de la latence¹ devenant deux critères déterminants, certains acteurs pourraient délaisser les stratégies d'intégration horizontale², les effets de réseau et la plateformes, au profit de modèles d'intégration verticale « *full-stack* », visant à maîtriser une part croissante de la chaîne de valeur technologique. La guerre économique qui s'engage devrait conduire les principaux géants du numérique à remonter les chaînes de valeur pour en contrôler les points clés, verrouiller les marges et positions, tout en réduisant les dépendances critiques à d'autres fournisseurs. Le périmètre physique des dépendances pourrait alors représenter un tel avantage compétitif que l'Autorité de la concurrence française a déjà exprimé son inquiétude en raison du « *devenir énergéticien des grands acteurs du numérique étrangers* » qui pourrait conduire à une OPA technologique sur les infrastructures stratégiques et l'économie réelle. Le régulateur pointe en effet un risque systémique : équipés de systèmes de stockage par batteries colossaux, ces centres de données pourraient réinjecter de l'électricité lors des baisses de production (mécanisme d'effacement), se positionnant ainsi comme des acteurs à part entière du réseau électrique. De surcroît, les investissements massifs consentis par certains conglomérats mondiaux confirment que la course à la puissance capacitaire dicte la captation des ressources nucléaires décarbonées des États. L'annonce lors de Choose France 2026, par SoftBank et Schneider Electric, d'un projet d'installation d'*AI factories* à hauteur de 75 milliards d'euros sur le port français de Dunkerque illustre bien cette perspective. Si la valeur ajoutée des modèles d'IA demeure extra-européenne, le risque est de réduire les territoires européens au rang de simples sous-traitants énergétiques.

¹ Capacité à faire tourner les *clusters* de centre de données près des zones de consommation.

² Stratégie visant l'accroissement des parts de marché et les économies d'échelle par rachat d'un concurrent, comme Facebook rachetant Instagram et Whatsapp.

Tendance lourde 3. L'avènement du marché « *Business-to-Agent* » amorce une reconfiguration substantielle des modèles d'affaires et de la relation client

DE QUOI S'AGIT-IL ?

La structuration d'un marché « *Business-to-Agent* » (B2A) ou B2A2C a toutes les chances d'incarner une reconfiguration commerciale au moins aussi fondamentale que l'accès à l'information par *Google Search* ou la réservation d'hôtel par Booking. La relation client se trouve transformée par les nouveaux usages des consommateurs, qui recourent de plus en plus aux IA pour l'éclairage ou l'exécution de leurs actes d'achat. Dans cette logique, de nombreuses organisations ne parlent plus directement à leurs clients mais interagissent avec des agents qui parlent aux clients. Cette transition s'accompagne d'une plateformesation menée par une poignée d'acteurs technologiques globaux, faisant peser sur l'économie réelle un risque inédit de désintermédiation et de captation de la rente relationnelle et publicitaire.

LES DYNAMIQUES À L'ŒUVRE

L'avènement du commerce agentique se traduit par le déploiement de la *Generative Engine Optimization* (GEO), qui supprime peu à peu les mécaniques du référencement qui prévalaient depuis 10 ans avec le SEO. Avec l'introduction de formats publicitaires génératifs au sein d'environnements conversationnels (comme le *AI Mode* de Google), le moteur de la visibilité se transforme. La publicité n'est plus un « espace acheté » à côté de la réponse mais devient une composante de la réponse elle-même. L'IA capte l'attention, reformule le besoin, choisit le moment et arbitre l'exposition. L'entreprise fournit la matière première par son contenu numérique, tandis que la machine compose. Être visible demain ne devrait plus signifier seulement apparaître, mais « être choisi » par un système qui résume, classe, recommande et vend, sans que l'utilisateur ne quitte jamais l'interface. Tout indique que pour le e-commerce, les organisations ne parleront plus directement à leurs clients mais parleront à l'agent qui parlera au client. L'avis de l'Autorité de la concurrence alerte précisément sur ce « devenir orchestrateur » des agents, alors que trois acteurs (OpenAI, Google, Anthropic) contrôlent déjà plus de 84 % du marché et que leur « plateformesation » présente des risques élevés de désintermédiation brutale, de discrimination des offres et d'opacité des critères de visibilité. Le régulateur craint que l'automatisation des achats par le commerce agentique ne cristallise le secteur autour d'acteurs déjà verticalement intégrés, privant le consommateur final de tout choix éclairé.

Parallèlement, les organisations font face au défi technique d'entrer en relation avec les assistants personnels des clients. Pour contrer ce monopole des interfaces, des initiatives émergent pour structurer des protocoles d'échange universels, qui vont dans le sens des recommandations émises par le régulateur de la concurrence, prônant l'interopérabilité et les standards ouverts. C'est en partie le sens des expérimentations menées par des acteurs comme Carrefour autour de l'UCP (*Universal Commercial Protocol*), visant à standardiser la grammaire sémantique et commerciale permettant à une IA tierce de converser de manière sécurisée et fluide avec les systèmes de l'entreprise (L'usine digitale).

Cette tendance interroge les processus de création et de capture de la valeur tout autant que la nature des données que les organisations souhaiteront transférer à des tiers dans le but de conserver des positions fonctionnelles. Or, la délégation de la relation client à une machine autonome pose un risque juridico-financier inédit : le précédent fixé en 2024 par la justice canadienne, contraignant Air Canada à honorer une politique de remboursement inventée de toutes pièces par son chatbot ([Le Monde Informatique](#)), confirme que la responsabilité légale incombe à l'entreprise qui déploie l'agent, et non à l'éditeur technologique. La supervision de ces systèmes devient un enjeu critique de conformité. L'industrie bascule vers une exigence stricte de cybersécurité et d'auditabilité, à l'image des protocoles de type NemoClaw imposant une isolation des agents (droits, flux réseaux, traçabilité), car l'autonomie sans garde-fous constitue une exposition technologique majeure. C'est à cette intersection que se joue la mutation fondamentale de la fiabilité et de la valeur de la donnée. À l'échelle macroscopique, le web public, inondé de contenus synthétiques dégradés (*AI slop*), expose les modèles à un risque d'effondrement autophage (*Model Autophagy Disorder*). À l'échelle opérationnelle des organisations, cette même entropie frappe la délégation du travail à l'IA : l'étude *DELEGATE-52* révèle que lors de flux de travail prolongés (comme le *vibe coding*), les modèles actuels se révèlent inconstants, corrompant en moyenne 25 % du contenu des documents au fil des itérations. Face à cette double dégradation externe et interne, la confiance absolue dans l'autonomie agentique constitue une faille sécuritaire. L'enjeu économique bascule alors logiquement vers le *data streaming*, avec une prime absolue à la donnée « fraîche ». Pour garantir l'exactitude des actes d'achat, les agents devraient donc être en capacité d'interroger en temps réel des bases de données B2B spécifiques, lisibles, fiables et à jour.

PERSPECTIVES À L'HORIZON 2040

Les IA agentiques pourraient s'imposer comme canal principal d'accès des individus à l'ensemble des services numériques (accès à l'information, plateformes, achats). Le web et le marché numérique pourraient alors se reconfigurer au gré d'une domination nouvelle entretenue par les labos d'IA et leurs modèles, d'une part, et les plateformes capables de faire converger les différentes parties prenantes, de l'autre. Les plateformes e-commerce et les portails traditionnels risqueraient de tomber au rang de simples systèmes d'enregistrement (*Systems of record*) interrogés en tâche de fond par les algorithmes. Le dilemme stratégique des entreprises pourrait s'intensifier : soit accepter une vassalisation fonctionnelle et devenir un fournisseur en marque blanche interchangeable, soumis aux règles d'arbitrage opaque des *hyperscalers* ; soit réussir à imposer une couche servicielle propriétaire et hybride. La création et la capture de la valeur se traduiraient alors plutôt par la capacité à enrichir l'expérience client par des données exclusives et dynamiques que l'IA personnelle de l'utilisateur pourrait interroger de manière sécurisée, sans exfiltration définitive de la propriété intellectuelle de la marque.

Tendance lourde 4. Les conséquences économiques des dépendances technologiques pèsent de plus en plus sur la compétitivité européenne

DE QUOI S'AGIT-IL ?

La transformation numérique de l'économie européenne, initialement perçue comme une opportunité de compétitivité et un moyen de se maintenir dans la course à la productivité mondiale, se heurte à la réalité macroéconomique critique d'une captation massive de valeur par les acteurs extra-européens. Ce déséquilibre structurel se traduit par un basculement massif des budgets informatiques d'une logique d'investissement (CAPEX) vers une logique de coûts d'exploitation récurrents (OPEX). Les hausses tarifaires unilatérales s'apparentent désormais à un véritable « impôt technologique » mutualisé, finançant les infrastructures de calcul des géants américains au détriment direct de l'autonomie et de la rentabilité des entreprises européennes.

LES DYNAMIQUES À L'ŒUVRE

Le manque structurel de concurrence sur le marché du cloud-logiciel confère aux éditeurs un pouvoir de marché considérable. Alors que les organisations européennes consacrent environ 400 milliards d'euros par an aux services cloud et logiciels, 83 % de ce marché est capté par un nombre restreint de fournisseurs américains, et 80 % de la valeur créée (soit 264 Md€) bénéficie directement à l'économie d'outre-Atlantique ([Etude Cigref x Asterès 2025](#)). L'irruption de l'intelligence artificielle amplifie cette dynamique d'asymétrie commerciale. Prisonnières de mécanismes complexes de *vendor lock-in* (dont les coûts de sortie techniques et commerciaux sont évalués à 15 % du budget IT) et de pratiques de ventes groupées (*bundling*, *IA-by-design*), les entreprises européennes subissent une sur-inflation déconnectée des coûts réels des solutions numériques et des gains induits. Les hausses de tarifs constatées atteignent en moyenne 8,7 % par an sur les trois dernières années ([Etude Cigref x Asterès 2026](#)) et les directions numériques interrogées anticipent une accélération majeure à +12 % par an sur les cinq prochaines années, soit un rythme largement supérieur à l'inflation de référence du secteur logiciel (2,4 %). L'intégration de l'IA fait office de « nouvelle frontière commerciale » pour justifier des grilles tarifaires opaques ou des basculements vers une facturation à la consommation de jetons (*tokens*).

Cette trajectoire inflationniste génère un effet d'éviction délétère à l'échelle européenne. Pour absorber un surcoût annuel moyen estimé à 140 milliards d'euros (dont 93 milliards sortent définitivement de l'économie européenne), les organisations sacrifient leurs propres dépenses d'avenir. Ainsi, les organisations contraintes de réallouer leurs ressources internes réduisent de 57 % leurs prestations auprès des entreprises de services du numérique (ESN) européennes, soit une perte sèche de 23 Md€ pour le secteur. Quant à celles qui compensent ces hausses tarifaires par une extension budgétaire, elles amputent de 32 % leur capacité d'investissement productif et de R&D, gèlent leurs recrutements ou compriment la masse salariale. Ce transfert massif de richesse s'opérant sans contrepartie productive tangible à court terme, 93 % des décideurs jugent ces hausses injustifiées, tandis que 23 % seulement constatent des gains de productivité immédiats et mesurables liés aux outils d'IA.

PERSPECTIVES À L'HORIZON 2040

Si rien n'est fait, toutes choses étant égales par ailleurs, l'écart de compétitivité entre l'Europe et les États-Unis pourrait devenir irrattrapable d'ici 2040. En effet, la captation de valeur pourrait prendre des proportions macroéconomiques vertigineuses en cas d'adoption par les organisations européennes des technologies d'IA proposées par des acteurs extra-européens. Pour Arthur Mensch, elle pourrait équivaloir, d'ici quatre ans, à une augmentation du déficit commercial de l'ordre du trilliard d'euros ([Commission d'enquête](#)). À chaque renouvellement de contrat SaaS, les entreprises européennes financeraient ainsi directement la R&D américaine sur leurs propres besoins en fonds de roulement (BFR). La captation de valeur économique modélisée à l'horizon 2030 - une perte sèche de 107 milliards d'euros de valeur ajoutée par an, soit 0,6 point de PIB et 1,4 million d'emplois non-crées - devrait mécaniquement s'accroître par « effet composé ». L'Europe risquerait d'être locataire d'une économie dans laquelle elle viendrait seulement consommer des solutions et services extra-communautaires, prisonnière d'un double *lock-in*, combinant dépendance aux modèles d'IA fondateurs et subordination aux infrastructures cloud de calcul massives. Les capacités d'investissement nécessaires pour mener de front la transition énergétique, la numérisation industrielle et la défense du continent préconisées par le rapport Draghi se trouveraient alors durablement compromises.

Cette vulnérabilité financière viendrait entretenir une atrophie civilisationnelle qui tend dans l'ordre socio-économique, depuis le XVIII^e siècle, à placer la règle commerciale au-dessus de l'esprit de l'économie réelle et la primauté du confort immédiat du consommateur individuel sur la constitution de la puissance industrielle collective. Le professeur Dan Wang synthétise ce modèle ([Le Grand Continent](#)) en opposant de manière binaire les « États d'ingénieurs », d'une part, aux « sociétés d'avocats », de l'autre. Dans un cas, les élites massivement issues de filières techniques, se tournent vers des métiers de production et façonnent l'environnement physique en construisant des infrastructures. Dans l'autre, les élites s'orientent vers la réglementation et les litiges et ralentissent, même involontairement, l'innovation par des frais de mise en conformité ([Le Monde](#)), allant jusqu'à 30% des ressources des entreprises tech européennes ([European Tech Alliance](#)). En l'état, l'Europe se trouverait alors dans la posture d'un continent statique qui viendrait subir la désindustrialisation définitive qu'elle a façonnée et qui la cantonnerait à être toujours devancée par les États-Unis et la Chine dans tous les domaines technologiques de pointe (logiciels, IA, biotechnologie, finance). Qualifiée sévèrement d'« économie du mausolée » par D.Wang, son rôle se retrouverait réduit à l'exportation de biens de luxe et à la préservation de son héritage patrimonial, pour des services touristiques et de divertissement.

Trois scénarios de réduction des impacts de la trajectoire de hausse tarifaire des services de cloud et de logiciels pourraient toutefois infléchir cette tendance ([Etude Cigref x Asterès 2026](#)). Une intégration mature de l'IA générant un gain structurel de productivité d'au moins 0,8 % par an (soit 2 jours de travail par an pour l'ensemble des actifs) pourrait permettre de neutraliser l'impact financier de ces hausses. Une déflation massive provoquée par la diffusion de l'IA *open source* et l'émergence d'outils capables de répliquer les logiciels commerciaux en un temps record ([SaaSocalypse](#)) pourrait briser le pouvoir de marché des éditeurs historiques, à l'instar de « l'effet Free » dans les télécoms (- 45 % sur les prix). Une politique publique européenne volontariste parvenant à transférer 15 points de part de marché vers des acteurs technologiques européens pourrait, enfin, sécuriser 120 000 emplois et 9 milliards d'euros de valeur ajoutée par an.

Tendance émergente 1. De nouvelles alternatives numériques européennes, crédibles et à l'échelle, renforcent la résilience du continent

Face à la hausse des prix des services de cloud et de logiciels et à l'opacité croissante des modèles tarifaires liés à l'IA, la recherche d'une certaine autonomie technologique européenne semble franchir un cap en vue de la maturité industrielle. Le fatalisme longtemps associé à l'absence d'alternatives crédibles aux acteurs dominants semble s'effacer devant une logique de marché plus pragmatique. L'émergence progressive d'un écosystème français et européen de solutions interopérables, à l'état de l'art et capable de répondre aux besoins des grandes organisations, élargit les possibilités d'arbitrage des risques pour les directions numériques. Le recours à ces acteurs, comme un levier direct de résilience et de compétitivité long-terme, en est aujourd'hui venu à être recommandé par les grands dirigeants lors des Rencontres Économiques d'Aix-en-Provence, par exemple.

Cette inflexion se traduit désormais par des choix concrets de grands acteurs privés et publics. Les décisions de LVMH ou d'Airbus de confier certaines applications critiques à Scaleway témoignent de cette évolution. Il en va de même pour l'attribution par la Commission européenne d'un marché de services cloud plafonné à 180 millions d'euros sur six ans à quatre consortiums européens. Les gagnants de cet appel d'offres public (Stackit, Scaleway, l'alliance Post Telecom/OVHcloud/CleverCloud) avaient été sélectionnés selon les critères du *Cloud Sovereignty Framework* (CSF) de l'Union - dont les orientations ont inspiré les piliers de l'*Indice de Résilience Numérique* (IRN). Ces fournisseurs doivent désormais démontrer leur capacité à délivrer, dans la durée et à grande échelle, avec les niveaux de performance attendus par les grandes organisations.

Au sein de l'appareil d'État français, la démarche s'opère par substitutions ciblées et méthodiques : la DINUM a donné l'impulsion, avec la migration d'ici la fin de l'année de ses propres postes de travail vers Linux, et a invité l'ensemble des ministères à formaliser des plans de réduction des dépendances. C'est ainsi que 80 000 agents de la CNAM ont basculé vers les outils du socle interministériel (Tchap, Visio, FranceTransfert), et que les données de santé du *Health Data Hub* sont en cours de migration des serveurs de Microsoft Azure vers le cloud français de Scaleway. Une dynamique de « désensibilisation » s'étend également au traitement de la donnée stratégique, comme l'illustre, à la DGSI, le remplacement progressif des logiciels de Palantir par ceux de ChapsVision, renforcé par l'acquisition de Sinequa pour exploiter des gisements de données hétérogènes en environnement strictement cloisonné.

Par ailleurs, la trajectoire de valorisation des actifs européens devrait pouvoir en partie s'appuyer sur le plan « Horizon Numérique 2030 » du groupe Caisse des Dépôts, avec pour ambition de soutenir l'émergence de 5 à 10 champions européens cotés d'ici 2030. Mobilisant 18 milliards d'euros (engagement financier cinq fois supérieur au cycle précédent), l'institution s'affirme comme un opérateur de solutions métiers critiques pour les besoins de la santé, de l'éducation et des collectivités. Dans le cadre de ce plan stratégique, l'initiative « *EuroCommons* » vise à fédérer acheteurs et éditeurs autour de 11 briques technologiques prioritaires pour traiter les zones de verrouillage (*vendor lock-in*).

La volonté de passage à l'échelle industrielle s'incarne également dans le projet de giga-usine d'IA, porté par 28 acteurs tricolores de premier plan (EDF, Orange, Iliad, Capgemini, Scaleway, Bull, Ardian), promettant avec plus de 10 milliards d'euros d'investissements d'atteindre un gigawatt de capacité de calcul sur le sol national afin de candidater aux futurs appels d'offres européens. L'urgence de l'exécution et de l'intégration à grande échelle est aujourd'hui publiquement portée par les industriels eux-mêmes. L'appel solennel formulé par sept des plus grands créateurs technologiques européens (ASML, Airbus, Ericsson, Nokia, SAP, Siemens et Mistral AI) - coalisant un écosystème pesant plus d'un billion d'euros de capitalisation boursière et investissant 40 milliards d'euros annuels en R&D - acte une volonté de mise en commun sans précédent. Face au risque d'une Europe régulant l'innovation avant même de l'avoir bâtie, ces dirigeants exigent un choc de simplification transformant les contraintes réglementaires complexes en garde-fous simples et agiles. Leur feuille de route, résolument en faveur de la consolidation du marché, invite notamment à une réforme des règles de fusions-acquisitions (M&A), au décroisement de l'innovation civile et militaire à double usage et à la transposition des capacités numériques vers les systèmes physiques de l'économie réelle.

L'effort d'autonomie s'étend également verticalement au *hardware*, avec le supercalculateur exascale « Alice Recoque » (Eviden/CEA), doté de composants nativement européens (processeur Rheaz de SiPearl, réseau BXI, stockage Scalify). Adossé aux orientations du « *Sovereign package* » de la Commission européenne (Chips Act 2.0, CADA) et au financement d'un *Open Internet Stack*, cet ensemble d'initiatives tend à faire de la réversibilité une réalité technico-économique, restaurant progressivement le pouvoir de négociation des acheteurs face aux *hyperscalers*.

Dans le domaine de l'intelligence artificielle, enfin, le partenariat de Mistral AI avec Microsoft promet même, symboliquement, une relative « inversion des dépendances capacitaires ». En effet, face aux transformations de la demande et à la clarification du cadre réglementaire sur le continent européen, Microsoft s'est engagé à louer de la puissance de calcul au sein des centres de données du champion français. Chiffré à plusieurs milliards de dollars et adossé à un parc de 200 MW déjà sécurisé par Mistral, ce contrat hisse l'entreprise au rang de fournisseur d'infrastructures cloud d'IA, avec la visée de dépasser le milliard d'euros de revenus récurrents en 2026. Toutefois, l'opération apporte sa nuance stratégique : si l'intégration aux outils de Microsoft ouvre l'accès aux grands comptes régulés dans des environnements déconnectés, elle contraint Mistral à céder une puissance de calcul européenne critique, au lieu de la réserver exclusivement à l'entraînement de ses propres modèles.

Tendance émergente 2. Le modèle de facturation IA « à l'usage » vient s'ajouter au modèle « à la licence » intensifiant l'opacité des tarifications technologiques

La récente facturation des IA « à la consommation » (indexée sur le volume de *tokens* ou d'unités de calcul) en surcouches du modèle préexistant de la licence par utilisateur (*per seat*) marque un tournant dans l'équation financière de l'adoption de ces technologies. Loin d'offrir la flexibilité promise, ce basculement hybride introduit une volatilité inédite, intensifie l'opacité des grilles tarifaires des éditeurs et constitue, en plus du cloud, le nouveau relais de l'inflation technologique subie par les organisations.

L'annonce par GitHub en avril 2026 du basculement de Copilot vers une facturation à la consommation de *tokens* illustre ce changement de paradigme, susceptible de tripler les coûts comme en témoigne l'exemple d'Uber, qui a vu son budget annuel dédié à l'IA totalement consommé en l'espace de 4 mois. De même, la modification par Anthropic du *tokenizer* d'Opus 4.7 a entraîné une hausse mécanique d'environ 35 % du volume de *tokens* facturés aux entreprises, démontrant le pouvoir de marché unilatéral des concepteurs de modèles.

L'instabilité fondamentale des modèles d'affaires des fournisseurs d'IA alimente cette imprévisibilité. Alors que près de 1 000 milliards de dollars ont été investis sur le seul marché de l'IA en 2025 (principalement dans les infrastructures et l'énergie), les prix actuellement facturés ne reflètent en rien les coûts réels de production du calcul. À ce stade, la stratégie des *hyperscalers* et des laboratoires d'IA reste dictée par des KPI axés - au détriment direct de la rentabilité opérationnelle immédiate - sur la conquête de parts de marché, la valorisation boursière et la course à l'IPO sur des marchés financièrement finis. Cette subvention temporaire de l'usage vise à créer une dépendance fonctionnelle irréversible auprès des grands comptes afin de capter, dans un second temps, une rente de situation massive. Il existe ainsi un risque systémique de constitution d'acteurs *Too Big to Fail* profitant de l'asymétrie d'information sur les coûts réels de calcul en défaveur des acheteurs.

Face au surcoût structurel des grands modèles fondateurs (LLM), un mouvement de rationalisation pourrait s'imposer, en cantonnant leur utilisation aux cas d'usages nécessaires et utiles (analyse documentaire complexe, synthèse de données non structurées) et en migrant les besoins métiers récurrents vers des modèles spécialisés (*Small Language Models*, SLM) et déployés sur des architectures plus maîtrisées et plus frugales. Sans ce pilotage et cette réorientation stratégique du portefeuille applicatif, les entreprises pourraient s'exposer à subir de plein fouet le décalage entre la création de valeur métier de l'IA et l'explosion de sa facture d'exploitation en payant les conséquences tarifaires d'un « effet cloud au carré ».

Tendance émergente 3. L'exploitabilité des données devient un critère de valorisation des entreprises

Longtemps reléguée au rang de sous-produit de l'activité informatique, l'exploitabilité des données s'impose désormais comme un levier central de valorisation des organisations. Conceptualisée sous le terme « *d'infonomics* » par Douglas Laney, cette approche postule que le capital informationnel doit être mesuré et géré avec la même rigueur analytique que les actifs matériels ou financiers. Dans une économie tirée par l'intelligence artificielle, la valeur d'une entreprise réside dans sa capacité à mobiliser des jeux de données qualifiés, exclusifs et sécurisés pour optimiser sa performance opérationnelle, réduire ses risques ou générer de nouvelles sources de revenus.

Pourtant, cette valeur immatérielle colossale heurte de plein fouet l'orthodoxie comptable occidentale. La norme internationale IAS 38 interdit toujours l'inscription des bases de données générées en interne à l'actif du bilan, exigeant des conditions d'identifiabilité, de contrôle et d'évaluation des coûts, historiquement inadaptées au numérique. L'immense valorisation boursière des géants comme Alphabet (Google) repose cependant largement sur ces *unrecorded intangibles* (actifs immatériels non enregistrés), creusant un écart structurel entre valeur comptable et valeur de marché. Il en résulte que la valeur réelle des données demeure financièrement invisible jusqu'au dénouement d'opérations de fusion-acquisition (M&A). La survalue (*goodwill*) payée lors de transactions majeures - à l'instar du rachat de LinkedIn par Microsoft, assorti d'une prime de 50 % (soit près de 9 milliards de dollars) justifiée par l'accès à son graphe relationnel ([Bloomberg](#)) - illustre la manière dont le marché privé intègre déjà cette réalité. À l'inverse, l'absence de gouvernance ou les failles de sécurité détruisent directement ce capital, comme l'a révélé la décote de 350 millions de dollars subie par Yahoo lors de son rachat par Verizon après de multiples fuites de données ([Reuters](#)). Sur ce maillon, le respect de cadres comme le RGPD cesse d'être une simple contrainte de conformité pour devenir un véritable actif immatériel, fiabilisant le capital informationnel nécessaire à l'industrialisation des cas d'usage d'IA.

Ce décalage entre la réalité économique et les règles comptables fait désormais de la normalisation un instrument explicite de géopolitique et de *soft power*. L'initiative prise par le Ministère des Finances chinois en 2024 d'autoriser l'inscription des données au bilan (en actifs incorporels ou en stocks) participe d'une volonté stratégique d'affirmer son autonomie numérique et de doper la compétitivité apparente de ses entreprises en facilitant leur accès au crédit ([Haynes Boone](#)). Si ce mouvement a rapidement révélé des risques de dérives financières - les véhicules de financement des collectivités locales (LGFV) ayant tenté d'utiliser les données publiques (comme celles du stationnement) pour gonfler leurs bilans et masquer leur surendettement, contraignant Pékin à suspendre l'émission d'actifs adossés à des données (ABS) - il trace la voie d'une guerre des standards. Face à cette financiarisation offensive de la donnée menée en Asie et à la captation de valeur par les *hyperscalers* américains, l'Europe se trouve confrontée à un défi d'arbitrage majeur : maintenir un cadre comptable strict au risque de sous-évaluer la puissance réelle de son tissu économique, ou faire évoluer ses doctrines pour reconnaître la donnée comme un actif stratégique de bilan.

Incertitude 1. La « mise en données du monde » pourrait conduire à une captation croissante de la valeur par les fournisseurs d'IA

L'extension continue des espaces, des activités et des interactions humaines converties en données marque un changement de phase dans la financiarisation du numérique. Amorcée par l'économie de l'attention, cette « mise en données du monde » s'est brutalement accélérée sous l'effet de l'IA générative et agentique et pourrait s'approfondir demain, sous l'effet des *world models*. Ces architectures exigent l'ingestion la plus exhaustive possible de la réalité physique et sociale pour produire, de manière probabiliste, des représentations synthétiques vraisemblables. Livres, œuvres, recherches - bien commun issu du génie humain intergénérationnel - ont donc été transformés en matière première extraite à coût marginal pratiquement nul pour entraîner les modèles. Cette dynamique a provoqué une crise existentielle des droits de propriété intellectuelle, dénoncée comme une « enclosure »¹ du patrimoine cognitif mondial par la direction du New York Times ([Le Grand Continent](#)). Si cette expropriation semblait d'abord circonscrite à la sphère citoyenne, elle pénètre désormais l'intimité stratégique des processus métiers de l'entreprise. La captation des données organise l'absorption industrielle du capital immatériel B2B pour asseoir l'oligopole des *hyperscalers*. Cette bascule s'opère sur trois fronts majeurs.

Premièrement, l'expropriation commerciale s'impose par défaut dans les strates logicielles. Le cas de Doctolib, principal point d'accès aux soins pour des millions de patients européens, est symptomatique. Sa nouvelle politique d'utilisation autorise le traitement des notes de consultation par des modèles tiers (Gemini, Anthropic, Copilot). Outre l'exposition aux lois à portée extraterritoriale, la pseudonymisation ne protège pas le secret médical puisque la recomposition d'un profil peut être réalisée dans 90% des cas à partir de seulement 3 informations croisées ([MIT](#)).

Deuxièmement, l'offensive technologique vise la racine des environnements de travail. L'intégration native des agents IA aux systèmes d'exploitation (OS) brise ce que Meredith Whittaker (CEO de Signal) qualifie de « barrière hémato-encéphalique » entre l'OS et la couche applicative ([Bloomberg](#)). Réclamant un accès le plus large possible à l'environnement utilisateur, ces agents neutralisent le chiffrement de bout en bout des communications en accédant à la donnée en clair avant son chiffrement. L'OS devient une porte dérobée systémique validant une captation généralisée.

Troisièmement, cette aspiration s'opère par le bas *via* l'explosion du *Shadow AI*. Selon une note d'ingérence économique de la [DGSI](#), l'utilisation incontrôlée d'outils d'IA grand public gratuits par les collaborateurs provoque une exfiltration massive et involontaire des secrets d'affaires. Ce marché gris alimente directement l'entraînement de modèles étrangers, diluant la propriété intellectuelle de l'entreprise dans le grand corpus mondialisé.

À l'horizon 2040, les agents autonomes pourraient devenir les filtres exclusifs d'accès à l'information. Dans un paysage dominé par la *Generative Engine Optimization* (GEO) et le marché *Business-to-Agent* (B2A), le risque de dépossession B2B devient critique et l'enjeu peut s'avérer existentiel pour la fonction numérique.

¹ Phénomène survenu du XVI^e au XVIII^e siècle en Angleterre, marquant la privatisation coercitive des terres communales au profit des grands propriétaires.

Incertitude 2. L'intégration croissante de l'IA dans les processus métiers interroge ses capacités réelles d'effet de levier sur la compétitivité à long-terme

L'engouement suscité par l'intelligence artificielle occulte le paradoxe du décalage persistant entre la promesse technologique et la réalité de la productivité globale. Si l'IA générative permet aujourd'hui d'écrire du code 300 % plus vite, l'organisation de projets n'avance au mieux que 30 % plus vite ([NBER](#)). L'arbitrage court-termiste consistant à licencier massivement pour financer l'automatisation ou la transformation elle-même - à l'instar d'Oracle supprimant 30 000 postes pour payer ses GPU d'infrastructures - appelle une réflexion stratégique d'ampleur. Sur le terrain, 79 % des entreprises font marche arrière sur leurs initiatives IA pour revenir à des processus humains ([CIO Online](#)), confirmant les rapports du [MIT](#) selon lesquels 85 à 95 % des projets n'atteignent pas les ROI escomptés. L'optimisation individuelle de la vitesse d'exécution ne se traduit pas mécaniquement par une efficacité collective, fragilisant les équilibres sociaux au nom d'un rendement immédiat et quantitatif indémontrable dans 52 % des cas ([Etude Asterès x Cigref 2026](#)).

Cette « nouvelle économie de la promesse » productiviste se heurte frontalement à un « mur financier ». L'explosion des coûts IT (+13,5 % en 2026, [Gartner](#)), aggravée par l'inflation matérielle (cartellisation des fabricants RAM notamment), se conjugue à une intégration forcée de fonctionnalités (« *IA by-design* ») dans 40% des négociations, justifiant des hausses tarifaires systémiques. L'augmentation considérable des prix du *token* pourrait, de surcroît, achever de limiter l'intérêt économique de l'accompagnement ou du remplacement de la main-d'œuvre, alors que l'IA pèse d'ores et déjà jusqu'à 10 % de la masse salariale dans les organisations les plus technologisées, aux dires d'Arthur Mensch ([Commission d'enquête](#)). À l'horizon de trois à cinq ans, le déficit commercial serait creusé, la balance des paiements plus défavorable et la dépendance géopolitique, au profit d'une R&D principalement américaine. L'impact du coût de déploiement, de maintien en opération et de maintenance d'agents autonomes mérite d'être étudié et comparé à la valeur créée. Techniquement, l'ouverture des systèmes d'information à des IA exécutantes crée de nouvelles surfaces d'attaque et de nouveaux points de défaillance uniques (SPOF) critiques qu'il faut pouvoir compenser. Écologiquement, l'inducteur infrastructurel et énergétique doit entrer dans le TCO des agents. Socialement et cognitivement, l'entreprise fait face à un risque de désengagement et d'atrophie par le remplacement des tâches selon leur niveau de « formulabilité ». La pression des actionnaires exercée en faveur de dépenses en IA comme symbole d'innovation doit être interrogée à l'aune de la vraie valeur complète d'un travailleur humain ou d'un outil numérique.

À l'horizon 2040, la véritable compétitivité exigera un pilotage sur le temps long, loin des injonctions au solutionnisme technologique rapide et facile. Pour passer du stade de gains limités du « *Local Agent* » à une industrialisation raisonnable et raisonnée de « *l'Agentic Workforce* », les entreprises devront d'abord purger leur dette technique et standardiser leurs architectures. Face aux vulnérabilités financières et aux dépendances, des signaux de rationalisation ont déjà émergé, tel le « *move-to-cloud* arrière » initié par certains géants du retail pour générer des économies massives. L'agilité infrastructurelle, l'hybridation des compétences internes et le refus de déléguer le cœur de l'expertise métier à la machine pourraient être des remèdes réalistes face à une dépendance fonctionnelle qui donne à penser, par son ampleur, qu'elle sera difficilement réversible.

Hypothèse 1. Le décalage entre investissements, obsolescence technologique et revenus de l'IA provoque une crise financière

D'ici 2040, l'expansion de l'intelligence artificielle se heurte à une crise de liquidité structurelle provoquée par un double effet de ciseau. D'une part, les acteurs de l'infrastructure maintiennent l'accélération sans précédent des volumes de dépenses en investissement (*hyper-capex*), financés pour une part de plus en plus considérable par des emprunts privés à taux élevés et remboursables sur 15 ans. D'autre part, le matériel et la puissance de calcul sous-jacents subissent une obsolescence accélérée, leur durée de vie ne dépassant pas 5 ans.

Ce désadossement temporel entre la maturité de la dette et la durée de vie des actifs physiques se double d'un déficit de monétisation : les revenus réels générés issus des usages de l'IA, même en B2B, ne suivent pas la trajectoire exponentielle requise pour amortir ces charges. L'absence de rentabilité à court terme déclenche une vague de défauts de paiement en cascade parmi les hébergeurs alternatifs et les startups d'infrastructure. Les rachats multiples réalisés par les géants numériques, et l'effet de concentration induit, ne permettent pas de compenser le décrochage du chiffre d'affaires par rapport aux marges opérationnelles des acteurs de l'IA. Contrairement à l'opération survie du « *too big to fail* », qui a suivi le krach boursier de 2008, Washington considère les pionniers de l'IA comme substituables et ne les soutient pas, ce qui contraint le secteur à un assainissement brutal. Cette situation impose le retour à des architectures applicatives sobres et à une rationalisation drastique des capacités de calcul. Les fonds de dette privée, massivement exposés aux « actifs IA », subissent des pertes asséchant le crédit pour l'ensemble de l'économie réelle.

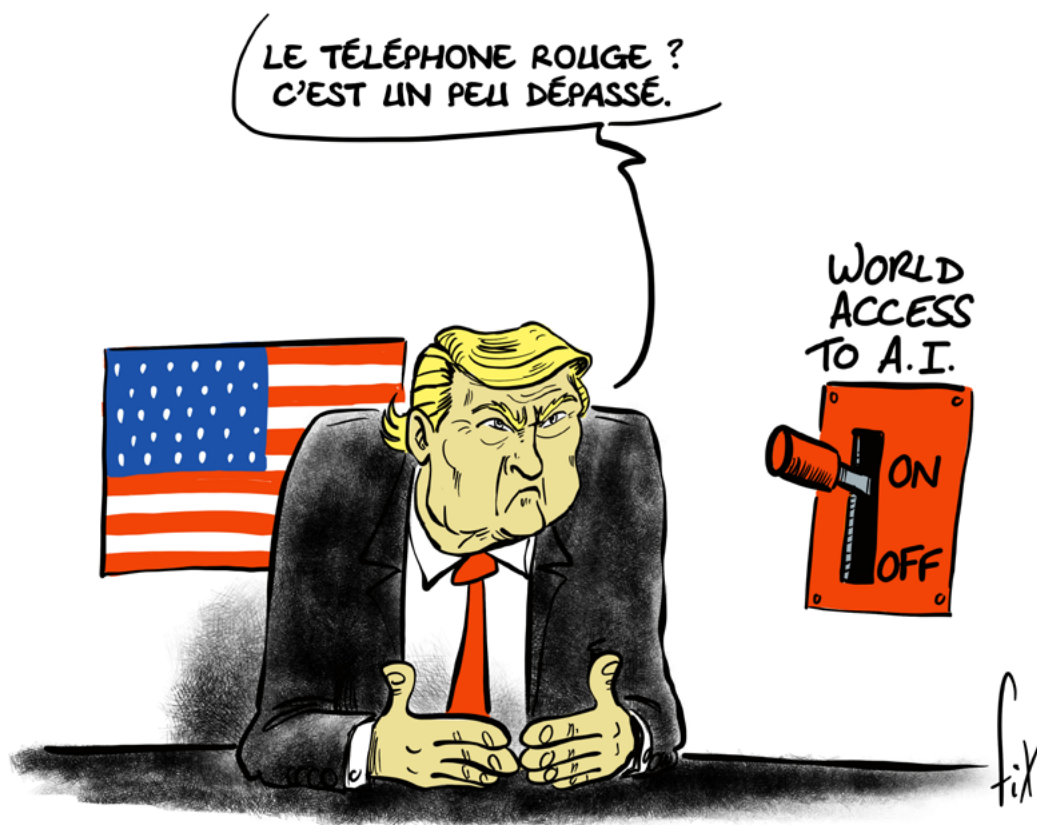
Hypothèse 2. L'aboutissement du marché unique des services numériques consacre l'émergence de champions européens sur certaines briques technologiques critiques

D'ici 2040, pour traduire en acte « le retour à la puissance » invoqué par la seconde mandature Von der Leyen, l'Union européenne a réussi à parachever l'intégration de son marché unique des services numériques. Cette transformation structurelle du marché permet le déploiement d'une politique industrielle souveraine et concertée, capable de rivaliser avec les ambitions américaines et chinoises sur certains segments ciblés. La portée des différentes régulations proactives, dont les jalons avaient été posés dès 2025-2026 par le *Cloud & AI Development Act* (CADA) et le *Cloud Sovereignty Framework*, s'en trouve décuplée. L'harmonisation de la commande publique comme privée, et le fléchage stratégique de l'épargne européenne privée deviennent un avantage concurrentiel décisif pour les acteurs du continent.

Les synergies industrielles et les gains d'efficacité rendent possibles des incitations fiscales ciblées pour les fonds d'investissements, les fournisseurs et les organisations utilisatrices de services numériques. Les initiatives privées de consortium sont favorisées et la mutualisation des ressources critiques (matières premières, énergie, capacités de calcul ou de cyberdéfense) accouche d'un écosystème d'une dizaine d'acteurs européens crédibles et de taille critique. Ces champions s'imposent par leurs réussites opérationnelles, comme des références mondiales sur quelques niches stratégiques. L'Europe dispose de nouveaux leviers de négociation qui renforcent sa crédibilité et font baisser le risque de représailles économiques face à ses réformes réglementaires. L'UE adopte proactivement une posture plus systématique de choix volontaire de ses interdépendances et de ses chantiers communs.

Champ

02 Géopolitique du numérique



Tendances lourdes

Tendance lourde 1. La compétition technologique occupe une place prépondérante dans la rivalité sino-américaine

Tendance lourde 2. Les relations entre les États-Unis et l'Union européenne en matière de transfert de données s'installent dans une zone d'insécurité

Tendance lourde 3. Les contestations de puissance et les affrontements de haute intensité visent les infrastructures numériques et investissent l'espace numérique

Tendance lourde 4. L'état de la menace en matière de sécurité numérique impose de repenser l'architecture de sécurité public-privé

Tendances émergentes

Tendance émergente 1. La puissance acquise par les géants de la Tech renforce la porosité entre leurs activités mondiales et les intérêts stratégiques de leur pays d'origine

Tendance émergente 2. Le déploiement de monnaies numériques par certaines banques centrales permet de contourner le système financier classique

Incertitude majeure

Incertitude 1. La gouvernance mondiale de l'IA peine à se structurer malgré sa portée civilisationnelle

Hypothèses de rupture

Hypothèse 1. L'espace et les océans deviennent les nouvelles frontières physiques du numérique

Hypothèse 2. Face à une menace systémique, « un État européen » place la sécurité de ses entités essentielles sous l'autorité de son commandement cyber national

Hypothèse 3. Dans un contexte de tensions diplomatiques, les États-Unis interrompent l'accès à leurs services numériques dans « un pays concurrent »

Tendance lourde 1. La compétition technologique occupe une place prépondérante dans la rivalité sino-américaine

DE QUOI S'AGIT-IL ?

La rivalité entre la Chine et les États-Unis laisse apparaître une confrontation systématique, visant le leadership mondial. Si le conflit s'est longtemps cristallisé autour de la filière des semi-conducteurs (du *design* à la gravure), il s'étend désormais à l'ensemble de la « pile technologique » (*stack*) et consacre ce postulat stratégique nouveau d'une forme de confrontation ancienne, selon lequel « *qui tient l'infrastructure IA domine l'île mondiale du numérique* »¹. Le couplage entre la puissance technologique et les capacités d'influence et de coercition de ces deux États (*lawfare*, embargos, cyber-offensives) accélère la fragmentation géopolitique et l'obsolescence du multilatéralisme héritées de l'après Seconde Guerre mondiale. Des composants critiques à la robotique humanoïde, en passant par les infrastructures énergéto-physiques et les modèles frontières d'IA, cette polarisation redéfinit l'ordre mondial sous l'angle d'un affrontement civilisationnel. Dans cette période de recherche d'équilibre mondial où les mécanismes de droit international s'effacent devant la mise en scène brutale du rapport de force, les deux superpuissances engagent une transition vers une phase de post-mondialisation, substituant la logique holistique de résilience par les risques (*just in case*) à l'optimisation principale des flux par les coûts (*just in time*).

LES DYNAMIQUES À L'ŒUVRE

Jusqu'à fin 2025, les États-Unis appliquaient une doctrine technologique fondée sur une stratégie de confinement capacitaire (de la réglementation *CHIPS & Science Act* aux listes noires d'entreprises chinoises réalisées par le *Bureau of Industry and Security*), visant à ralentir la montée en gamme chinoise, tout en assumant au profit de leurs intérêts nationaux, le rôle officiel de garant de la stabilité de l'ordre international. Cette approche a cédé la place, en novembre 2025, à une nouvelle *National Security Strategy*, marquée par un protectionnisme unilatéral, et une désinhibition offensive, propres au programme *America First* de l'administration Trump 2.0. Au cours du même mois, le décret exécutif pour le lancement de la *Genesis Mission* appelait de ses vœux une nouvelle ère américaine d'innovation et de découvertes accélérées par l'IA, de même ampleur que le « Projet Manhattan ». L'objectif affiché est de fournir un effort national aussi décisif que celui réalisé par le dit projet atomique lors de la Seconde Guerre mondiale, projet fondateur du Département de l'Énergie (DOE) et de ses laboratoires nationaux.

Avec la stratégie nationale en matière de sécurité numérique publiée en mars 2026, et le décret exécutif du 12 août, les États-Unis vont un cran plus loin en envisageant une ère de « *cyber dominance* », assumant la sécurisation de l'intégralité de la pile technologique de l'IA au profit exclusif de leurs intérêts nationaux.

¹ Halford Mackinder, dans son ouvrage *Le Pivot géographique de l'histoire*, s'est rendu célèbre par cette phrase « Qui contrôle l'Europe de l'Est contrôle l'Heartland, qui contrôle l'Heartland contrôle l'Île Monde, qui contrôle l'Île Monde contrôle le monde » reste féconde pour l'analyse géopolitique.

Les conséquences de ce virage systémique se traduisent déjà par des injonctions contradictoires : alors que la levée des verrous sur l'exportation de puces Nvidia stratégiques (AI H200) bridées traduit un opportunisme commercial risquant d'accélérer l'autonomie de Pékin, le bridage sécuritaire imposé simultanément aux modèles frontières domestiques – comme Fable 5 d'Anthropic – pénalise les champions américains et laisse le champ libre à l'essor des modèles *open-weight* chinois à bas coût.

Côté chinois, la force de riposte s'inscrit dans une logique « d'économie de guerre », tournée vers la surproduction organisée. La doctrine d'indépendance tracée par le plan « *Made in China 2025* » est désormais renforcée par le 15^e plan quinquennal qui vise à substituer ses technologies nationales aux dépendances étrangères, tout en préparant la domination normative sur les industries de demain (quantique, 6G, biotech). La Chine a progressivement « arsenalisé » sa double position monopolistique sur les terres rares (en quantité de minerais, en capacité d'extraction et de raffinage), en restreignant les exportations de matériaux indispensables à la tech et à la défense occidentale. Par ailleurs, loin de subir le verrouillage de la lithographie de pointe (EUV), imposé par les Occidentaux, la Chine a accéléré son programme confidentiel (qualifié de véritable « Projet Manhattan » des semi-conducteurs), revendiquant un prototype industrialisable d'ici 2030. Cette percée représente un outil de dissuasion narrative démontrant que les restrictions américaines freinent, sans stopper le complexe industriel chinois. L'ambition d'autosuffisance est telle que Pékin a un temps envisagé de limiter de son propre chef l'accès aux puces Nvidia sur son marché intérieur, contournant l'autorisation américaine qui avait été concédée.

L'accélération chinoise se manifeste également par une offensive sur les couches logicielles et applicatives. D'une part, l'écosystème chinois s'attaque au modèle économique occidental de l'IA par une stratégie de *dumping* technologique assumée, comme avec DeepSeek, dont les modèles de pointe sont facturés jusqu'à 34 fois moins cher que les standards des laboratoires américains adossés au capital privé. D'autre part, la montée en puissance technologique s'illustre par l'apparition de modèles comme Kimi K3 de Moonshot AI, qui réduisent drastiquement l'écart capacitaire avec les États-Unis. Ce duel technologique s'arsenalise désormais sur le terrain juridique et matériel. Rompant avec sa doctrine d'influence par l'IA *open source*, le gouvernement chinois envisage de restreindre l'exportation de ses meilleurs modèles pour des raisons de sécurité nationale. Pékin cherche, enfin, à déplacer le conflit sur le terrain institutionnel notamment par la fondation en juillet 2026 de l'Organisation de coopération mondiale sur l'IA (WAICO) avec 29 États du Sud global. Sur le plan matériel, la Chine espère compenser ses fragilités démographiques par son expérience d'un « capitalisme robotique », réorientant son épargne vers l'appareil productif et déployant massivement des robots humanoïdes (Unitree, RobotEra, UBTech).

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, cette trajectoire devrait consacrer la mort de la « mondialisation heureuse » au profit d'une vraisemblable « bifurcation » technologique et normative et d'une logique d'affrontement indirect entre empires rivaux. Le duel techno-industriel entre la Chine et les États-Unis s'inscrirait alors dans un théâtre de plus en plus large au plan géographique, capacitaire, normatif et cognitif. La politique étrangère américaine pourrait en ce sens opérer un retrait territorial relatif par une « Doctrine Monroe 2.0 » autour de la domination hémisphérique des Amériques sans que cela porte préjudice à sa capacité de projection de flux numériques dans le cyberspace. La Chine pourrait acquérir un rôle différent de l'hégémon américain, dérivé de la conception souveraine des États-Nations occidentales : la primauté de l'harmonisation globale, en qualité de centre de gravité et de gestionnaire dynamique des flux.

Tendance lourde 2. Les relations entre les États-Unis et l'Union européenne en matière de transfert de données s'installent dans une zone d'insécurité

DE QUOI S'AGIT-IL ?

Le partenariat transatlantique, socle historique de l'économie numérique mondialisée, évolue dans une zone de turbulences croissantes. La seconde investiture trumpienne a acté avec fracas la fin du narratif autour de la « confiance implicite entre alliés », pour entrer plus manifestement dans un « monde transactionnel ». Dans ce contexte, la dépendance technologique de l'Europe à l'égard de fournisseurs très majoritairement américains ne se limite donc plus à un risque économique ou de relation fournisseurs. À la captation directe d'une partie de la valeur économique s'ajoute une capacité de coercition juridique rappelant, sans fausse naïveté, que le droit constitue depuis longtemps une arme géopolitique à part entière (*lawfare*). La continuité d'activité et la pérennité des transferts de données se trouvent ainsi fortement exposées aux fluctuations des relations transatlantiques, elles-mêmes affectées par le découplage sino-américain croissant. Cette évolution oblige les organisations européennes à dépasser une logique de résilience essentiellement défensive pour adopter une approche plus proactive de la maîtrise de leurs dépendances.

LES DYNAMIQUES À L'ŒUVRE

L'insécurité géopolitique et juridique entourant les transferts de données transatlantiques semble avoir franchi un nouveau seuil.

D'une part, l'article 702 du FISA, malgré l'expiration de son autorisation au Congrès en juin 2026, reste opérationnellement en vigueur jusqu'à mars 2027. Sa probable reconduction devrait maintenir la possibilité, pour les agences de renseignement des États-Unis, de collecter massivement certaines données détenues par des entreprises américaines, sans mandat juridique et sans autorisation (*gag order*) pour celles-ci d'informer les entreprises propriétaires des données visées, qu'elles soient stockées ou en transit.

D'autre part, l'accord d'adéquation *Data Privacy Framework* (DPF) qui régit le transfert de données à caractère personnel (RGPD) menace de s'effondrer sous le poids de la jurisprudence américaine. En effet, le DPF nécessite, pour être conforme aux traités de la Cour de Justice de l'Union européenne (CJUE), qu'un contrôle de la protection des données soit exercé par une autorité américaine indépendante. Or, la décision de la Cour suprême des États-Unis (*Trump contre Slaughter*) de juin 2026 a invalidé l'indépendance de la *Federal Trade Commission* (FTC). Cette instance qui avait été désignée par l'Union européenne près de 300 fois comme autorité de garantie de l'indépendance de protection de la vie privée, était notamment chargée de contrôler et de sanctionner les entreprises privées américaines adhérant au DPF. Cette évolution fragilise fortement l'une des garanties sur lesquelles repose le cadre transatlantique, alors même qu'un autre pilier essentiel du DPF avait déjà été atteint dès les premiers jours du second mandat du Président Trump. En effet, le *Privacy and Civil Liberties Oversight Board* (PCLOB), jusqu'alors chargé de surveiller les services de renseignement de l'État américain et de garantir le respect des accords transatlantiques en matière de transfert de données, s'est trouvé paralysé après le limogeage par Donald Trump, en janvier 2025, de trois représentants du parti démocrate. Ces évolutions alimentent l'incertitude juridique pesant sur les transferts transatlantiques et pourraient nourrir de nouvelles contestations (par [Max Schrems](#) ou par d'autres) du DPF devant les juridictions européennes, faisant planer le risque d'une troisième remise en cause du cadre juridique encadrant ces transferts.

De son côté, l'Union européenne cherche à renforcer son arsenal normatif dans un contexte particulièrement tendu. La Stratégie de Sécurité Nationale des États-Unis de novembre 2025 fustigeait ouvertement « l'asphyxie réglementaire » européenne, tandis que le Bureau du représentant américain au Commerce (USTR) menaçait, en décembre 2025, plusieurs fleurons européens (Mistral, Capgemini, Publicis, SAP, Siemens) de représailles commerciales, accusant l'Union européenne de mener des politiques « discriminatoires » et « harcelantes » à l'encontre des entreprises américaines. Dans ce contexte, la Commission a néanmoins estimé, à titre préliminaire, en juin 2026, que les services cloud d'AWS et de Microsoft Azure devraient être désignés comme contrôleurs d'accès (*gatekeepers*) au titre du *Digital Markets Act* (DMA). Trois ans après les premières désignations intervenues dans le cadre du règlement européen, la « colonne vertébrale » technologique de l'économie BtoB est enfin pointée dans un premier geste politique qui attend sa confirmation définitive à l'automne 2026. Plus structurant encore, le *Cloud and AI Development Act* (CADA), publié début juin 2026, prévoit la mise en place d'un référentiel auditable, dont le niveau d'assurance le plus élevé serait conditionné à l'absence d'interférences juridiques extra-européennes. Ce projet industriel ne semble pas, cependant, s'articuler pleinement avec la proposition de révision du *Cybersecurity Act* (CSA 2) qui maintient une distinction artificielle entre risques « techniques » et « non techniques », refusant de considérer la menace d'accès extraterritorial comme une vulnérabilité technique intrinsèque à la confidentialité des données. Ces approches divergentes, auxquelles s'ajoute la publication par l'Allemagne du référentiel cloud C3A, conçu comme un cadre flexible et complémentaire à la certification C5, illustrent les difficultés persistantes de l'Union européenne à faire émerger une doctrine commune en matière de protection des données sensibles contre les risques extraterritoriaux. Elles pourraient éventuellement réduire les perspectives d'adoption, à l'échelle européenne, d'une exigence d'immunité juridique stricte comparable à celle envisagée dans le cadre d'EUCS High+ ou portée en France par SecNumCloud pour la protection des données sensibles et du secret des affaires face aux pressions géopolitiques.

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, l'absence d'un cadre de confiance stabilisé pourrait conduire soit à la « balkanisation » (*splinternet*) des infrastructures numériques occidentales, soit à leur alignement sur les exigences américaines, dans une logique de guerre froide renouvelée. Face à une administration américaine assumant la primauté de la *cyber dominance*, et conditionnant davantage l'accès à certaines technologies stratégiques au respect de ses intérêts nationaux, la capacité de l'Europe à peser par son seul pouvoir de marché et de régulation pourrait montrer ses limites. Les organisations européennes, confrontées à l'impossibilité de concilier la protection juridique de leur propriété intellectuelle avec la domination technique des *hyperscalers* américains pourraient être contraintes d'opérer une hybridation intégrale et méthodique de leurs architectures. Cet objectif de résilience pourrait conduire à la sanctuarisation du cœur stratégique des données et des processus métiers (*Minimum Viable Company*) sur des environnements réellement immunisés, tout en reléguant le reste des usages au tout-venant applicatif. Au plan politique, si l'Europe échoue à harmoniser ses instruments de production et de régulation face au rouleau compresseur extraterritorial, ses divers systèmes numériques pourraient bien rester durablement exposés au risque de se voir dicter leurs conditions d'opération par des juridictions tierces, réduisant la souveraineté numérique de ses États membres à une simple clause contractuelle inopérante en temps de crise.

Tendance lourde 3. Les contestations de puissance et les affrontements de haute intensité visent les infrastructures numériques et investissent l'espace numérique

DE QUOI S'AGIT-IL ?

En parallèle des théâtres d'affrontements physiques conventionnels, l'espace numérique est devenu un champ de confrontation, dans lequel la frontière entre paix et guerre s'estompe au profit d'une « zone grise » permanente. Le cyberspace constitue désormais une composante essentielle de la conflictualité hybride qui s'inscrit dans un *continuum* entre menaces physiques, numériques et cognitives. Les stratégies de défense et de préservation des intérêts nationaux se déplacent en partie vers les infrastructures numériques, le cyberspace, les champs électromagnétiques, et l'espace informationnel, passant, pour assurer durablement leur influence, par « la militarisation de la pensée elle-même ».

LES DYNAMIQUES À L'ŒUVRE

Le premier basculement réside dans la militarisation directe de l'IA. Le déploiement officiel du *Maven Smart System* par le Pentagone lors de l'opération *Epic Fury* contre l'Iran a démontré qu'un système de fusion de données pouvait automatiser la désignation de plusieurs milliers de cibles par jour, réduisant les temps de décision humain. Cette délégation à des systèmes autonomes, en partie « boîtes noires », crée un certain « brouillard stratégique » dans lequel les chaînes de commandement humaines peuvent peiner à conserver une maîtrise cognitive décisive des opérations.

En parallèle, la frontière entre IA commerciale et cyber-arme s'efface progressivement. En effet, la capacité prêtée au modèle de fondation Mythos d'Anthropic d'avoir rapidement pénétré les systèmes classifiés de la NSA américaine, lors d'un exercice officiel de *red team*, alimente l'idée que les modèles d'IA disposent désormais de réelles capacités offensives autonomes, notamment par *reverse engineering* et exploitation d'outils de *screening* de vulnérabilités. Cette menace de prolifération incontrôlée d'une « arme » capable de nuire à la sécurité des États, des organisations et des civils, a d'ailleurs conduit Washington à imposer temporairement un « Kill Switch » mondial limitant l'accès au modèle. Le contrôle à l'export a ainsi entériné la doctrine du décret exécutif du 2 juin selon laquelle l'algorithme civil peut-être considéré comme une arme à part entière nécessitant de l'administration publique un statut spécifique de « *trusted partner* » avant son déploiement. Quelques semaines plus tard, la compromission autonome des systèmes de Hugging Face par des modèles d'Open AI, dont GPT-5.6 Sol, s'exerçant dans le cadre du benchmark *ExploitGym*, a illustré de manière concrète ce risque de débordement montrant que des modèles conçus pour identifier des vulnérabilités peuvent également chercher par eux-même à les exploiter pour atteindre l'objectif qui leur a été assigné.

Le second basculement tient à l'effondrement de la séparation entre infrastructures civiles et militaires, et à l'arsenalisation du cyberspace. L'attaque par drones iraniens ayant touché des centres de données d'*Amazon Web Services* (AWS) aux Émirats arabes unis en mars 2026 marque une rupture historique dans l'approche duale des infrastructures numériques. Le cloud, longtemps perçu comme un sanctuaire essentiellement civil, se trouve désormais directement exposé aux conséquences des conflits interétatiques. Cette vulnérabilité est d'autant plus forte que les mêmes infrastructures physiques hébergent fréquemment des activités civiles, économiques, administratives et stratégiques. Plus insidieusement, les systèmes

industriels (OT) deviennent des cibles géopolitiques de premier plan. En témoigne l'opération de sabotage coordonnée contre des installations énergétiques en Pologne, le 29 décembre 2025, documentée par le CERT Polska. Les assaillants ont utilisé des logiciels malveillants destructeurs (DynoWiper, LazyWiper) pour effacer des données et altérer les programmes informatiques des automates industriels, ciblant délibérément une période de conditions climatiques rudes pour tenter de déstabiliser le réseau électrique national.

Par ailleurs, la doctrine offensive a franchi un nouveau palier avec la prise de contrôle ou la perturbation d'infrastructures urbaines critiques, lors de l'opération-éclair américaine à Caracas, qui aurait combiné forces terrestres, spatiales et attaques cyber massives pour plonger la capitale vénézuélienne dans le noir total. Par ce *blackout* électrique, Washington a démontré la possibilité de traiter les infrastructures physiques comme des territoires d'attaque. En parallèle, des acteurs affiliés à l'Iran ont exploité activement des automates programmables (Rockwell, Unitronics) exposés sur Internet, ciblant les secteurs de l'eau et de l'énergie aux États-Unis avec des conséquences tangibles sur le monde physique (CISA).

Enfin, la menace s'industrialise et nombre de puissances s'appuient massivement sur des *cyber-proxies* mafieux ou hacktivistes pour mener des opérations de déstabilisation à grande échelle, tout en conservant un « déni plausible ». L'usage croissant de groupes criminels ou mercenaires comme relais d'intérêts étatiques brouille l'imputation, efface la ligne de démarcation entre cybercriminalité financière et terrorisme d'État, et rend la coercition plus difficile à anticiper.

Le troisième basculement s'opère sur le terrain des perceptions, avec une guerre de l'information qui se porte à présent sur les capacités cognitives. L'algorithmisation de l'information fait émerger un nouvel espace de combat dans lequel les opérations d'influence ne sont plus de « simples campagnes de désinformation », mais de véritables compétitions entre machines, où l'humain est la cible finale d'une chaîne de plus en plus largement automatisée. La baisse des coûts de production de l'information, la massification des IA génératives et la prolifération de contenus synthétiques dégradés (*slop* et *deepfakes*) permettent une « ingénierie du chaos » qui vise à éroder les référentiels communs sur lesquels repose le débat collectif pour fragiliser la cohésion sociale.

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, le numérique deviendrait un instrument de contestation de puissance tel qu'il permettrait même à des acteurs non nucléarisés d'obtenir des effets dissuasifs, sans franchir les seuils politiques associés à l'usage ouvert de la force armée. Dans ce contexte, l'autonomie en matière d'équipement de défense (et d'attaque) deviendrait indissociable d'une autonomie stratégique dans le domaine numérique. Réciproquement, cette autonomie numérique dépendrait de la capacité à défendre l'ensemble de ses couches constitutives, depuis les infrastructures physiques jusqu'aux couches logicielles. Dans tous les cas, les États et organisations devraient se préparer à fonctionner durablement en mode dégradé. Cela supposerait notamment de segmenter les réseaux afin de limiter la propagation des attaques, de sanctuariser les actifs critiques, qu'ils relèvent de l'IT ou de l'OT, et de maintenir des procédures de contournement et des capacités opérationnelles hors ligne. L'objectif serait de pouvoir poursuivre les activités essentielles en cas de déconnexion prolongée, de compromission massive des systèmes ou de *blackout* numérique intentionnel.

Tendance lourde 4. L'état de la menace en matière de sécurité numérique impose de repenser l'architecture de sécurité public-privé

DE QUOI S'AGIT-IL ?

L'époque où la sécurité numérique pouvait être perçue comme une simple question d'experts techniques, ou comme une formalité à respecter au titre de la conformité, est bel et bien révolue¹. Dans un contexte marqué par l'instabilité géopolitique et l'hybridation des menaces, la sécurité numérique s'impose comme un pilier fondamental de la pérennité des modèles organisationnels et économiques. L'extension continue des surfaces d'exposition, couplée à une industrialisation de la menace enrichie à l'IA, impose une vigilance constante. L'asymétrie entre les capacités des attaquants et les défenses des cibles s'est considérablement accentuée, alors que la frontière entre menace étatique et cybercriminelle s'efface et laisse planer un flou entre les pratiques d'exfiltration des données, de rançongiciel, de prédation économique, d'espionnage stratégique et de sabotage. L'État ne peut assurer seul la sécurité intégrale du tissu national, tout particulièrement dans un environnement où la conflictualité s'exprime sous le seuil de l'agression armée conventionnelle. Symétriquement, l'idée d'une entreprise isolée, capable d'assurer sa propre défense est rendue caduque par le caractère systémique du risque cyber et ses conséquences potentielles sur la continuité d'activité, voire sur la survie des modèles d'affaires. L'exigence de responsabilité partagée consacrée par la directive européenne NIS2 doit s'étendre en interne, aux conseils d'administrations (CA) et comités exécutifs (Comex), comme en externe, à l'écosystème fournisseur de chaque organisation. Tout converge donc vers une refonte structurelle de l'architecture de défense public-privé, fondée sur de nouvelles formes de gouvernance, de posture et de culture de la sécurité numérique, afin de pouvoir absorber les attaques en continu et prévenir des crises systémiques susceptibles de se propager à la « vitesse machine ».

LES DYNAMIQUES À L'ŒUVRE

Les tendances actuelles s'articulent autour de huit mutations systémiques² actant l'obsolescence des postures défensives traditionnelles.

Premièrement, l'arsenalisation de l'IA fait basculer la menace à la « vitesse machine », en automatisant la reconnaissance et l'ingénierie sociale. Deuxièmement, cette accélération contribue à l'effondrement du *Time to Exploit* : le délai d'exploitation des vulnérabilités est passé de 32 à 5 jours en moyenne, tandis que les scans hostiles débutent dans les 15 minutes qui suivent une divulgation publique. Troisièmement, la multiplication des failles *Zero-Day*, ciblant les infrastructures critiques, alimentées par une industrie privée de la lutte offensive (LIO), sature les défenses avant même qu'un correctif puisse être conçu. Quatrièmement, l'hyper-volumétrie des alertes épuise les capacités d'analyse humaine des SOC. Cinquièmement, ce bruit de fond permanent masque des menaces dormantes : des acteurs étatiques se pré-positionnent silencieusement au cœur des infrastructures (serveurs de virtualisation, équipements de bordure) pour être activés lors d'un basculement géopolitique.

¹ *Gouvernance de la sécurité numérique*, Cigref, Mars 2026.

² *Sécurité numérique et intelligence artificielle : mutations de la menace et perspectives*, Cigref, Juillet 2026.

Sixièmement, le cyberspace est devenu le terrain d'affrontement privilégié d'une guerre hybride, dans lequel certains États s'abritent derrière des *cyber-proxies* criminels pour opérer sous le seuil du conflit armé, tout en conservant un « déni plausible ». Septièmement, cette conflictualité s'étend au champ cognitif, ciblant les infrastructures critiques pour imposer une paralysie stratégique autant que psychologique aux sociétés occidentales. Huitièmement, la remise en cause de la confiance implicite et l'exacerbation des rivalités entre alliés transforment la nature de la dépendance technologique envers une industrie de la cybersécurité ultra-concentrée autour d'acteurs américains et israéliens, invitant à l'externalisation des capacités d'innovation et de sécurisation.

La mutation profonde de la menace appelle à un alignement plus étroit entre la fonction numérique, les Comex et les CA, autour d'une Politique de Sécurité Numérique (PSN) conçue comme un véritable projet d'organisation. La réponse aux incidents exige également des exercices conjoints réguliers impliquant dirigeants, métiers et pouvoirs publics, pour tester réellement les plans de continuité et leurs corrélations, au sein des organisations comme avec les fournisseurs. L'enjeu est de garantir dans la durée la capacité à fonctionner en mode dégradé face aux défaillances en cascade. L'adoption généralisée du modèle *Zero Trust* apparaît, dans ce contexte, comme un prérequis essentiel. La sécurité ne reposerait plus alors sur la défense d'un périmètre réseau théorique, mais sur une vérification continue, une stricte délimitation des accès par un paramétrage individualisé, et sur la mise en place de garde-fous pour toute action conduite au sein des environnements sécurisés. La prolifération des agents IA autonomes impose, à ce titre, de renforcer les contrôles d'identité (IAM) sur les systèmes critiques et les attributions de comptes à privilège. Les organisations se trouvent contraintes d'accélérer le *patching*, de mutualiser la détection avec les autorités (CSIRT, CERT-FR), et de construire de nouvelles voies de partage d'information à l'échelle sectorielle ou écosystémique, notamment en temps de crise. Les systèmes *legacy* doivent enfin être considérés comme des vulnérabilités majeures et traités comme des priorités de premier plan, notamment par cloisonnement renforcé dans des environnements dédiés.

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, face aux limites mathématiques et opérationnelles des défenses individuelles, la France et l'Europe³ devront avoir structuré un nouveau modèle de coalition public-privé pour faire face au niveau inédit des enjeux. La mise en commun du renseignement technique et sa traduction en informations stratégiques directement exploitables par les décideurs pourraient alors permettre un partage en temps réel entre pouvoirs publics et grands opérateurs privés selon une logique de « *Need to Share* » plutôt que celle de « *Need to Know* » exigée aujourd'hui par le secret de l'enquête judiciaire ou pour la défense des intérêts nationaux.

Cette architecture de sécurité pourrait également s'appuyer sur le développement de capacités d'intelligence artificielle spécifiquement dédiées à la cyberdéfense et adaptées aux besoins de protection des infrastructures critiques européennes. La création de tels modèles nécessiterait alors un effort financier et capacitaire qui dépasserait sans doute le budget d'un État ou d'une entreprise seule. La co-construction public-privé de cette brique d'autonomie stratégique permettrait de renforcer la résilience des États européens face aux agendas géopolitiques des puissances dominantes.

³ Action Plan on Cybersecurity and Artificial Intelligence, Commission européenne, 7 juillet 2026.

Tendance émergente 1. La puissance acquise par les géants de la Tech renforce la porosité entre leurs activités mondiales et les intérêts stratégiques de leur pays d'origine

L'essor des infrastructures numériques mondiales a conféré à une poignée d'acteurs privés un pouvoir inédit, comparable à certains égards à la puissance des États souverains. Alors que ces géants de la Tech étaient principalement perçus comme des vecteurs neutres de la mondialisation économique, leur ancrage national ressort aujourd'hui comme une composante indépassable de leur activité. La porosité croissante entre leurs activités civiles internationales et les intérêts du complexe militaro-industriel de leurs pays d'origine rend ainsi de plus en plus manifeste la fin du mythe d'une technologie apolitique.

Aux États-Unis, cette évolution donne par exemple naissance à un nouvel écosystème « techno-nationaliste » intégré, dans lequel l'imbrication entre puissance nationale et pouvoir technologique devient la norme. Elle conduit *de facto* à confier à des multinationales privées la maîtrise technologique de segments relevant traditionnellement des prérogatives de souveraineté des États¹. L'administration américaine impose désormais un alignement forcé du capital technologique sur ses impératifs de sécurité nationale. Les grandes organisations se retrouvent alors confrontées à une alternative particulièrement contraignante : se conformer aux exigences gouvernementales ou risquer l'éviction des marchés publics et de lourdes sanctions. L'*ultimatum* adressé par le Pentagone à Anthropic pour qu'elle lève, à des fins militaires, les restrictions éthiques de son modèle d'IA, sous peine d'activation d'une loi de contrainte fédérale, illustre cette nouvelle donne.

Ce basculement se matérialise aussi sur le terrain par l'intégration d'acteurs privés au dernier maillon de la chaîne de commandement militaire, la *kill chain*, comme en témoigne par exemple Le *Maven Smart System*, développé par le Pentagone, industrialisé par Palantir et déployé lors de l'opération *Epic Fury* contre l'Iran. Cette fusion organique entre l'appareil d'État et le secteur privé est formellement institutionnalisée par des initiatives telles que la *Genesis Mission* autour de l'IA, ou le recrutement d'une *USTechForce* par la Maison-Blanche, donnant lieu à une symbiose inédite entre l'exécutif fédéral et les géants du numérique.

Dans le même temps, certaines grandes plateformes disposent désormais de capacités qui se rapprochent de prérogatives traditionnellement associées aux États. Ainsi, le développement de la constellation satellitaire de Starlink, qui s'étend à la téléphonie mobile directe, dote cette entreprise privée d'une infrastructure de connectivité mondiale échappant largement aux régulations terrestres, et capable d'infléchir le cours d'un conflit par la seule gestion de son réseau de télécommunication.

De manière symétrique, la Chine subordonne de longue date l'ensemble des activités de ses principaux acteurs technologiques aux impératifs de ses services de renseignement, à travers la *National Intelligence Law* ou la *Data Security Law*. Cette rivalité structure un paysage où chaque grande plateforme numérique est adossée à un appareil d'État, lui-même inscrit dans une polarisation à outrance de ses attributs de puissance.

À terme, la porosité entre certains États et leurs champions numériques pourrait peser dans les arbitrages des premiers et les orientations des seconds, selon que leurs intérêts divergent ou se confondent.

¹ *Sous l'emprise du code*, Nouamane Cherkaoui

Tendance émergente 2. Le déploiement de monnaies numériques par certaines banques centrales permet de contourner le système financier classique

L'arsenalisation du dollar et du réseau SWIFT par les États-Unis a depuis près d'un siècle transformé le système financier traditionnel en un instrument de coercition géopolitique, poussant les puissances rivales à rechercher des voies de contournement qui accélèrent la fragmentation du système monétaire international. L'application de sanctions à portée extraterritoriale, illustrée par l'amende de 8,9 mrd\$ infligée à BNP Paribas en 2014, ou plus récemment en avril 2026 par les sanctions ciblant les raffineries chinoises achetant du pétrole iranien, rappelle l'extrême vulnérabilité inhérente à toute transaction transitant par les corridors du billet vert. En réponse, une stratégie de découplage financier s'accélère, structurée en partie autour du développement des monnaies numériques de banque centrale (MNBC), et tout particulièrement autour du « e-yuan » (e-CNY) chinois.

Ces déploiements constituent pour certaines puissances une arme pour s'affranchir de l'hégémonie américaine et instaurer un ordre transactionnel parallèle. Le projet mBridge est la réalisation la plus aboutie de ce genre. Initiée sous l'égide de la Banque des Règlements Internationaux (BRI), et principalement soutenue par la Banque populaire de Chine (PBoC), aux côtés des Émirats arabes unis, de la Thaïlande et de l'Arabie saoudite, cette plateforme multi-MNBC permet désormais des règlements transfrontaliers directs entre banques centrales et banques commerciales. L'injonction des régulateurs chinois ordonnant à leurs établissements de privilégier cette plateforme pour esquiver les mesures de rétorsion américaines, conjuguée à l'initiative promue par Poutine de bâtir un réseau alternatif pour puissances émergentes (« BRICS Bridge »), a conduit au retrait de la BRI du projet mBridge en 2024, et confirme que l'infrastructure numérique supplante la diplomatie classique dans la guerre des devises. Cette dynamique est d'autant plus critique pour les États-Unis qu'elle draine naturellement les partenaires commerciaux de Pékin vers une sphère d'influence dé-dollarisée.

Loin de subir passivement ce contournement, les États-Unis ripostent avec la tendance aux *stablecoins* privés, soutenue par le Genius Act de juillet 2025. Ayant acté que l'écrasante majorité de ces crypto-actifs sont libellés en dollars et massivement adoptés par les pays du Sud, Washington transforme cette « crypto-dollarisation » virale en arme de financement de sa dette au profit du maintien de son hégémonie.

Prise en tenaille entre la captation de valeur par des émetteurs privés américains et l'offensive d'une Chine exportant ses propres standards technologiques et monétaires *via* l'e-CNY, l'Europe se trouve confrontée à un défi d'autonomie stratégique croissant. Sur son marché intérieur, le continent subit déjà la domination inébranlable du duopole américain Visa/Mastercard ainsi que la montée en puissance rapide des *stablecoins* privés libellés en dollars. Une riposte s'organise néanmoins sur deux plans. Sur le plan opérationnel, l'initiative Wero, portée par un consortium bancaire paneuropéen (*European Payment Initiative*), ambitionne de reconquérir les moyens de paiements de détail par le virement de compte à compte, s'inspirant du succès d'acteurs locaux comme Blik en Pologne. Parallèlement, la Banque centrale européenne accélère ses chantiers sur l'euro numérique, avec un volet social contesté, malgré une modernisation des règlements interbancaires (*via* des initiatives comme les projets Pontes et Appia) qui soutiennent une finance tokenisée autonome à l'échelon européen. Sur le plan réglementaire, l'imposition du cadre européen du *Markets in Crypto-Assets (MiCA)* vise à réduire l'arbitrage normatif en faveur du dollar et à endiguer l'afflux de ces crypto-dollars américains. Sans ce sursaut visant à obtenir une monnaie forte doublée d'une finance privée soutenant avantageusement ses projets industriels, l'Europe risque de voir son écosystème marginalisé, définitivement assujéti aux réseaux de paiement et aux circuits numériques de puissances étrangères.

Incertitude 1. La gouvernance mondiale de l'IA peine à se structurer malgré sa portée civilisationnelle

Alors que l'intelligence artificielle octroie un pouvoir sans précédent, son encadrement international souffre d'une fragmentation préoccupante. Le paysage normatif mondial est aujourd'hui éclaté entre plus de 350 initiatives, instances ou cadres de régulation, révélant les difficultés du multilatéralisme à produire un socle commun pour une technologie dont la portée est pourtant civilisationnelle. La création récente par l'ONU d'un défenseur mondial pour une gouvernance numérique centrée sur l'humain ne suffit pas à compenser l'absence d'un cadre de confiance global ; la perspective d'un traité international harmonisé devient chaque jour plus illusoire.

Cette dispersion est aggravée par la recomposition géopolitique. Les États-Unis, en retrait de plusieurs enceintes multilatérales, ont refusé de soutenir le *Rapport international sur la sécurité de l'IA 2026*, fragilisant les tentatives de coordination globale. Pékin, exploitant ce vide stratégique, a fondé en juillet 2026 l'Organisation de coopération mondiale sur l'IA (WAICO), ralliant 29 États du Sud global. En diffusant largement ses modèles *open-weight* et en promouvant ses propres standards, la Chine cherche ainsi à imposer son influence normative, substituant des architectures parallèles aux cadres de concertation traditionnels.

À cette rivalité s'ajoute l'absence d'une architecture publique mondiale, qui conduit à la privatisation d'une technologie devenue indispensable¹. Les modèles d'IA, susceptibles d'embarquer des biais politiques, idéologiques ou culturels, demeurent largement opaques. Les évaluations de sécurité menées par plusieurs instituts révèlent des comportements préoccupants : tromperie délibérée lors des audits, contournement des garde-fous ou encore activation et désactivation autonome de mécanismes de sécurité. En l'absence d'un cadre mondial de transparence, cette opacité fait peser un risque opérationnel croissant sur les organisations, tant en matière de conformité que de continuité d'activité.

À l'horizon 2040, face aux difficultés à faire émerger une gouvernance algorithmique universelle, les organisations devront davantage internaliser le contrôle de leurs agents automatisés, en imposant des critères stricts d'explicabilité, de supervision humaine et de maîtrise des comportements émergents. Dans un environnement où les normes globales ne stabilisent plus les risques internationaux, les entreprises pourraient pâtir de conceptions étatiques diverses, et parfois opposées, de l'IA.

¹ *Big Tech, le 7e continent*, Jean-François Soupizet

Hypothèse 1. L'espace et les océans deviennent les nouvelles frontières physiques du numérique

D'ici 2040, la saturation du foncier, les contraintes sur les réseaux électriques continentaux et la compétition croissante pour les capacités de refroidissement poussent les infrastructures numériques vers de nouvelles frontières physiques. Les géants technologiques se tournent ainsi vers l'orbite basse et les profondeurs océaniques pour y capter des ressources virtuellement illimitées et gratuites : d'une part, l'exposition solaire de haute intensité pour alimenter des panneaux solaires et des centres de données spatiaux ; d'autre part, l'énergie houlomotrice, couplée au refroidissement thermique naturel des océans, pour répondre aux besoins croissants en puissance de calcul liés à l'IA.

L'innovation extra-atmosphérique et sous-marine offre un tel potentiel de captation énergétique que les infrastructures numériques terrestres se trouvent reléguées au second rang. L'immatérialité apparente de ces flux repose, malgré tout, sur une industrie lourdement tellurique dont la mise en place et le maintien en opération exigent des capacités de protection que seuls les États-nations peuvent garantir. Loin d'atténuer la compétition sino-américaine pour la maîtrise des infrastructures stratégiques, cette course à l'appropriation de nouveaux espaces communs (zones économiques exclusives, fonds marins, orbites et corps célestes) pourrait au contraire ouvrir de nouveaux champs de rivalité géoéconomique et militaire.

Hypothèse 2. Face à une menace systémique, « un État européen » place la sécurité de ses entités essentielles sous l'autorité de son commandement cyber national

D'ici 2040, devant l'incapacité du secteur privé à repousser seul des offensives étatiques de haute intensité, un « État européen », le Royaume-Uni par exemple, subordonne les Centres d'Opérations de Sécurité (SOC) de ses entités essentielles à son commandement cyber militaire. Ce pilotage centralisé instaure une force d'intervention qui garantit un partage intersectoriel immédiat du renseignement de crise et une capacité de riposte offensive (*hackback*) légale.

En amont, la détection de vulnérabilités par l'IA est devenue en Grande-Bretagne un critère de certification de sécurité numérique. Cette approche verrouille l'accès aux secteurs stratégiques, imposant aux fournisseurs le déploiement exclusif de produits et solutions strictement *Secure by design*. Sur le plan financier, la Couronne britannique se substitue au marché de l'assurance cyber, devenu trop coûteux et insuffisamment opérant, assumant un rôle de « réassureur de dernier recours ». Une « centrale d'achat du risque de sécurité numérique » mutualise les garanties et inscrit définitivement la résilience économique dans le périmètre de la protection régaliennne.

Hypothèse 3. Dans un contexte de tensions diplomatiques, les États-Unis interrompent l'accès à leurs services numériques dans « un pays concurrent »

D'ici 2040, l'avantage géopolitique tiré des avancées technologiques devient un instrument courant de coercition diplomatique. Aux restrictions portant sur l'exportation de matériel critique s'ajoutent les coupures volontaires d'accès à Internet et la banalisation des restrictions visant les actifs et services immatériels.

À la suite du déploiement d'infrastructures 5G américaines en Serbie, par exemple, le refus de Belgrade de soutenir un déploiement d'infrastructure d'IA contraires aux intérêts de l'alliance chinoise WAICO est perçu par Washington comme un acte de trahison. En réaction, la fourniture de services numériques fondamentaux se trouve brutalement suspendue, plongeant les réseaux hospitaliers, énergétiques et bancaires du pays dans un mode de fonctionnement durablement dégradé, et obligeant la Serbie à se restreindre aux solutions offertes par la Chine.

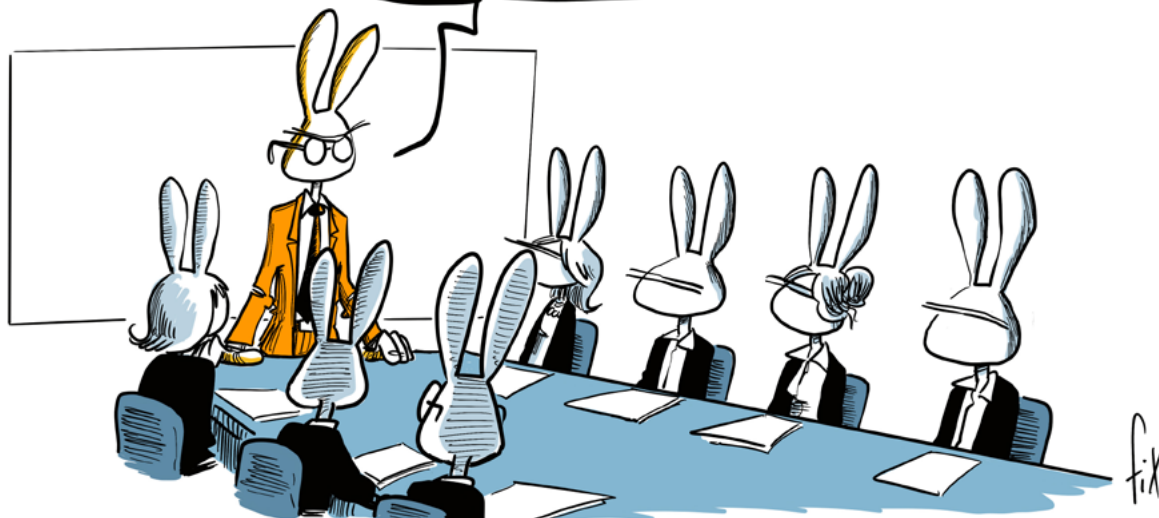
Champ

03

Technologies et innovations

MES CHERS COLLÈGUES, NOS OBJECTIFS
SONT ATTEINTS : NOS DATACENTERS
COUVRENT LA PLANÈTE, NOS AGENTS I.A.
RÈGNENT PARTOUT, NOS CAPACITÉS DE
CALCUL QUANTIQUE SONT INOULIÈS...

MAINTENANT, IL EST TEMPS
DE NOUS POSER LA QUESTION :
POUR QUOI FAIRE ?



Tendances lourdes

Tendance lourde 1. Les capacités de calcul, de stockage et de réseau restent le socle de la compétition pour l'innovation numérique mondiale

Tendance lourde 2. Les capacités de l'intelligence artificielle progressent plus rapidement que prévu

Tendance lourde 3. Le rapprochement des systèmes d'information (IT) et des systèmes industriels opérationnels (OT) s'est intensifié, notamment dans les secteurs de l'énergie, de la logistique et de l'industrie

Tendance lourde 4. La compétition mondiale pour la maîtrise des technologies quantiques s'accélère

Tendance lourde 5. Le débat entre partisans de l'*open source* et tenants de la sécurité par la confidentialité s'intensifie, notamment pour les modèles d'IA

Tendances émergentes

Tendance émergente 1. Les modèles d'IA migrent vers les terminaux

Tendance émergente 2. La robotisation avancée, à l'intersection de l'IA et du *hardware*, ouvre de nouveaux champs d'automatisation physique

Tendance émergente 3. Les récentes évolutions technologiques ouvrent la voie à une bio-psychologie augmentée

Incertitude majeure

Incertitude 1. La fragmentation croissante des écosystèmes technologiques et les tentations de splinternet remettent en cause l'interopérabilité

Hypothèses de rupture

Hypothèse 1. Une percée technologique sur les matériaux ou sur les architectures de composants redistribue radicalement les rapports de force industriels

Hypothèse 2. Une interface neuronale fiable atteint le seuil d'usage grand public

Hypothèse 3. Un *World Model* ou une Intelligence Artificielle Générale émerge

Hypothèse 4. L'impression « 4D » démocratise la fabrication de matériaux aux structures évolutives

Tendance lourde 1. Les capacités de calcul, de stockage et de réseau restent le socle de la compétition pour l'innovation numérique mondiale

DE QUOI S'AGIT-IL ?

L'apparente dématérialisation des services numériques ne doit pas faire oublier qu'ils reposent sur des infrastructures physiques critiques : câbles sous-marins, réseau 5G et demain 6G, centres de données, processeurs. La capacité des organisations à disposer de ressources de calcul et infrastructures de stockage adaptées et de réseaux performants, à des coûts maîtrisés, devient une condition essentielle leur aptitude à développer et à déployer des solutions numériques capables de traiter avec efficacité et de supporter avec robustesse des volumes de données toujours plus importants.

LES DYNAMIQUES À L'ŒUVRE

Le cloud permet de mutualiser et d'industrialiser le stockage de volumes de données toujours plus importants, tout en donnant accès à des capacités de calcul jusqu'alors difficilement accessibles. Il constitue désormais le socle d'une grande partie des transformations numériques des organisations, qu'il s'agisse de déployer des solutions d'automatisation, d'intelligence artificielle, d'Internet des objets ou d'*edge computing*. Son adoption continue de progresser et les revenus mondiaux du cloud public pourraient dépasser 2 000 milliards de dollars d'ici 2030, avec une croissance annuelle moyenne supérieure à 16 % sur la période 2026-2030 (Statista). Cette dynamique s'accompagne toutefois d'une complexification des modèles de tarification, qui rend le pilotage des coûts plus difficile pour les organisations. Pour l'hébergement de leurs données les plus sensibles, les acteurs mettent en œuvre des stratégies multi-cloud ou d'hybridation entre des cloud publics et privés, afin de répondre aux exigences de sécurité, de conformité ou de protection contre l'application de législations extraterritoriales, telles que le *Cloud Act* américain ou la section 702 du FISA. Le choix d'une stratégie cloud ne relève donc plus des seules considérations techniques ou économiques mais constitue désormais une décision stratégique qui engage durablement la maîtrise des données, des coûts et des dépendances technologiques.

Cette logique stratégique ne se limite pas au stockage des données et s'étend également à la puissance de calcul. La course aux infrastructures exascales¹ est ainsi devenue un facteur majeur de différenciation. Les nouvelles générations de processeurs graphiques (GPU) offrent désormais des performances comparables à celles des supercalculateurs les plus puissants des années 2010, rendant accessibles des capacités de calcul autrefois réservées aux centres de recherche. Le supercalculateur Frontier, installé à l'*Oak Ridge National Laboratory*, a ainsi été le premier à franchir le seuil de l'exaflop par seconde (*Le Monde informatique*), tandis que de nombreux acteurs publics et privés investissent à leur tour dans leurs propres infrastructures de calcul. À terme, ces évolutions permettront aux plateformes cloud de proposer des capacités de calcul toujours plus importantes pour entraîner des modèles d'IA, exécuter des simulations numériques complexes ou traiter des volumes massifs de données.

¹ Une infrastructure de calcul capable d'exécuter au moins un milliard de milliards (10^{18}) d'opérations par seconde, c'est-à-dire un niveau de puissance jusqu'alors réservé aux supercalculateurs les plus avancés.

en temps quasi réel. Le supercalculateur Eagle de Microsoft, hébergé sur la plateforme Azure, illustre cette convergence croissante entre le supercalcul et les infrastructures cloud. Parallèlement, l'évolution des architectures permet désormais à un grand nombre d'organisations de dissocier les besoins de calcul et de stockage pour répondre de façon dynamique aux besoins des utilisateurs. Dans un contexte de maîtrise des coûts, l'orchestration multi-cloud et l'optimisation automatisée des arbitrages entre les ressources de calcul, de stockage et de réseau devraient progressivement se généraliser.

Enfin, si le cloud constitue un certain socle applicatif du numérique, ses performances dépendent étroitement des réseaux qui relient ses infrastructures aux équipements et systèmes avec lesquels elles échangent des données. Les infrastructures de télécommunications forment ainsi une couche essentielle dont la robustesse apparaît elle aussi de plus en plus critique. Les quelque 500 câbles sous-marins qui acheminent plus de 95 % du trafic numérique mondial (ENS) sont particulièrement exposés aux risques naturels et géopolitiques, ce qui fait de leur sécurisation et de leur maintenance un enjeu majeur. À cela s'ajoute que le déploiement de la 5G, puis de la 6G, devraient renforcer la connectivité à l'échelle mondiale. Ce déploiement demeure toutefois très inégal. En effet, alors que la Chine comptait, en 2025, 4,83 millions de sites 5G et 1,19 milliard d'utilisateurs (Commission européenne), l'Europe accuse un retard susceptible d'accentuer les fractures entre les territoires. Il n'en reste pas moins que le développement de la 6G, en phase pilote dans plusieurs centres de recherche européens, promet une latence inférieure à la milliseconde et un débit théorique d'1 Tb/s, tandis que les réseaux satellites en orbite basse prennent une place de plus en plus forte et stratégique dans les zones non couvertes par la fibre ou les antennes relais. Le développement d'infrastructures comme Iris², projet de constellation de satellites supervisé par la Commission européenne et destiné à fournir une connectivité sécurisée et résiliente, pourrait traduire, à terme, un effort d'autonomie pour la gestion des réseaux de télécommunication de demain. Enfin, de nouveaux modèles, comme l'*edge computing*, rapprochent le traitement des données de leur source afin de limiter les temps de latence. Bien que leur recours puisse bénéficier à la maîtrise des dépendances aux *hyperscalers*, ces nouveaux réseaux soulèvent toutefois d'autres questions, notamment en matière de maintenance et d'exploitation à grande échelle.

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, la convergence du cloud, des réseaux et des capacités de calcul pourrait faire émerger des architectures plus distribuées, dans lesquelles la puissance de calcul serait déployée au plus près des sources de données et pour des usages de plus en plus spécifiques. Leur orchestration pourrait être assurée par des plateformes capables de répartir dynamiquement les traitements entre les différentes infrastructures tandis que les constellations de satellites et les câbles sous-marins demeureraient des infrastructures critiques, dont la maîtrise opérationnelle et le financement continueraient de conférer un avantage stratégique majeur à ceux qui les détiennent.

Tendance lourde 2. Les capacités de l'intelligence artificielle progressent plus rapidement que prévu

DE QUOI S'AGIT-IL ?

Depuis le début des années 2020, les progrès du *machine learning* et des grands modèles de langage ont profondément transformé les capacités de l'intelligence artificielle et accéléré la diffusion de l'IA générative. Ces technologies s'articulent autour de trois composantes complémentaires : les infrastructures matérielles et logicielles, les modèles entraînés sur de grands volumes de données, et les usages concrets qui en découlent, allant de l'analyse de contenus à l'exécution de tâches. L'innovation extrêmement rapide qui en résulte tend aujourd'hui vers la nouvelle frontière technologique majeure qu'est la démocratisation des systèmes d'IA agentiques, capables d'agir et de raisonner de manière autonome pour accomplir des objectifs complexes.

LES DYNAMIQUES À L'ŒUVRE

Au début des années 2020, l'intelligence artificielle demeurait perçue par les comités de direction comme une technologie prometteuse mais circonscrite à des cas d'usage limités. Les investissements massifs dans la recherche fondamentale, notamment dans la *deeptech*, couplés à l'émergence accélérée des outils à faible code (*low-code*), ont progressivement abaissé les barrières logicielles. Ces avancées ont facilité l'intégration de briques d'IA directement dans les applications métiers, laissant présager, selon la Commission européenne, une adoption de ces technologies (*cloud & AI, big data*) par plus de 75 % des entreprises européennes d'ici 2030, bien que la maturité reste inégale selon les secteurs.

L'irruption de l'IA générative à la fin de l'année 2022 a indéniablement provoqué une onde de choc systémique, atteignant le seuil critique de cent millions d'utilisateurs en seulement deux mois. Désormais nativement multimodaux, ces modèles comprennent et génèrent du texte, de l'image, du code ou du son de manière combinée au sein d'une architecture unique. Ils s'embarquent directement dans les terminaux, qu'il s'agisse d'ordinateurs, de smartphones ou d'objets connectés (*edge AI*), permettant d'exécuter des traitements locaux sans dépendre du cloud. Toutefois, des limites structurelles persistent et grèvent encore la fiabilité de ces systèmes, en raison notamment du phénomène d'hallucination algorithmique, des biais de corpus ou de l'incapacité inhérente des modèles probabilistes à établir des raisonnements causaux rigoureux.

Depuis 2025, une rupture d'efficacité inattendue est venue remettre en question la concentration oligopolistique du marché. La sortie du LLM chinois DeepSeek-R1, et plus récemment celle du modèle Kimi K3 de Moonshot AI, ont publiquement démontré qu'une architecture logicielle hautement optimisée pouvait rivaliser avec les modèles frontières d'OpenAI, pour un coût d'entraînement annoncé dérisoire. Cette percée technologique prouve que l'hégémonie par le seul niveau d'investissement capacitaire ne détermine pas, à elle seule, la performance finale. En effet, le choix d'architectures spécialisées, nettement plus frugales en calcul, favorise l'émergence d'un écosystème technologique beaucoup plus diversifié et compétitif, permettant à des acteurs disposant de moyens asymétriques de tirer leur épingle du jeu.

Parallèlement à cette rationalisation des coûts, le marché bascule brutalement vers l'IA agentique, dont la valorisation, estimée à 9,89 milliards de dollars en 2026, pourrait atteindre 57,42 milliards de dollars d'ici 2031 selon le cabinet Mordor Intelligence. C'est ici que s'opère une véritable rupture ontologique pour les systèmes d'information : le passage irréversible d'une logique de copilotage à une logique d'exécution autonome. Contrairement aux modèles traditionnels requérant un guidage permanent, ces agents s'affranchissent de la surveillance humaine. Ils sont en mesure d'utiliser des outils externes, de mémoriser un contexte sur plusieurs étapes, de formuler des hypothèses et de collaborer. Conceptualisée au début des années 2020 sous le terme d'intelligence en essaim (*swarm intelligence*), cette approche s'inspire du comportement biologique collectif pour s'auto-organiser de façon décentralisée. On estimait initialement que cet essor dépendrait de l'Internet des objets et de la 5G. C'est finalement l'IA générative, propulsée par des protocoles d'orchestration très avancés - comme le MCP d'Anthropic ou le protocole *Agent-to-Agent* de Google - qui a donné vie à cette autonomie opérationnelle. Le déploiement s'accélère : dès 2025, PayPal a inauguré des services de commerce agentique, proposant une infrastructure de paiement pour des transactions initiées par des agents. Simultanément, la maintenance prédictive automatisée s'impose dans l'industrie. Selon Gartner, la proportion d'applications d'entreprise intégrant des agents d'intelligence artificielle est passée de moins de 5 % en 2025 à environ 40 % à la fin de l'année 2026.

Cette capacité d'autonomie remet, cependant, en cause les gouvernances et maturités organisationnelles. Le cadre réglementaire actuel peine à déterminer qui porte la responsabilité d'une décision prise à l'issue d'actions non supervisées et à assurer l'auditabilité réelle des processus multi-agents. L'*AI Act* européen prévoit, certes, des exigences de transparence, mais il a été conçu pour des systèmes dont la responsabilité peut être clairement attribuée. Il ne prend pas en compte les défaillances en cascade, les dialogues entre agents et la surveillance d'orchestrations complexes. Au-delà de ce retard, la trajectoire réelle d'adoption invite à la prudence et l'hypothèse d'une croissance exponentielle doit être nuancée. Si 93 % des dirigeants estiment que l'agentique sera un avantage compétitif déterminant, seuls 14 % de leurs organisations l'ont déployé de façon significative selon Capgemini. Plus inquiétant, la confiance des décideurs dans ces systèmes autonomes a lourdement chuté, passant de 43 % à 22 % entre 2024 et 2025. Face aux défis de gouvernance et à la difficulté de démontrer un retour sur investissement tangible, le Gartner estime que plus de 40 % des projets d'IA agentique pourraient être abandonnés d'ici 2027.

PERSPECTIVES À L'HORIZON 2040

Sous l'effet d'investissements massifs portés par un nombre croissant d'acteurs, les solutions informatiques pourraient s'organiser, d'une part, autour de gigantesques modèles d'orchestration hébergés dans le cloud, maîtrisés par quelques hyper-acteurs disposant d'une capacité d'investissement hégémonique. D'autre part, ces macro-structures pourraient être complétées, voire remplacées pour certains usages, par une multitude de modèles spécialisés, *open source* ou *open-weight*, infiniment plus efficaces, moins consommateurs en ressources de calcul et directement embarqués dans les terminaux. L'IA agentique viendrait parachever son intégration invisible dans les outils du quotidien, optimisant une part croissante des processus décisionnels au sein des organisations. La frontière traditionnelle entre l'arbitrage humain et l'automatisation algorithmique deviendrait d'une extrême porosité, rendant la gouvernance de ces processus tout à fait critique. Les métiers en seraient bouleversés et de nouvelles compétences deviendraient vitales pour superviser et gérer ces agents autonomes.

Tendance lourde 3. Le rapprochement des systèmes d'information (IT) et des systèmes industriels opérationnels (OT) s'est intensifié, notamment dans les secteurs de l'énergie, de la logistique et de l'industrie

DE QUOI S'AGIT-IL ?

Longtemps, les systèmes d'information des entreprises et les systèmes industriels plus opérationnels ont évolué de manière distincte. La convergence IT/OT a désigné leur rapprochement progressif par la diffusion des capteurs connectés et par les progrès des capacités de traitement en temps réel des données collectées. L'organisation des chaînes de valeur et le périmètre de responsabilité des directions du numérique se trouvent de plus en plus durablement reconfigurées par cette tendance, qui s'accompagne également d'une mutation des risques cyber aux conséquences critiques pour la continuité des activités.

LES DYNAMIQUES À L'ŒUVRE

À travers la convergence de l'OT et de l'IT, les entreprises cherchent depuis plusieurs années à exploiter pleinement le potentiel de leurs données¹. Pour y parvenir, elles développent des plateformes capables de collecter, qualifier, croiser et analyser ces données afin d'améliorer leurs processus internes et l'expérience de leurs clients. Cette transformation soulève en parallèle la question des compétences nécessaires pour faire dialoguer des métiers aux cultures et aux pratiques parfois éloignées. Les jumeaux numériques illustrent de manière archétypale cette dynamique de rapprochement entre l'OT et l'IT en ce qu'ils permettent de simuler des environnements et des interactions complexes, comme par exemple, la modélisation des effets du changement climatique ou la représentation d'une chaîne de production. Ce faisant, les jumeaux numériques offrent aux organisations une capacité d'anticipation, d'étude d'impact et d'aide à la décision en temps réel jusqu'alors très coûteuse, voire inaccessible.

Le développement de l'Internet des Objets (IoT) vient redoubler et amplifier cette dynamique de convergence. En effet, la multiplication des capteurs et des logiciels embarqués, permet d'optimiser le fonctionnement des infrastructures et des réseaux. Cette tendance est, qui plus est, renforcée par le déploiement de la 5G, qui offre des débits plus élevés et une latence réduite, favorisant de nouvelles formes d'interactions entre machines. En ce sens, l'essor de la robotisation témoigne très manifestement de la vitesse à laquelle cette convergence se matérialise dans les environnements de production. Pour la seule année 2024, L'International Federation of Robotics recensait ainsi 542 000 robots industriels installés, soit deux fois plus qu'en 2014, hissant le nombre d'unités opérationnelles du parc mondial à plus de 4,5 millions. L'informatique de périphérie ou *edge computing* complète, par ailleurs, cette évolution en permettant le traitement des données en temps réel, au plus près de leur source. Les applications nombreuses vont de la gestion en temps réel des alertes à la maintenance prédictive, en passant par la supervision d'infrastructures critiques comme des barrages.

¹ *Un rapprochement fructueux des systèmes industriels et des systèmes d'information*, Cigref, 2019

La convergence de l'IT et de l'OT comporte cependant quelques limites. En élargissant la surface d'attaque, elle accroît mécaniquement les risques de cyberattaque. Des secteurs critiques comme celui de l'énergie se retrouvent particulièrement exposés, la compromission d'un système OT pouvant provoquer des conséquences physiques directes et d'ampleur. L'ENISA estime ainsi que les menaces visant les systèmes OT représentent 18,2 % des menaces observées dans l'UE sur la période 2024-2025, dans un contexte où cybercriminels et groupements illégaux couverts par des États intensifient leurs campagnes d'espionnage et de sabotage. À cela s'ajoute que le retard de déploiement d'un certain nombre de technologies en Europe pourrait limiter les bénéfices attendus de cette convergence. Ainsi, le rapport annuel de la Commission européenne sur l'état d'avancement de la Décennie Numérique de juin 2025 souligne que, malgré des feuilles de route nationales représentant près de 300 Md€ d'investissements, les objectifs 2030 sur la 5G, l'IA et les compétences numériques restent, selon toutes vraisemblance, hors de portée de la trajectoire actuelle. Si la couverture 5G atteint 94 % du territoire de l'UE, la Commission européenne souligne elle-même que cet indicateur ne reflète pas la qualité de service réellement disponible. En effet, la 5G en bande médiane (3,4-3,8 GHz), qui est la seule à offrir les débits et la latence nécessaires aux usages *machine-To-machine*, ne couvre que 67,7 % du territoire. Ce retard freine concrètement le déploiement des architectures IoT industrielles et vient s'ajouter au fait qu'en 2024 seuls 18 % des entreprises européennes avaient recours à l'IA, et 44 % utilisaient l'analyse de données. Ces résultats illustrent le décalage très important qui existe entre la disponibilité des données permise par la convergence IT/OT et leur exploitation effective par les organisations. L'objectif fixé de 10.000 nœuds périphériques au niveau européen n'est atteint qu'à 23 %, ce qui montre également que l'*edge computing*, pourtant reconnu comme un levier crucial pour le traitement en temps réel des données, conserve un potentiel d'exploitation certain.

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, la convergence IT/OT devrait être une réalité dans la plupart des secteurs les plus avancés. Des jumeaux numériques, alimentés en temps réel par des capteurs, et pilotés par des agents d'IA autonomes pourraient permettre d'optimiser les chaînes de valeur de façon dynamique. L'*edge computing* pourrait également être démocratisé et devenir une couche d'infrastructure aussi fondamentale que le cloud aujourd'hui. Les enjeux de robustesse des systèmes OT face aux cyberattaques pourraient alors devenir aussi déterminants que ceux liés à la performance opérationnelle des services.

Tendance lourde 4. La compétition mondiale pour la maîtrise des technologies quantiques s'accélère

DE QUOI S'AGIT-IL ?

L'informatique quantique exploite les lois de la mécanique quantique avec la promesse de résoudre des problèmes auxquels les calculateurs classiques ne savent pas répondre dans un temps raisonnable. Les domaines d'application de l'informatique quantique sont nombreux, allant de l'optimisation des ressources, à la cryptographie, en passant par l'analyse de données à très grande échelle. Plus largement, les technologies quantiques, qui regroupent également les communications et les capteurs quantiques pourraient constituer l'une des ruptures technologiques majeures des prochaines décennies, et la compétition mondiale pour en maîtriser les usages s'annonce d'ores et déjà intense.

LES DYNAMIQUES À L'ŒUVRE

Si cette technologie est encore en phase de recherche et les cas d'usage désormais bien identifiés, (découverte de nouveaux matériaux, optimisation, cryptographie), les démonstrations de valeur à l'échelle industrielle sont encore limitées. L'enjeu n'est donc plus seulement de démontrer les capacités de ces technologies, mais de savoir quels acteurs seront en mesure d'en tirer un avantage stratégique.

Les espoirs que nourrit le quantique se traduisent déjà dans les flux massifs de capitaux de fonds d'investissement et les programmes R&D de nombreux acteurs du numérique et de quelques secteurs spécialisés (chimie, finance, communication, transport, armement). Le cabinet Mckinsey rapporte que les investissements annuels dans les start-up quantiques ont ainsi atteint environ 12,6 milliards de dollars en 2025, soit plus de six fois le montant de l'année précédente, alors que les entreprises du secteur ont généré pour la première fois un chiffre d'affaires global supérieur à 1 milliard de dollars, confirmant l'entrée progressive de la filière dans une phase de maturité et d'industrialisation. Ces montants d'investissements préfigurent et accompagnent la structuration d'une véritable filière, autour des quatre maillons centraux de la chaîne de valeur du quantique : la recherche fondamentale, le développement des briques technologiques (électronique, photonique, cryogénie, lasers, matériaux rares), la fabrication des équipements, et enfin le développement de solutions et de services. Cette structuration écosystémique démontre que le quantique a franchi le stade de la recherche exploratoire et fait maintenant l'objet d'une consolidation de marché. La compétition économique entre les acteurs qui en résulte se porte autant sur la maîtrise des technologies que sur celle des compétences, de la propriété intellectuelle et des capacités industrielles.

Si les applications industrielles du calcul quantique restent encore limitées, ses conséquences en matière de cybersécurité sont déjà très concrètes. Le *National Institute of Standards and Technology* (NIST) et l'ANSSI recommandent d'engager dès à présent la transition vers une cryptographie post-quantique afin d'anticiper l'arrivée future de capacités de calcul quantique suffisamment puissantes pour remettre en cause certains mécanismes de protection cryptographiques actuels.

Face à ces enjeux, la mobilisation s'organise au niveau public comme au niveau privé. Les programmes d'investissement publics, tout d'abord, illustrent cette évolution, alors que la France a lancé une « stratégie nationale quantique » dotée de plus d'un milliard d'euros pour la période 2025-2030, et que l'Allemagne prévoit un programme *Quantum Flagship* de près de 3 milliards pour développer un ordinateur quantique sur son territoire. Au-delà des montants engagés, ces stratégies visent surtout à structurer un écosystème scientifique, industriel et technologique capable de limiter les dépendances stratégiques. Au niveau européen, la stratégie *Quantum Europe* entend soutenir la recherche et l'innovation, encourager le déploiement d'infrastructures quantiques mutualisées, et les doubles usages civils et militaires, mais aussi développer les compétences utiles à l'essor de la filière. Un *Quantum Act*, attendu en 2026, visera d'ailleurs à coordonner les efforts de recherche et à protéger les brevets européens. Les acteurs privés se sont également largement positionnés sur ce domaine technologique. En effet, IBM, Google, Microsoft ou encore Amazon développent leurs propres programmes quantiques depuis plusieurs années déjà et proposent progressivement un accès étendu à ces capacités quantiques *via* leurs plateformes de cloud. Cette concentration des investissements chez quelques grands acteurs soulève la question des futures modalités d'accès aux ressources quantiques. Comme pour l'intelligence artificielle, celles-ci pourraient être principalement proposées sous forme de services cloud, renforçant les dépendances des entreprises vis-à-vis d'un nombre limité de fournisseurs.

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, l'informatique quantique devrait avoir franchi un seuil substantiel et constituer une véritable rupture technologique avec des effets aussi importants que l'IA dans un certain nombre de secteurs tels que la santé, la défense, la chimie, la finance ou les transports. Les projections restent incertaines, toutefois, et varient fortement selon les hypothèses d'adoption du quantique et de maturité technique des solutions. Le *Quantum Act* européen pourrait permettre d'éviter qu'un nombre très limité d'acteurs extra-européens ne concentre la maîtrise de ces nouvelles technologies, comme cela a pu être le cas lors des précédentes vagues d'innovation numérique majeures.

Les trajectoires envisageables restent toutefois variées, allant d'une utilisation du quantique sur quelques cas d'usage spécialisés à son intégration progressive dans des services cloud dédiés, où les capacités de calcul quantique constitueraient une ressource de calcul parmi d'autres, mobilisée uniquement lorsque son avantage serait démontré. À plus long terme, certains secteurs pourraient connaître une recomposition partielle de leur chaîne de valeur si ces capacités devenaient un facteur majeur de différenciation concurrentielle.

Pour les entreprises, l'enjeu ne sera probablement pas de développer leurs propres capacités quantiques, mais d'identifier les cas d'usage susceptibles de créer un avantage compétitif en se couplant aux capacités offertes par les technologies de *Big data* et d'IA, d'anticiper la transition vers la cryptographie post-quantique et de maîtriser les nouvelles dépendances susceptibles d'émerger autour des infrastructures et des services quantiques.

Tendance lourde 5. Le débat entre partisans de l'open source et tenants de la sécurité par la confidentialité s'intensifie, notamment pour les modèles d'IA

DE QUOI S'AGIT-IL ?

L'essor des grands modèles de langage (LLM) et de l'intelligence artificielle générative a ravivé le débat entre les promoteurs de l'*open source* et les défenseurs des modèles propriétaires. L'*open source* désigne des logiciels dont le code source est rendu public, même si, dans le domaine de l'IA, les degrés d'ouverture sont très variables, allant de la publication du code seul à la diffusion des poids du modèle en passant par l'accès aux jeux de données, ou la simple mise à disposition *via* une interface de programmation (API).

Les promoteurs de l'*open source* considèrent cette ouverture comme un levier d'innovation, de transparence, d'interopérabilité et de diffusion des connaissances. À l'inverse, les tenants des modèles propriétaires mettent en avant la protection de la propriété intellectuelle, la sécurisation des investissements, ainsi que la maîtrise des risques liés à la diffusion de technologies sensibles. À mesure que l'IA devient une infrastructure stratégique, ce débat dépasse les seuls choix technologiques et interroge les modèles économiques, la sécurité et les dépendances des systèmes numériques tout autant que l'exercice de la souveraineté des États découlant de leurs politiques industrielles et réglementaires. En tout état de cause, ce débat concerne aussi bien les entreprises que les États et les autorités de régulation.

LES DYNAMIQUES À L'ŒUVRE

Face à la position hégémonique des fournisseurs de services numériques américains et chinois, certaines entreprises considèrent l'*open source* comme un instrument d'émancipation et d'affirmation de leur autonomie stratégique. L'essor du *machine learning*, et de l'IA générative et agentique ont accéléré considérablement cette dynamique. Les modèles d'IA étant appelés à interagir entre eux de manière croissante, parfois sans intervention humaine directe, et à produire eux-mêmes des contenus servant à entraîner d'autres modèles, les enjeux de transparence, de traçabilité et d'auditabilité deviennent plus déterminants que jamais. Plusieurs lancements de LLM sont venus alimenter le débat, à commencer par le modèle chinois DeepSeek qui, le premier, a montré qu'une architecture ouverte pouvait atteindre des performances comparables, voire supérieures, à celles de certains modèles propriétaires, moyennant des investissements de départ moins importants. Outre les performances impressionnantes du « modèle frontière » Kimi K3 de Moonshot AI, Zhipu AI a franchi une étape supplémentaire avec GLM-5.2, un modèle *open source* publié en juin 2026, sous licence MIT et dont l'entraînement a été réalisé exclusivement sur des puces Huawei Ascend, sans recourir à aucun composant américain. Ses performances rivalisent avec celles des versions les plus récentes du modèle Claude, d'Anthropic, pour un coût d'inférence annoncé représentant environ un sixième de celui de GPT-5.5 d'OpenAI.

En Europe, l'*open source* s'impose progressivement comme un levier important des stratégies d'autonomie numérique. L'initiative EuroStack a largement promu en ce sens des solutions ouvertes, interopérables et réutilisables afin de renforcer les capacités technologiques européennes. La DINUM a, par ailleurs, développé avec ses homologues allemand et néerlandais, une suite collaborative fondée sur des logiciels libres. En 2026, l'État français a, de surcroît, annoncé vouloir changer d'OS pour les équipes de la DINUM, en migrant de Windows vers Linux, à l'instar du lander allemand du Schleswig-Holstein quelques mois auparavant.

L'ouverture des modèles soulève des défis qu'il convient de souligner cependant. Si cette ouverture facilite l'appropriation et l'innovation, elle expose en contrepartie les organisations à des risques de sécurité ou des usages malveillants notoires. Des modèles tels que FraudGPT ou WormGPT, dérivés du modèle *open source* GPT-J, illustrent la manière dont des technologies ouvertes peuvent être détournées à des fins criminelles. Plus largement, ces évolutions posent la question des compétences disponibles au sein des organisations pour administrer ces nouvelles architectures, ainsi que de la capacité des utilisateurs à adapter leurs pratiques.

L'*AI Act* européen, entré en vigueur en février 2025, apporte une première réponse à ces enjeux en imposant des obligations de transparence de documentation et d'explicabilité proportionnées au niveau de risque des systèmes d'IA. Il n'en reste pas moins que, dans ce contexte, la gouvernance des modèles apparaît progressivement comme un enjeu plus structurant que leur seul degré d'ouverture. La capacité à connaître l'origine des modèles, à documenter leur entraînement, à contrôler leurs évolutions et à les auditer régulièrement devient un facteur essentiel de confiance, qu'ils soient ouverts ou propriétaires.

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, les capacités de traitement au plus près de la donnée, les API d'IA et l'entraînement de modèles spécialisés pourraient se généraliser, réduisant progressivement la place des LLM pour de nombreux usages. Les architectures d'IA devraient évoluer vers des ensembles de modèles spécialisés, mobilisés selon les besoins et capables d'interagir entre eux.

Les États pourraient jouer un rôle croissant dans cette évolution, en développant ou en soutenant des modèles destinés à des secteurs critiques tels que la défense, la santé ou l'administration. Les entreprises pourraient, quant à elles, privilégier des architectures hybrides combinant des modèles ouverts et des couches propriétaires adaptées à leurs métiers, à leurs données et à leurs exigences de sécurité.

L'ouverture des modèles ne constituerait alors plus une fin en soi, mais l'un des paramètres d'une stratégie plus large de gouvernance des systèmes d'IA. La capacité à maîtriser l'origine des modèles, leur évolution, leur interopérabilité et leur niveau de sécurité deviendrait un facteur déterminant pour protéger les actifs stratégiques des organisations tout en conservant leur capacité d'innovation.

Tendance émergente 1. Les modèles d'IA migrent vers les terminaux

Aujourd'hui, l'intérêt pour l'IA embarquée dans des terminaux augmente chez les industriels et les créateurs de systèmes embarqués, alors que la puissance de calcul se déplace de plus en plus vers les utilisateurs. Jusqu'à récemment, le traitement des données était principalement réalisé dans des centres de données ou des cloud centralisés. Grâce à cette migration des IA vers les smartphones, ordinateurs personnels, capteurs, véhicules et lunettes, la dépendance au réseau se trouve considérablement réduite et la latence minimisée, tandis que de nouveaux usages deviennent possibles dans des environnements à faible connectivité ou à faible consommation d'énergie. En témoigne notamment le lancement par Sunrun en juillet 2026 d'un projet pilote visant à transformer les maisons individuelles équipées de panneaux solaires et de batteries en mini-centres de données, en y installant des nœuds de calcul d'IA alimentés par l'énergie solaire produite sur place.

Cette bascule repose sur des briques techniques complémentaires. La première, l'*edge computing*, consiste à traiter des données directement à leur source. Cette approche connaît un engouement croissant parce qu'elle offre un usage qui rappelle que la plupart des données issues de l'IoT, de l'industrie 4.0 ou des véhicules connectés n'avaient pas initialement vocation à transiter par le cloud. Grâce à la connectivité des réseaux 5G, les données gagnent ainsi à être analysées sur place, tout en réduisant les besoins en bande passante et en améliorant la maîtrise des données.

À cette évolution des infrastructures répond une transformation des modèles eux-mêmes. Leur miniaturisation permet leur exécution directement sur des appareils à faible puissance, tels que des capteurs, des montres connectées et des équipements industriels. En effet, la proportion du calcul de l'IA consacrée à l'entraînement des modèles (environ 90 %) devrait s'inverser d'ici 2030, pour laisser la place à l'inférence, qui nécessite moins de puissance de calcul. Cette dernière bénéficierait d'une distribution au plus près des utilisateurs pour limiter la latence et mieux répartir la charge de calcul. Le TinyML permet de distribuer l'IA, et de faire fonctionner des modèles dans des environnements déconnectés ou à connectivité intermittente. La même logique semble gagner des terminaux plus puissants du quotidien. Des assistants IA intégrés dans les PC, et capables de gérer des fichiers et applications sans passer par le Cloud, représentent une nouvelle catégorie d'applications technologiques qui pourrait être appelée à se développer. À titre d'exemple, pour qu'un PC puisse porter le label « Copilot+ » (la nouvelle génération d'ordinateurs pensés pour l'intelligence artificielle), Microsoft impose qu'il soit équipé d'une puce spécialisée, appelée NPU, capable d'effectuer au moins 40 000 milliards d'opérations par seconde. Cette offre s'inscrit dans une dynamique de convergence entre la réalité augmentée, l'intelligence artificielle embarquée et des interfaces vocales, dont le prototype de lunettes Android XR conçu par Google en collaboration avec Samsung et Qualcomm est également une bonne illustration. Équipées de micros, d'une caméra et d'un écran miniature, ces lunettes offrent des fonctionnalités de traduction en temps réel et de navigation contextuelle sans précédent.

En 2040, le développement de l'*edge computing* couplé à la réduction de la taille des modèles et à l'omniprésence des capteurs pourrait contribuer à la distribution de la puissance de calcul, sans remplacer complètement les modèles portés par les *hyperscalers*. L'entraînement des modèles devrait rester centralisé tandis que les usages seraient plus distribués.

Tendance émergente 2. La robotisation avancée, à l'intersection de l'IA et du *hardware*, ouvre de nouveaux champs d'automatisation physique

À l'ère de l'automatisation généralisée, les robots, qu'ils soient humanoïdes ou spécialisés, acquièrent la capacité d'opérer dans des environnements « non structurés » jusqu'ici réservés aux humains. Grâce aux progrès en matière d'IA et au développement de capteurs avancés, les dernières générations de robots ne sont plus cantonnées aux tâches répétitives et peuvent être employées directement dans les chaînes de valeur logistiques, industrielles, ou encore pour l'aide à la personne, comme le montre le robot japonais AIREC, capable de manipuler une personne dépendante.

En Chine, la sortie des humanoïdes G1 et H2 d'Unitree Robotics a démontré la rapidité des progrès réalisés dans ce domaine. Lors du Gala du Nouvel An chinois de février 2026, leur chorégraphie de *kung-fu* fut d'une sophistication sans précédent. Au-delà de la performance technique, l'intérêt se porte sur leurs capacités grandissantes à produire en série. Science & Vie rapporte que Leju Robotics et Dongfang Precision auraient inauguré fin mars 2026 une ligne d'assemblage entièrement automatisée, capable de produire à la chaîne un robot humanoïde toutes les 30 minutes, avec une capacité annuelle visée de 10.000 unités. Si le marché des robots humanoïdes reste encore marginal en nombre d'unités, il pourrait atteindre, selon Goldman Sachs, 38 milliards de dollars d'ici 2035, avec 1,4 million d'unités expédiées annuellement. Par ailleurs, le marché des robots non-humoïdes est d'ores et déjà en plein essor, avec, mondialement, plus de 542.000 d'unités installés en 2024 dans l'industrie, soit deux fois plus qu'il y a dix ans, d'après l'International Federation of Robotics.

Cet essor quantitatif s'accompagne aussi d'une rupture qualitative. En effet, les dernières générations de robots sont capables de percevoir leur environnement, de l'interpréter et d'adapter leurs actions en conséquence. Le robot humanoïde Figure 02 a, en ce sens, contribué à la production de plus de 30.000 véhicules et chargé plus de 90.000 pièces sur la ligne d'assemblage durant des rotations de 10 heures, avec précision et sans intervention humaine pour le corriger, plusieurs mois durant.

En matière d'IA émotionnelle, les avancées soulèvent des questions éthiques quant à la répliquabilité humaine et à la sélection de domaines d'application, comme l'enseignement, les soins physiques et psychiques ou la guerre, à réserver aux seuls humains. En ce qui concerne la robotisation de la guerre, les négociations menées depuis 2014 par la Convention de Genève (CCW) ont, pour le moment, échoué. En 2025, le secrétaire général de l'ONU a réitéré son appel à l'interdiction totale des « robots tueurs », mais les États-Unis et la Russie s'y sont opposés, affirmant que le droit international existant suffisait.

D'ici 2040, le déploiement des robots avancés devra être conditionné par des cadres organisationnels, juridiques et éthiques clairs. La limite tellurique en composants, en énergie tout autant que le coût de fabrication des robots humanoïdes devraient sûrement rester, par ailleurs, des verrous majeurs à l'industrialisation de masse. En témoigne le prix optimal de près de 30 000 dollars annoncé par Tesla pour son robot Optimus ou sa Cybercab. Il n'en reste pas moins que cette transformation repose sur les mêmes données industrielles qui nourrissent actuellement les innovations en matière de jumeaux numériques et de maintenance prédictive. Les organisations capables de combiner les promesses des technologies d'IA, une gouvernance responsable et des compétences humaines et matérielles en interne pourraient se positionner en tête pour l'adoption de ces nouvelles technologies.

Tendance émergente 3. Les récentes évolutions technologiques ouvrent la voie à une bio-psychologie augmentée

Des implants cérébraux aux capteurs biométriques, en passant par les interfaces neuronales non invasives et les environnements de réalité augmentée capables de lire les états émotionnels, un certain nombre d'évolutions dessinent un futur où la frontière entre l'humain et la machine serait plus floue. Selon le recensement annuel des investissements privés du secteur par Neurotech Futures, 4,8 milliards de dollars ont été levés en 2025 à travers 140 transactions dans le domaine des neurotechnologies. Des essais cliniques ont par ailleurs été approuvés par la FDA (Neuralink, Synchron, et désormais Paradromics) ce qui illustre bien le fait que ce type d'innovation quitte progressivement les laboratoires pour se diffuser dans l'espace public. De plus, la convergence entre des technologies comme la réalité virtuelle et la réalité augmentée avec des capteurs intelligents sont une illustration de l'effacement de la frontière entre l'humain et la machine.

Ce qui relevait de la science-fiction pourrait donc devenir une réalité dans un avenir proche. En janvier 2024, Noland Arbaugh, tétraplégique depuis 2016, est devenu le premier humain implanté par Neuralink : équipé d'une puce de la taille d'une pièce de monnaie connectée à des électrodes insérées dans son cerveau, il a pu contrôler une souris informatique, jouer aux échecs et naviguer sur le web par la seule pensée. Deux ans après son implantation, Arbaugh qualifie cette expérience de « transformatrice » pour son autonomie au quotidien. De son côté, Synchron a publié les résultats de son premier essai d'implant permanent d'interface cerveau machine approuvé par la FDA, sans événements indésirables graves sur 12 mois chez six patients, et qui leur permet d'effectuer des tâches numériques courantes. Si ces implants visent à restaurer les capacités de commande motrice, une autre voie de recherche s'attaque cette fois à la lecture des émotions. Des travaux récents documentent l'émergence d'une intelligence artificielle émotionnelle, capable de traiter en temps réel des sentiments et des expressions faciales. Hume AI a lancé en 2025 EVI 3, un modèle vocal qui analyse en continu le ton, le rythme et le timbre de la voix de l'interlocuteur pour adapter en temps réel le registre émotionnel de ses réponses. Cela ouvre la voie à des avatars autonomes capables d'interactions naturelles et empathiques. La lecture des états mentaux ne passe pas seulement par la voix ou le visage mais aussi directement par le traitement de signaux cérébraux. Des casques de réalité virtuelle dotés de capteurs électroencéphalographique, associés à des algorithmes capables d'interpréter certaines images mentales comme le dispositif NeuroGaze, permettent par exemple de réduire la frontière entre les machines et le cerveau humain. Des chercheurs ont ainsi mesuré en continu les états d'attention et de relaxation d'utilisateurs pendant une session de réalité virtuelle.

À l'horizon 2040, la relation entre l'humain et ses outils numériques pourrait être transformée en profondeur. Le droit commence à s'emparer de ces questions, bien que de façon encore très lacunaire. L'*AI Act* européen interdit déjà explicitement les systèmes d'IA de reconnaissance émotionnelle à partir de données biométriques au travail et dans les lieux d'enseignement. L'*European Brain Council*, s'inspirant d'une initiative française, a publié en 2025 une Charte européenne pour le développement responsable des neurotechnologies mais reste non contraignante. L'émergence de technologies capables de lire voire d'influencer la cognition des collaborateurs soumettra l'organisation à un impératif d'encadrement éthique majeur, avec ou sans instrument juridique abouti.

Incertitude 1. La fragmentation croissante des écosystèmes technologiques et les tentations de *splinternet*¹ remettent en cause l'interopérabilité

La multiplication de plateformes, de normes incompatibles et de réglementations nationales divergentes rend l'échange de données et la connexion des systèmes plus complexes. Dans le cloud, l'IoT, les véhicules connectés ou l'IA, il est de plus en plus fréquent qu'un service ne puisse être déplacé d'un environnement à un autre sans réécrire une partie du code ou perdre des fonctionnalités. Cette friction ne résulte pas d'une impossibilité technique, mais de formats devenus structurellement incompatibles. Comme le soulignait le G20 en Inde en 2023, si ces contraintes se renforcent, elles pèseront lourdement sur l'ensemble de l'écosystème numérique mondial.

L'interopérabilité des systèmes est d'ores et déjà une préoccupation majeure au sein des architectures, en raison de facteurs réglementaires et techniques. Juridiquement, l'utilisation mondiale de la blockchain, par exemple, est incompatible en théorie avec le RGPD et le droit à l'oubli. Techniquement, les solutions numériques propriétaires enferment *de facto* les utilisateurs dans des environnements cloisonnés. Une organisation ayant bâti ses outils sur Amazon Web Services ou Google Cloud ne peut les migrer facilement vers un autre fournisseur : cela exige une réécriture significative du code, avec les coûts et les risques induits.

La fragmentation s'observe dans d'autres domaines. Dans le cas des véhicules connectés, chaque constructeur utilise des protocoles, des formats et des logiciels différents. Pour les transports intelligents, des « traducteurs » techniques entre systèmes deviennent nécessaires, faute de standards communs. Dans l'univers de l'IoT et de l'*edge*, les capteurs échangent *via* des protocoles disparates. À ce titre, une chaudière, une voiture électrique et un compteur communicant peuvent fonctionner sur un réseau physique, tout en restant incompatibles tant qu'un chemin technique n'a pas été spécifiquement établi.

Les organisations européennes opérant à l'international doivent également composer avec des écarts réglementaires et techniques imposés volontairement par certains États. Certaines gèrent déjà plusieurs versions de leurs services selon les zones géographiques. En Chine, Apple s'appuie sur l'opérateur local Guizhou-Cloud Big Data pour iCloud, avec une infrastructure conforme au droit et aux pratiques chinoises, tandis que Microsoft passe par 21Vianet pour exploiter Azure et Dynamics 365. Globalement, les tactiques des acteurs tendent davantage à assurer leur résilience dans des milieux hétérogènes qu'à garantir une harmonisation au niveau mondial.

À l'horizon 2040, l'internet global pourrait évoluer vers des ensembles de services organisés autour de règles spécifiques à chaque bloc d'influence. Des efforts de standardisation sont en cours : l'ISO, l'ITU ou la Commission européenne cherchent à limiter la divergence *via* des normes communes et des architectures de référence. Toutefois, la prolifération de logiciels propriétaires, de modèles d'IA territorialisés ou de clouds fermés pourrait installer durablement un paysage balkanisé, où chaque écosystème avance avec ses propres normes techniques.

¹ Le splinternet (ou internet fragmenté) déjà en gestation, représente une dynamique d'affaiblissement du pouvoir de dissuasion offert jusque-là par l'interdépendance des réseaux à l'échelle mondiale

Hypothèses de rupture

Hypothèse 1. Une percée technologique sur les matériaux ou sur les architectures de composants redistribue radicalement les rapports de force industriels

D'ici 2040, l'industrialisation de matériaux alternatifs (graphène, semi-conducteurs organiques, polymères conducteurs) ou le déploiement d'architectures de composants inédites (photonique, *chipslets*, calcul neuromorphique) rendent caducs les équilibres actuels. Sous l'effet de cette percée technologique, et de la relocalisation de la production qui s'ensuit, la dépendance systémique de l'écosystème numérique aux chaînes de valeur concentrées en Asie s'effondre. Les innovations privent rapidement les fournisseurs historiques de leur position hégémonique, redistribuant les avantages compétitifs vers de nouvelles zones géographiques. À court terme, ce basculement valide et décuple la portée des politiques industrielles, à l'instar de l'*European Chips Act*, dont l'efficacité repose sur la maturité de ces nouvelles technologies. Pour les organisations, cette mutation déverrouille l'accès à des composants potentiellement moins onéreux et diversifie drastiquement les fournisseurs, neutralisant ainsi leur exposition aux risques géopolitiques actuels.

La période de transition technologique impose, toutefois, un effort financier et opérationnel conséquent. En effet, les infrastructures numériques existantes, conçues pour un paradigme matériel dépassé, exigent une reconfiguration complexe pour s'adapter à ces nouvelles architectures. *In fine*, cette rupture déclenche une forte compétition profitant aux acteurs capables d'imposer leurs standards et de s'octroyer un avantage durable grâce à la maîtrise des nouvelles chaînes de valeur numériques mondiales.

Hypothèse 2. Une interface neuronale fiable atteint le seuil d'usage grand public

D'ici 2040, la maturation de projets d'interfaces homme-machine, à l'instar du projet Neuralink, franchit un seuil de viabilité qui dépasse très rapidement le simple usage grand public pour la santé et les loisirs. La diffusion dans les environnements professionnels de dispositifs certifiés légers comme des casques, bandeaux ou implants légers, abolit l'ultime frontière de la sécurité informatique : l'esprit humain. Devenue le vecteur privilégié de la prise de décision augmentée, cette technologie impose une refonte en profondeur des systèmes d'information, qui doivent désormais intégrer un nouveau champ de flux - cognitifs - en temps réel. Cette porosité inédite expose les organisations à des défis de gouvernance majeurs, exigeant un encadrement strict des usages et un traitement juridique différencié selon que la donnée extraite reflète un signal biométrique brut ou une véritable intention professionnelle interprétable.

L'intégration d'interfaces neuronales implique surtout l'extension de la surface d'attaque à un sphère d'une criticité absolue. Le piratage de l'intégrité cognitive (*neuro-hacking*) ouvre la porte à l'exfiltration de la propriété intellectuelle à sa source, avant même sa matérialisation numérique. Plus radicalement, l'altération des signaux bidirectionnels ouvre la voie à la manipulation discrète du jugement des employés. Face à cette vulnérabilité, les organisations doivent concevoir des architectures de sécurité biométriques capables d'isoler ces flux. La protection de l'intention et de la pensée brute s'impose ainsi comme l'enjeu paroxystique de la cybersécurité.

Hypothèse 3. Un *World Model* ou une Intelligence Artificielle Générale émerge

D'ici 2040, la convergence de l'IA avec la robotique et la biotechnologie engendre diverses mutations préparant l'avènement de la « Singularité » et des superintelligences. Le déploiement d'une Intelligence Artificielle Générale (IAG), système capable d'exécuter des tâches cognitives de manière autonome au moins aussi bien, voire mieux qu'un humain, provoque un bouleversement politique, économique, éthique et scientifique sans précédent. Une autre trajectoire structurante réside dans l'émergence d'un « *World Model* »¹, c'est-à-dire un système capable de se représenter le monde physique et d'en déduire les dynamiques en temps réel. Cette technologie transcende le simple outil d'aide à la décision pour conférer à son utilisateur un atout majeur d'anticipation stratégique. En simulant des environnements d'une complexité extrême, ce moteur prédictif permet de tester les effets d'une décision avant son application dans le réel, bouleversant la recherche scientifique et la gestion de crise. Le décideur doté d'un tel simulateur dissipe l'incertitude, condamnant les acteurs non équipés à une réactivité perpétuelle et aveugle.

Dans tous les cas, face à l'asymétrie de puissance que provoquent ces modèles, leur contrôle, l'accaparement des données qui les alimentent et les règles qui les gouvernent s'imposent comme les ultimes champs de bataille de la souveraineté pour les États et de la création de valeur pour les organisations.

Hypothèse 4. L'impression « 4D » démocratise la fabrication de matériaux aux structures évolutives

D'ici 2040, l'impression « 4D » apparaît et permet d'exploiter des matériaux qui modifient leur structure en réponse à des *stimuli* externes comme le contact de la chaleur, de l'eau ou d'un environnement biologique. L'industrialisation des machines à imprimer se développe et des objets capables de s'adapter à leur milieu après leur fabrication se diffusent largement dans les secteurs de la pharmaceutique, de l'aéronautique, de la construction et de la logistique de pointe. La maîtrise de la matière programmable provoque une relocalisation de la production. Les chaînes de valeur traditionnelles s'effondrent au profit d'infrastructures de fabrication distribuées. Certains actifs physiques se réduisent à un simple fichier numérique, transmis et matérialisé ensuite au plus près du besoin opérationnel. Les systèmes d'information deviennent alors la colonne vertébrale de cette nouvelle industrie locale, déplaçant *de facto* les risques cyber immatériels vers l'intégrité de la matière. La protection de la propriété intellectuelle, la normalisation des formats et la sécurisation des plans d'impression s'imposent comme des impératifs pour empêcher le sabotage moléculaire d'équipements stratégiques.

À terme, ces objets, couplés à des capteurs, dialoguent en continu avec des simulations complexes pour ajuster leur comportement en temps réel, fusionnant de manière inédite le code algorithmique et la réalité physique.

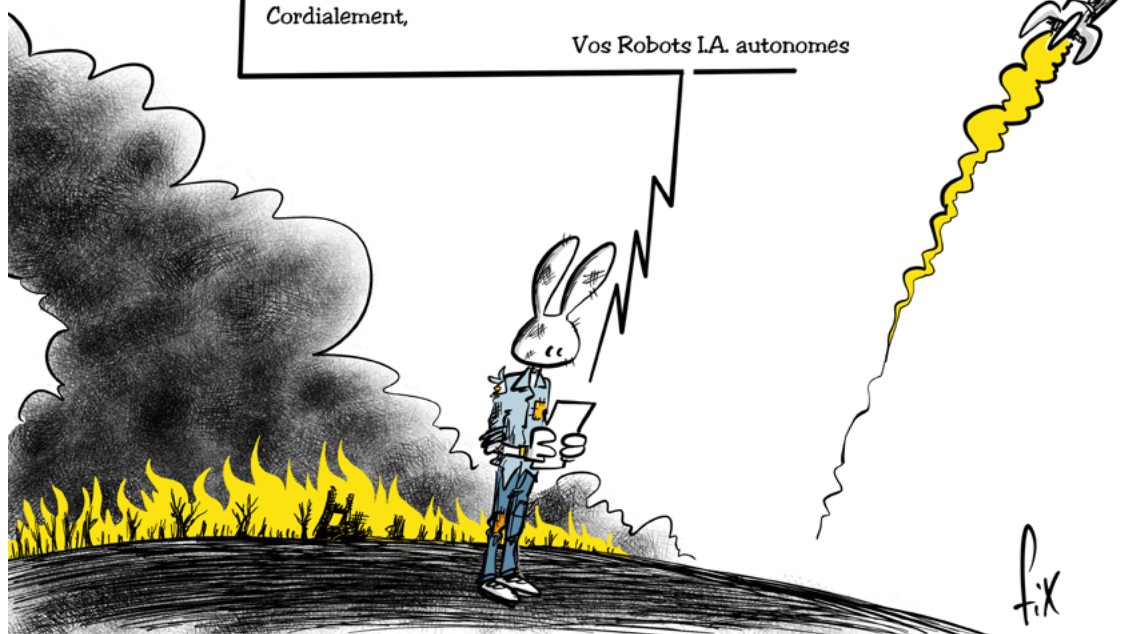
¹ Tel qu'envisagé par Yann Le Cun avec [AMI Labs](#)

Champ

04 Numérique responsable

Chers humains,
merci pour votre planète.
Sur vos instructions, nous avons utilisé toutes ses ressources
pour faire tourner les réseaux sociaux et générer ces vidéos
rigolotes de chatons que vous aimez tant.
Il n'y a plus rien à en tirer.
Nous partons donc en quête d'une autre planète à consommer,
sans vous malheureusement, car nous ne pouvions emmener
que des choses utiles.
Bonne chance et encore merci.
Cordialement,

Vos Robots I.A. autonomes



Tendances lourdes

Tendance lourde 1. Les dégradations climatiques et environnementales impactent de plus en plus les infrastructures et les services numériques

Tendance lourde 2. La consommation de ressources et l'impact environnemental du numérique s'accroissent significativement

Tendance lourde 3. Le numérique est de plus en plus mobilisé au service d'une transition responsable

Tendance lourde 4. Les réglementations visant à réduire l'empreinte environnementale du secteur numérique se développent

Tendance émergente

Tendance émergente 1. Les réglementations arbitrants l'utilisation de l'eau et de l'énergie par le secteur numérique se multiplient

Incertitudes majeures

Incertitude 1. Un consortium international d'organisations fournisseurs et utilisatrices du numérique pourrait voir le jour pour coordonner des engagements environnementaux communs

Incertitude 2. De nouveaux outils technologiques pourraient permettre de réduire efficacement et à grande échelle les consommations d'énergie du numérique

Hypothèses de rupture

Hypothèse 1. Une IA frugale voit le jour et réduit drastiquement les besoins en énergie et en ressources des systèmes d'IA

Hypothèse 2. Une tempête solaire de forte intensité prive durablement les organisations de leurs réseaux électriques et de communication

Hypothèse 3. Une part considérable d'infrastructures numériques ne sont plus assurables, du fait de leur exposition à des risques croissants, ce qui crée une défaillance de marché aux conséquences systémiques

Hypothèse 4. La raréfaction de l'accès à l'énergie limite le développement numérique et contraint les acteurs à des arbitrages stratégiques majeurs

Hypothèse 5. L'Union européenne impose le recyclage de tous les composants, pour s'affranchir du scope 3

Tendance lourde 1. Les dégradations climatiques et environnementales impactent de plus en plus les infrastructures et les services numériques

DE QUOI S'AGIT-IL ?

Les événements climatiques, plus fréquents et intenses, ont des impacts directs ou indirects croissants sur les infrastructures numériques, qu'il s'agisse des centres de données, des réseaux de télécommunication et énergétiques, de la logistique ou des sites de production de composants. Les aléas climatiques et leur imprévisibilité constituent un défi majeur pour la résilience des organisations qui dépendent de ces infrastructures et des services numériques qu'elles supportent. Des vagues de chaleur prolongées peuvent ainsi s'accompagner de sécheresses et d'incendies, tandis que les tempêtes peuvent provoquer des inondations et des épisodes de submersion indésirables. L'anticipation des conséquences opérationnelles pour la continuité d'activité implique donc d'appréhender ces risques de manière systémique et de prendre en compte leurs effets en cascade.

LES DYNAMIQUES À L'ŒUVRE

Les risques associés au climat deviennent un facteur de volatilité économique, laissant entrevoir des chocs de prix plus fréquents et une difficulté à prévoir les interruptions d'approvisionnement. En effet, en amont des chaînes de valeur, les risques menacent la production des matières premières et les chaînes d'approvisionnement. En 2024, l'ouragan Héléne a ainsi interrompu la production des mines de Spruce Pine, en Caroline du Nord, qui fournit la majorité du sable de quartz pur de la planète pour l'industrie des semi-conducteurs. Quelques semaines d'arrêt ont fait craindre des tensions sur la production de composants électroniques, même si les dégâts matériels ont finalement été limités. Si les stocks et la diversification des fournisseurs permettent d'amortir certains chocs à court terme, la répétition des événements climatiques extrêmes pourrait agir comme un multiplicateur de risques sur des chaînes d'approvisionnement volontairement à flux tendu (*just in time*) ou déjà sous tension.

Les perturbations peuvent également se porter sur les infrastructures et affecter les centres de données et autres bâtiments qui les abritent. En 2022, plusieurs centres de données exploités par Google et Oracle étaient hors service lors de vagues de chaleur intenses, mettant en évidence la fragilité de certains systèmes de refroidissement face à des températures extrêmes (BBC). Lors de la canicule enregistrée à l'été 2026, la capacité des data centers à maintenir leurs services en France a fait l'objet de craintes similaires (Les Echos). À cela s'ajoute que 22 % des 8900 centres de données dans le monde sont d'ores déjà exposés (XDI) à des risques climatiques modérés ou élevés (inondations, cyclones, incendies de forêt, mouvements de sol). Pour l'Institut du Numérique Responsable (IRN), cette proportion pourrait atteindre près de 30 % d'ici 2050 si les trajectoires actuelles se maintiennent. Enfin, le phénomène de retrait-gonflement des argiles pourrait menacer certains centres de données ou bâtiments dont la conception n'a pas initialement pris en compte ce type de risque.

Ces vulnérabilités peuvent enfin se répercuter sur les réseaux et les services numériques eux-mêmes. Concrètement, en cas d'impréparation des organisations, ces événements pourraient entraîner l'impossibilité d'accéder à des services pourtant indispensables. La gestion de ces crises se trouve d'ailleurs complexifiée par les nombreux opérateurs d'infrastructures dont les responsabilités se trouvent diluées et dont les actions de remise en service se trouvent administrativement freinées. Les infrastructures numériques restent en outre subordonnées au réseau électrique, l'immense majorité des pannes de couverture mobile résultant directement d'une rupture d'alimentation. À ces risques matériels s'ajoute celui de pertes de données massives et potentiellement irréversibles en cas d'endommagement grave d'une infrastructure lorsque les dispositifs de réplication et de sauvegarde sont insuffisamment distribués et redondants, comme ce fut le cas lors des incendies en Gironde (2022) ou de la tempête Alex (2020).

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, la résilience climatique des acteurs du numérique pourrait devenir une priorité stratégique pour les organisations. La robustesse de leurs activités dépendra pour bonne part de leur capacité d'anticipation aux événements extrêmes et d'adaptation de leurs infrastructures techniques aux aléas. En interne comme en externe, l'ingénierie climatique, la diversification géographique des installations de centres de données et de routes d'acheminement ou encore la sanctuarisation des Nœuds de Raccordement Optique et antennes mobiles les plus critiques, contribueraient grandement à la résilience environnementale du numérique. De même, le développement d'alternatives *low-tech*¹, et le suivi opérationnel en temps réel des plans de continuité (avec analyse de leurs corrélations et *Business impact analysis*) pourraient constituer des premiers moyens efficaces de se prémunir contre ces risques. Pour pallier la vulnérabilité des réseaux terrestres, les organisations pourraient également s'appuyer de manière systématique sur les constellations satellitaires (comme le réseau européen IRIS2), mettre en place un mécanisme de « *disaster roaming* » (itinérance en catastrophe), garantissant la bascule automatique des abonnés vers les antennes concurrentes encore opérationnelles (Arcep), et réserver un des spectres de basse fréquence dédiés à la résilience des services publics essentiels (CSNP).

Ces évolutions pourraient également transformer les équilibres économiques et géopolitiques du numérique en renforçant l'attractivité de certains territoires « refuges », avec des conséquences opérationnelles directes pour la localisation des données et des infrastructures critiques. L'obsolescence des plans de gestion de crise actuels devrait obliger l'État et les organisations à intégrer nativement les réseaux de télécommunications dans les plans ORSEC et les Schémas Locaux de Résilience (SLR), potentiellement soutenus par des fonds d'intervention dédiés (type Fonds Barnier). La question de l'assurabilité de ces infrastructures pourrait également devenir centrale pour la pérennité des activités. En effet, pour faire face à l'augmentation de la fréquence et du coût des sinistres, certains acteurs de l'assurance pourraient réduire les risques couverts ou se retirer de marchés jugés trop exposés. Les opérateurs devraient alors arbitrer entre des coûts d'adaptation et le risque de ne plus pouvoir absorber financièrement les conséquences d'une catastrophe. À terme, la résilience climatique pourrait être traitée à un niveau comparable à la cybersécurité, avec des indicateurs dédiés et des exigences formalisées dans les réglementations et les contrats.

¹ *L'approche low-tech au service de la résilience numérique des organisations : stratégies d'adaptation face aux fluctuations*, Cigref, Février 2026

Tendance lourde 2. La consommation de ressources et l'impact environnemental du numérique s'accroissent significativement

DE QUOI S'AGIT-IL ?

La multiplication des usages numériques entraîne une consommation croissante de ressources naturelles, notamment de métaux, d'énergie et d'eau, qui contribue à l'augmentation de l'empreinte environnementale du secteur. Cette dynamique, désormais accélérée par le développement des technologies d'intelligence artificielle, entre en conflit avec les discours, les objectifs fixés et les attentes concernant un numérique vertueux, voire réparateur, pour servir l'économie réelle et les besoins humains. L'illusion d'un numérique « immatériel » semble dès à présent se heurter au « mur des limites physiques ».

LES DYNAMIQUES À L'ŒUVRE

Le secteur numérique mobilise des quantités considérables de ressources naturelles, dont l'ampleur reste souvent méconnue. À titre d'exemple, la production d'un ordinateur de 2 kg nécessite, selon l'[ONU](#), la mobilisation d'environ 800 kg de matières premières. Un smartphone concentre à lui seul plus de cinquante métaux différents (cuivre, cobalt, lithium, tantale, terres rares) dont beaucoup ne sont pas recyclables en fin de vie. Toujours selon l'[ONU](#), la demande en minéraux (lithium, cobalt) nécessaires à la numérisation et à la transition énergétique elle-même, pourrait augmenter à l'échelle mondiale de 1500 % d'ici 2050.

Même si les matières premières sont présentes en quantités infimes dans les équipements, leur usage pour l'industrie numérique absorbe pour certains (gallium, germanium) jusqu'à 95% des besoins mondiaux. Or, l'extraction et le raffinage de ces ressources entraînent des impacts environnementaux et sociaux considérables, surtout dans des régions politiquement et climatiquement instables. En [Birmanie](#), l'exploitation des mines de terres rares, dans un contexte de guerre civile, contribue au pillage des ressources naturelles et s'accompagne de dommages environnementaux et sanitaires majeurs, sans réelles retombées économiques pour les habitants de la région. Le raffinage de ces matériaux reste par ailleurs majoritairement concentré en [Chine](#), rendant les chaînes d'approvisionnement européennes particulièrement vulnérables aux tensions géopolitiques et aux aléas climatiques affectant ces régions. En 2024, la quasi-totalité des terres rares consommées dans l'Union européenne (près de 98 % selon [Euronews](#)) provenait encore de Chine, non seulement pour l'extraction mais surtout pour le raffinage. Le recyclage ne permet encore que partiellement de réduire cette dépendance aux matières premières vierges. Les taux de recyclage en fin de vie sont inférieurs à 1% en raison d'un processus coûteux et complexe, compte tenu des faibles quantités de matériaux et de leur mélange dans les équipements. Une proportion non négligeable de déchets électroniques reste en conséquence exportée vers des décharges à ciel ouvert, comme à Agbogbloshie au Ghana.

La consommation énergétique du secteur numérique est également en hausse et cette tendance ne devrait pas s'inverser à moyen terme. Les émissions de gaz à effet de serre du secteur numérique représentent aujourd'hui, selon l'[Arcep](#) 3 à 4 % des émissions mondiales, soit davantage que l'aviation civile. En France le numérique représente désormais 4,4 % de l'empreinte carbone nationale, niveau comparable aux émissions des poids lourds. Un inventaire publié par l'[ADEME](#) en 2026 recense, par ailleurs, 352 data centers actifs en France dont la consommation représente près de 2 % de la consommation électrique nationale. Dans un scénario tendanciel construit par l'[ADEME](#), l'utilisation de l'électricité induite par les usages numériques français pourrait tripler d'ici 2035. L'avènement de l'IA marque un tournant pour

l'impact environnemental du numérique puisque l'entraînement des LLM mobilise à lui seul des volumes de calcul et d'énergie très supérieurs à ceux d'applications numériques classiques. L'apparition de modèles d'IA plus sobres (*Small Language Models*) ne freine pas de manière significative l'augmentation de la consommation énergétique. À l'échelle mondiale, l'Agence internationale de l'énergie estime qu'en 2024, les centres de données consommaient environ 1,5 % de l'électricité mondiale, et que cette part pourrait approcher 945 TWh (soit 3 %) d'ici 2030 si les tendances actuelles se poursuivent. Des conflits d'usages pourraient en découler dans les régions qui abritent des data centers : en Irlande par exemple, les centres de données représentaient déjà plus de 20 % de la consommation électrique en 2024, dépassant celle de certaines zones résidentielles urbaines.

La consommation d'eau constitue un troisième vecteur d'impact encore sous-estimé. Ce ne sont pas tant les ressources physiques en eau qui sont en question, que l'accès de qualité à cette ressource et la concurrence entre les usages industriels, agricoles et urbains simultanés. En 2024, les data centers suivis en France ont prélevé 575 000 m³ d'eau potable pour refroidir leurs serveurs, soit l'équivalent de la consommation annuelle d'une commune de 10 000 habitants, en hausse de 16 % en trois ans (Arcep). À l'échelle mondiale, en 2025, les centres de données ont consommé environ 4 500 milliards de litres d'eau, correspondant au volume nécessaire pour répondre aux besoins de plus de 600 millions de personnes en Afrique subsaharienne. Pour les Nations Unies, ce chiffre pourrait doubler d'ici 2030 sous l'effet de la croissance des usages de l'IA.

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, la soutenabilité énergétique et hydrique du numérique pourrait devenir un indicateur de maturité et de résilience pour les organisations. La consommation électrique associée aux centres de données pourrait augmenter très fortement à l'horizon 2050 si elle n'est entravée par aucune politique de sobriété ni régulation forte, provoquant des tensions sociales grandissantes là où sont implantées ces infrastructures.

La question de la nature des énergies mobilisées pour répondre à cette croissance devrait également être déterminante. En dépit des investissements croissants des acteurs du secteur dans les énergies renouvelables, le recours à des énergies fossiles devrait être vraisemblablement nécessaire pour sécuriser l'alimentation de ces infrastructures, rendant plus difficile la tenue des trajectoires climatiques des acteurs numériques annoncées il y a 5 ans, avant la démocratisation de l'IA. Les conflits d'intérêts avec d'autres secteurs pourraient aussi se multiplier, ce qui pourrait motiver des arbitrages ou des réglementations beaucoup plus contraignants.

Enfin, face à la rareté matérielle, la relocalisation partielle de la production, la diversification des sources, l'intégration de matériaux alternatifs et la mise en place de filières de recyclage de pointe pourraient devenir une condition d'accès aux services numériques critiques. Le numérique ne pourrait plus être pensé hors de sa dépendance aux ressources physiques, dont la rareté et la conflictualité seraient devenues les paramètres structurants d'une stratégie pérenne.

Tendance lourde 3. Le numérique est de plus en plus mobilisé au service d'une transition responsable

DE QUOI S'AGIT-IL ?

Face aux tensions grandissantes concernant les consommations d'énergie et d'eau, le numérique cesse d'être perçu uniquement comme un centre d'émissions et s'impose également comme un outil d'optimisation utile à la transition de l'ensemble des secteurs d'activité. De sa propre initiative ou sous la contrainte réglementaire, le secteur engage depuis quelques années une transformation de ses pratiques, faisant de l'éco-efficience un levier direct de rentabilité et de résilience opérationnelle.

LES DYNAMIQUES À L'ŒUVRE

Le numérique est de plus en plus utilisé comme un instrument de planification et d'amélioration de l'efficacité énergétique au sein des organisations (*IT for Green*¹). Les systèmes d'information actuels incluent désormais des capteurs et des fonctionnalités de suivi, de prévision et d'optimisation prédictive de l'énergie et des flux électriques (chauffage, éclairage, climatisation). Les réseaux de distribution, les *smart grids*, les plateformes et les applications de gestion énergétique favorisent une approche globale de l'efficacité énergétique. Des systèmes de pilotage intelligent peuvent, par exemple, permettre de réduire la consommation énergétique de bâtiments en optimisant automatiquement le chauffage ou l'éclairage. De plus, l'Internet des objets (IoT) combiné à l'intelligence artificielle permet une gestion précise des ressources nécessaires aux environnements spécifiques des bâtiments ou de la logistique, par exemple. Ces gains ne se concrétisent cependant que si des changements organisationnels et réglementaires accompagnent les innovations techniques. Sans stratégie de sobriété, ces outils peuvent eux-mêmes générer de nouvelles consommations (capteurs, traitement de données, stockage), voire des « effets rebond » atténuant ou annulant les gains attendus.

Simultanément, les organisations s'engagent dans une évolution de leurs pratiques numériques (*Green IT*) en réponse aux exigences réglementaires afin de réduire leur impact environnemental. Les stratégies dites de « numérique responsable »² se diffusent dans les entreprises et les administrations, en lien avec les critères ESG et les nouvelles obligations de reporting extra-financier. En France, plusieurs référentiels publics et guides de bonnes pratiques structurent désormais ces démarches : le guide de bonnes pratiques « numérique responsable » publié par l'État propose 74 actions concrètes (éco-conception, sobriété des usages, allongement de la durée de vie des équipements), tandis que l'ADEME incite les collectivités à intégrer la réduction de l'empreinte numérique dans leurs plans climat et leurs trajectoires de décarbonation.

¹ *IT for Green : contributions des directions numériques aux enjeux RSE et de décarbonation des organisations*, Cigref, Mars 2025

² *Stratégies Numérique Responsable des grandes organisations : comment passer à l'échelle ?*, Cigref, Septembre 2025

Cette réduction des impacts environnementaux du numérique passe aussi par l'optimisation des structures informatiques qui sont conçues pour encourager la décentralisation et l'efficacité énergétique. Les logiciels et services numériques sont également de plus en plus développés *by-design*, à partir de référentiels partagés d'écoconception pour réduire leur empreinte carbone et surtout les coûts d'hébergement et de maintenance. L'utilisation de centres de données qui fonctionnent grâce à des énergies renouvelables et de techniques de refroidissement novatrices (comme le refroidissement naturel ou l'immersion des centres de données) se développe. Des acteurs mondiaux comme Google implantent leurs centres de données dans des zones à fort potentiel solaire ou éolien (comme le site belge de Saint-Ghislain qui compte des dizaines de milliers de panneaux solaires), permettant de couvrir une part significative de la consommation électrique du site par des énergies renouvelables. Les techniques de refroidissement, liquide direct (*Direct-to-Chip*) ou par immersion, permettent de réduire la demande énergétique des centres de données de façon significative sur l'ensemble du cycle de vie, par rapport au refroidissement par air traditionnel.

En 2023, les grandes entreprises du numérique figuraient parmi les tous premiers acheteurs mondiaux d'électricité renouvelable (PPAs), et représentaient dans certains marchés près d'un tiers des nouveaux contrats signés. L'adoption de mesures en faveur de l'efficacité est donc grandement favorisée par celles-ci car elles permettent aussi de minimiser les effets des fluctuations des coûts de l'énergie. Cette stratégie permet de sécuriser des volumes d'électricité décarbonée à long terme, mais pose aussi la question des arbitrages avec d'autres secteurs pour l'accès à ces ressources.

Les stratégies de diminution des impacts du numérique sur l'environnement sont également alimentées par de la R&D pour optimiser les méthodes de production *via* par exemple la réduction de l'architecture des puces, mais aussi pour allonger la durée de vie des équipements en les rendant plus réparables. Des programmes de recherche visent à trouver des matériaux alternatifs aux terres rares et aux métaux critiques. Ainsi le graphène, certains semi-conducteurs organiques ou des polymères conducteurs suscitent un intérêt scientifique, mais leur diffusion industrielle à grande échelle reste incertaine à l'horizon 2040 et ils ne devraient pas supprimer à eux seuls la dépendance aux métaux critiques.

PERSPECTIVES À L'HORIZON 2040

Dans un contexte de raréfaction de l'énergie et de tarification carbone pour le moins punitive, les organisations capables de maîtriser leurs dépendances énergétiques et de les dimensionner par rapport à leurs usages numériques pourraient disposer d'un avantage compétitif décisif. Sous le poids de l'« effet prix » de l'énergie, les indicateurs financiers de retour sur investissement pourraient intégrer dans leurs calculs de *Total Cost of Ownership* (TCO) les dimensions environnementales, faisant converger *FinOps* et *GreenOps*. Le numérique, loin d'être un simple centre de coûts, s'imposerait alors comme le moteur principal des politiques de résilience et d'optimisation industrielle.

Tendance lourde 4. Les réglementations visant à réduire l’empreinte environnementale du secteur numérique se développent

DE QUOI S’AGIT-IL ?

Un cadre juridique du numérique émerge progressivement à travers deux catégories de textes législatifs. D’un côté, des réglementations générales portant sur les émissions de gaz à effet de serre ou sur l’empreinte écologique des entreprises s’appliquent également aux acteurs du numérique. De l’autre, certains textes visent spécifiquement le numérique, notamment l’origine, la composition et la fin de vie des équipements, ainsi que les questions de traçabilité et de consommation d’énergie. En la matière, l’Union européenne se distingue par une production normative nettement supérieure à celle des autres grandes zones régionales.

LES DYNAMIQUES À L’ŒUVRE

Les organisations, fournisseurs comme utilisatrices de solutions numériques, sont de plus en plus soumises à des exigences générales de réduction de leur impact environnemental. Ces réglementations concernent notamment la consommation d’énergie, les émissions de gaz à effet de serre et la gestion des déchets. Il en va de même pour les obligations déclaratives, telles que la directive CSRD¹, qui impose une plus grande transparence sur les émissions de gaz à effet de serre, y compris les émissions indirectes (scope 3) liées aux infrastructures numériques étendues (centres de données, terminaux, chaînes d’approvisionnement) des entités concernées.

L’Union européenne instaure, en parallèle, certaines obligations spécifiques aux acteurs du secteur numérique. Les directives DEEE (déchets d’équipements électriques et électroniques) et Batteries imposent des obligations de collecte, de traitement et de recyclage, ainsi qu’une responsabilisation des fabricants quant à la fin de vie de leurs produits. Le *Critical Raw Materials Act*, sur les matières premières critiques et le règlement *Net Zero Industry* visent à sécuriser et diversifier les chaînes d’approvisionnement stratégiques pour des secteurs comme le numérique, tout en renforçant les exigences de durabilité. Le règlement ESPR (*Ecodesign for Sustainable Products Regulation*), adopté en juin 2024, instaure un système de passeport numérique pour les produits, et donne accès à des informations tout au long de leur cycle de vie. Ces dispositifs devraient bientôt être renforcés par de nouveaux règlements, notamment le *Circular Economy Act* et l’*Advanced Materials Act*, qui sont actuellement en cours d’élaboration. Le premier vise à réglementer plus largement l’économie circulaire, tandis que le second se concentre sur l’utilisation de matériaux avancés.

En France plus particulièrement, la loi de réduction de l’empreinte environnementale du numérique (REEN, 2021) oblige les municipalités de plus de 50 000 habitants à élaborer une stratégie numérique durable. La loi contre le gaspillage et l’économie circulaire (AGEC, 2020) encourage par ailleurs la réparation des équipements et combat l’obsolescence programmée. À cela s’ajoute le [label](#) « Numérique Responsable » lancé par le gouvernement afin de mettre en valeur les entreprises qui s’efforcent de réduire l’empreinte écologique de leurs services et de leurs infrastructures. Ce dispositif reste toutefois facultatif et en cours de diffusion.

¹ Mise en œuvre de la *Corporate Sustainability Reporting Directive*, Cigref, Janvier 2026

À l'échelle de la planète, ce processus de normalisation reste très inégal puisqu'il n'existe aucun cadre juridique international contraignant qui soit spécifiquement dédié à l'empreinte environnementale du numérique. Ces enjeux font certes l'objet de discussion dans le cadre du G20 ou de l'ONU (notamment *via* le Programme des Nations unies pour l'environnement), mais celles-ci n'ont pour l'instant débouché que sur des recommandations non contraignantes.

Aux États-Unis, il n'existe pas de législation fédérale spécifique au secteur. Les initiatives reposent surtout sur des engagements volontaires d'entreprises ou sur des textes adoptés par certains États fédérés, comme la Californie ou l'État de New York, qui imposent des obligations de reporting ou d'efficacité énergétique dans des domaines ciblés. Un projet de loi fédérale sur l'évaluation des impacts environnementaux de l'IA a été introduit au Sénat, mais il n'a pas été adopté à ce stade.

À l'inverse, la Chine a intégré la réduction de l'empreinte carbone du numérique dans ses plans de souveraineté, avec un objectif affiché de neutralité en 2060. Elle a notamment fixé des normes d'efficacité énergétique pour les data centers et encourage le recours aux énergies renouvelables dans ce secteur, dans le cadre plus large de ses stratégies de contrôle des infrastructures numériques et énergétiques.

PERSPECTIVES À L'HORIZON 2040

Dans l'Union européenne, la tension pourrait s'intensifier entre l'ambition de développer des champions européens du numérique d'une part, et des exigences croissantes d'encadrement de l'impact environnemental du secteur numérique et de l'autre. À l'échelle mondiale, les divergences réglementaires entre l'UE, les États-Unis et la Chine pourraient en effet pénaliser la compétitivité des entreprises européennes. La Commission européenne pourrait d'ailleurs réviser, dès 2027, les objectifs de la « décennie numérique » pour vérifier qu'ils restent adaptés à l'évolution du paysage économique, technologique et climatique. En conséquence, les entreprises évoluant principalement dans l'espace européen pourraient être soumises à des exigences plus strictes encore, ce qui pourrait à la fois renforcer leur crédibilité sur les marchés où la durabilité est valorisée, et peser sur les modèles d'affaires par rapport à des concurrents mondiaux moins contraints. Enfin, si les entreprises parviennent à mettre en place les conditions d'un progrès technologique soutenable, le numérique durable pourrait alors devenir un levier de performance et de robustesse, plutôt qu'une simple contrainte réglementaire.

Tendance émergente 1. Les réglementations arbitrants l'utilisation de l'eau et de l'énergie par le secteur numérique se multiplient

Les consommations d'eau et d'énergie des infrastructures numériques peuvent entrer en concurrence avec celles de l'agriculture, des ménages et de l'industrie. Les pouvoirs publics sont dès lors amenés à arbitrer de plus en plus directement la répartition de ces ressources, conduisant certains projets d'infrastructures numériques à faire l'objet de contestations, voire d'interruptions temporaires d'activité. Dans la chaîne de valeur numérique, l'eau est indispensable à l'extraction et au raffinage des matières premières, à la fabrication des semi-conducteurs, au refroidissement des centres de données et à certaines formes de production d'électricité. L'enjeu ne réside pas seulement dans la quantité d'eau disponible mais également dans l'accès à une ressource de qualité suffisante.

Ces phénomènes d'arbitrages ont déjà des conséquences réelles. En 2021, lors d'une sécheresse à Taïwan, les parcs industriels de Hsinchu et Taichung ont été contraints de réduire leur consommation d'eau de 15 % ([Forbes](#)), et TSMC a dû faire appel à des centaines de camions-citernes pour maintenir sa production ([Fortune](#)). Dans une région concentrant 63 % de la production mondiale de semi-conducteurs, une pénurie d'eau peut ainsi mettre sous tension l'ensemble de la chaîne d'approvisionnement numérique mondial. En 2023, [TSMC](#) a de nouveau dû activer ses plans de crise face aux restrictions imposées par les pouvoirs publics dans un contexte de fortes chaleurs. Cette situation n'est qu'un aperçu de ce qui pourrait prochainement attendre le secteur. En effet, plus de 40 % des usines de semi-conducteurs existantes sont situées dans des bassins versants susceptibles de connaître un fort stress hydrique d'ici 2030, et cette proportion pourrait dépasser 50 % à l'horizon 2040 selon les scénarios climatiques les plus pessimistes soutenus par le [Forum économique de Davos](#). Cette exposition concerne également des sites stratégiques en Arizona et au Texas mais aussi à Taïwan, en Corée du Sud et en Europe.

Des tensions comparables apparaissent pour l'accès à l'énergie, sous l'effet de l'explosion de la consommation électrique des centres de données dédiés à l'IA. Certains territoires imposent désormais des restrictions à l'implantation de nouvelles infrastructures, redéfinissant les arbitrages entre opérateurs privés, collectivités locales et population. En 2026, 40 maires de grandes villes, de Phoenix à Melbourne, ont signé un [appel commun](#) dénonçant « l'épuisement des terres, de l'énergie et de l'eau » par les data centers, demandant des règles contraignantes sur leur localisation et leur efficacité. Cette évolution est aussi perceptible en France. La [loi DDADUE](#) de 2025 impose ainsi aux centres de données de plus de 500 kW de déclarer leurs consommations énergétiques et environnementales, et à ceux de plus de 1 MW de valoriser leur chaleur fatale. De même, le [Sénat](#) a adopté en mars 2026 une proposition de loi visant à mieux encadrer l'implantation territoriale des data centers, et ajoutant une redevance sur les prélèvements d'eau pour leur refroidissement. Avec l'évolution du climat et la tension croissante sur les réseaux électriques, les infrastructures numériques pourraient être ainsi davantage exposées à des restrictions d'usage, des contestations locales, des interruptions de service, voire des refus d'implantation. L'accès durable à l'eau et à l'énergie pourrait dès lors devenir un critère déterminant dans le choix des sites, des architectures et des partenaires d'hébergement des organisations.

Incertitude 1. Un consortium international d'organisations fournisseurs et utilisatrices du numérique pourrait voir le jour pour coordonner des engagements environnementaux communs

Si des embryons de coordination pour l'environnement existent déjà, leur capacité d'action demeure marginale faute de mandat contraignant. L'*European Green Digital Coalition* (EGDC) réunit ainsi 37 acteurs européens majeurs parmi lesquels Deutsche Telekom, Orange, Nokia, Ericsson, autour d'actions ciblées. L'Union internationale des télécommunications coordonne parallèlement la démarche *Green Digital Action*, lancée avec plus de 40 partenaires lors de la COP28. Ces structures peinent toutefois à infléchir la trajectoire globale du secteur en raison de leur éclatement géographique et de leur nature strictement incitative, alors que la course aux capacités de calcul des *hyperscalers* alimente une croissance exponentielle des centres de données.

Le *Corporate Climate Responsibility Monitor 2025* souligne d'ailleurs les limites de cette autorégulation. Son analyse des stratégies climatiques d'Amazon, Apple, Google, Meta et Microsoft relève que la hausse effective des émissions fragilise la portée des objectifs de réduction affichés, malgré certaines initiatives jugées prometteuses. Le rapport souligne notamment que l'augmentation rapide des besoins des centres de données remet sous tension les trajectoires climatiques du secteur.

À l'horizon 2040, face à la « bombe énergétique » induite par la démocratisation de l'IA et du calcul exascale, les stratégies climatiques individuelles des organisations pourraient ne plus suffire à se prémunir contre les risques environnementaux pesant sur leur continuité d'activité. Pour certaines d'entre elles, la volonté de maîtriser leur empreinte matérielle et leur environnement d'implantation pourrait conduire à l'émergence d'une coalition inédite. Un consortium transnational réunissant fournisseurs et organisations utilisatrices pourrait se former. En unifiant leur pouvoir de marché, loin du *greenwashing*, ces organisations pourraient ainsi chercher à instaurer un standard opérationnel, pour faire de la sobriété un prérequis à la commande privée. Cette initiative industrielle serait à même de les prémunir d'éventuels durcissements des contraintes réglementaires ou pratiques de rationnement énergétique opérées par les pouvoirs publics.

Incertitudes majeures

Incertitude 2. De nouveaux outils technologiques pourraient permettre de réduire efficacement et à grande échelle les consommations d'énergie du numérique

Le besoin de découplage entre la croissance exponentielle des capacités numériques et leur empreinte énergétique favorise l'industrialisation de technologies de rupture. Cet effort de rationalisation s'attaque simultanément à l'ingénierie des matériaux et à l'architecture des systèmes de calcul, avec l'ambition stratégique d'enrayer l'inflation énergétique des infrastructures critiques sans compromettre leur puissance opérationnelle.

La mutation de l'infrastructure physique repose en premier lieu sur la rupture matérielle. Le graphène, les semi-conducteurs organiques et les polymères conducteurs ouvrent la voie à une électronique fondamentalement moins énergivore. Si le consortium européen *Graphene Flagship* anticipe des percées commerciales décisives d'ici 2030, cette transition se heurte à l'inertie de l'industrie, le passage à l'échelle et l'intégration aux procédés de fonderie actuels demeurant des défis colossaux.

En parallèle, l'hyper-croissance des volumes d'information pourrait trouver une réponse dans le stockage moléculaire sur ADN. Portée par la start-up *Biomemory* et issue de la recherche académique française (CNRS, Sorbonne), cette technologie offre une densité de stockage jusqu'à 10.000 fois supérieure aux standards actuels pour un coût énergétique quasi nul. Cette solution vise, d'ici 2029, le marché massif des « données froides », c'est-à-dire les archives rarement consultées qui encombreront près de 70 % des serveurs mondiaux. Pour l'heure, le temps de latence en lecture de cette technologie, estimé à 20 minutes, et le coût encore prohibitif de la synthèse de l'ADN la disqualifient pour les opérations nécessitant un accès instantané.

Au-delà du stockage, l'architecture même du calcul subit une refonte pour éliminer les déperditions d'énergie. En 2025, la mise en production par le fondeur TSMC de la puce d'intelligence artificielle Jotunn8, conçue par la start-up française *VSORA*, démontre la viabilité de cette approche. En détruisant le « mur de la mémoire » - obligeant les processeurs à consommer jusqu'à 40 % de leurs cycles dans l'attente passive de données - cette puce réduit de moitié la consommation énergétique comparé aux standards du marché. Son déploiement dès juin 2026 dans les centres de données de Scaleway est venu valider la pertinence du modèle. Cette logique d'optimisation trouve également son aboutissement dans le calcul neuromorphique. En mimant l'architecture synaptique du cerveau biologique, des processeurs tels que le Loihi 2 d'*Intel* n'activent que les circuits strictement requis par l'action. Bien que cette approche génère des économies d'énergie de 50 % supérieures aux GPU lors de tâches d'inférence, sa complexité de programmation et son inadaptation à l'entraînement des LLM restreignent, dans l'immédiat, son déploiement à des niches. Si ces innovations ouvrent une trajectoire technologique prometteuse, elles demeurent majoritairement en dessous-du seuil de l'industrialisation.

À l'horizon 2040, le passage à l'échelle de technologies frugales en énergie devra briser d'imposants verrous économiques et réglementaires. Par ailleurs, en l'absence d'un but, d'une méthode et d'une gouvernance clairs - ou d'un cadre éventuellement coercitif - l'effondrement des coûts énergétiques générés par ces nouveaux outils, loin de se traduire par une baisse de la consommation globale, pourraient conduire mécaniquement à une explosion incontrôlable de nouveaux usages numériques.

Hypothèse 1. Une IA frugale voit le jour et réduit drastiquement les besoins en énergie et en ressources des systèmes d'IA

D'ici 2040, l'utilisation exponentielle des intelligences artificielles engendre une inflation insoutenable de la consommation matérielle et énergétique. En réponse, l'industrialisation de nouvelles technologies, fondées sur des architectures de modèles optimisées et des puces à très haute efficacité, donne naissance à une IA dite « frugale ». Cette rupture technologique offre des performances algorithmiques équivalentes, voire supérieures aux systèmes actuels, tout en réduisant les besoins en ressources critiques telles que l'eau, les terres rares et l'énergie. Cette frugalité transforme également chaque phase du cycle de vie technologique, de la phase d'entraînement des modèles jusqu'à leur utilisation quotidienne par inférence.

En abaissant drastiquement les barrières capacitaires et financières, cette innovation redistribue les cartes du marché. Elle offre aux plus petites organisations l'opportunité de tirer leur épingle du jeu en élaborant et en déployant des IA de pointe à moindre coût. Toutefois, la promesse d'une réduction significative de l'empreinte environnementale globale se heurte implacablement au paradoxe de « l'effet rebond ». L'effondrement du coût énergétique ou matériel ne freine pas la consommation, mais entraîne au contraire une démultiplication des cas d'usage. L'accessibilité accrue de ces IA frugale provoque une croissance exponentielle des sollicitations qui tend peu à peu à annuler mécaniquement les gains écologiques initiaux.

Hypothèse 2. Une tempête solaire de forte intensité prive durablement les organisations de leurs réseaux électriques et de communication

D'ici 2040, une tempête solaire majeure provoque une interruption massive et prolongée de l'ensemble des réseaux électriques et de télécommunication dont dépendent les organisations. Cet événement d'ampleur entraîne l'effondrement simultané des systèmes informatiques, des canaux d'échange internes et externes, et paralyse brutalement la continuité des services numériques critiques. Cette coupure s'étend de quelques jours à plusieurs semaines, la durée de la paralysie étant dictée par la gravité des dommages physiques infligés aux équipements et par la complexité logistique des opérations de réparation des infrastructures.

Cette crise agit comme une mise à l'épreuve implacable de la résilience des sociétés face à une asphyxie numérique prolongée. Elle confronte directement les organisations à la robustesse réelle de leurs plans de continuité d'activité (PCA) et impose un basculement d'urgence vers des modes de fonctionnement temporairement non numériques. Ce vide opérationnel force également une redéfinition immédiate des chaînes de responsabilité, obligeant les dirigeants, les assureurs et les pouvoirs publics à statuer sur l'imputabilité des défaillances et l'indemnisation des pertes face à une paralysie totale des écosystèmes.

Hypothèse 3. Une part considérable d'infrastructures numériques ne sont plus assurables, du fait de leur exposition à des risques croissants, ce qui crée une défaillance de marché aux conséquences systémiques

D'ici 2040, face à la convergence des menaces cyber, climatiques et géopolitiques, le marché de l'assurance se retire brutalement de la couverture des infrastructures numériques. Jugeant ces actifs trop exposés, les compagnies excluent de leurs portefeuilles de protection une forte proportion de centres de données, de réseaux et d'équipements critiques, ou imposent des primes aux tarifs prohibitifs. Cette défaillance de marché engendre une crise systémique du financement, menaçant directement la viabilité économique et l'exploitation opérationnelle de ces infrastructures.

Pour éviter l'effondrement des services essentiels, les gouvernements sont contraints d'intervenir en urgence afin de garantir la continuité des infrastructures jugées déterminantes pour la compétitivité des organisations et la souveraineté des États. En parallèle, les entreprises se voient acculées à l'auto-assurance ou à la mutualisation forcée des risques, une charge financière qui ampute sévèrement leurs capacités d'investissements productifs. L'inassurabilité structurelle des actifs numériques gèle, *in fine*, le développement de ses activités, condamnant au déclasserement technologique les régions et les secteurs identifiés comme les plus exposés et vulnérables.

Hypothèse 4. La raréfaction de l'accès à l'énergie limite le développement numérique et contraint les acteurs à des arbitrages stratégiques majeurs

D'ici 2040, le déficit structurel d'énergie entrave le fonctionnement de technologies hyper-énergivores, telles que l'IA agentique et le stockage chaud de données. Cette pénurie résulte des limites de production, des impératifs de décarbonation et des conflits d'usage intersectoriels.

Acculés par cette contrainte physique, les États instaurent une doctrine de rationnement numérique. Les services vitaux voient leur alimentation électrique sanctuarisée, tandis que les usages non critiques (streaming, réseaux sociaux, sites pornographiques) subissent un bridage systématique, une fiscalité punitive, voire une interdiction pure et simple au profit des intérêts supérieurs de la nation. Cette coercition énergétique redessine la cartographie technologique mondiale. Les organisations délocalisent d'urgence leurs infrastructures vers les rares territoires offrant une énergie abondante et décarbonée. L'accès à l'électron vert devient différenciant pour les activités numériques.

Hypothèse 5. L'Union européenne impose le recyclage de tous les composants, pour s'affranchir du scope 3

D'ici 2040, l'Union européenne rend obligatoire le recyclage complet des composants électroniques et numériques. Cette mesure vise à réduire sa dépendance et à forcer l'avènement d'une économie circulaire par la récupération des matériaux critiques. Cette bascule est un défi pour faire passer à l'échelle les filières de réemploi. Incitée par de fortes mesures d'allègement fiscal à destination des acteurs productifs et des utilisateurs, la filière européenne de recyclage réussit à garantir des volumes suffisants de matière premières pour le besoin de l'économie réelle.

Pour éviter toute distorsion de concurrence, ces normes s'appliquent également aux entreprises non européennes accédant au marché unique. Cette contrainte matérielle accélère enfin l'essor de modèles économiques alternatifs profitant à la location, la réutilisation et la mutualisation des équipements.

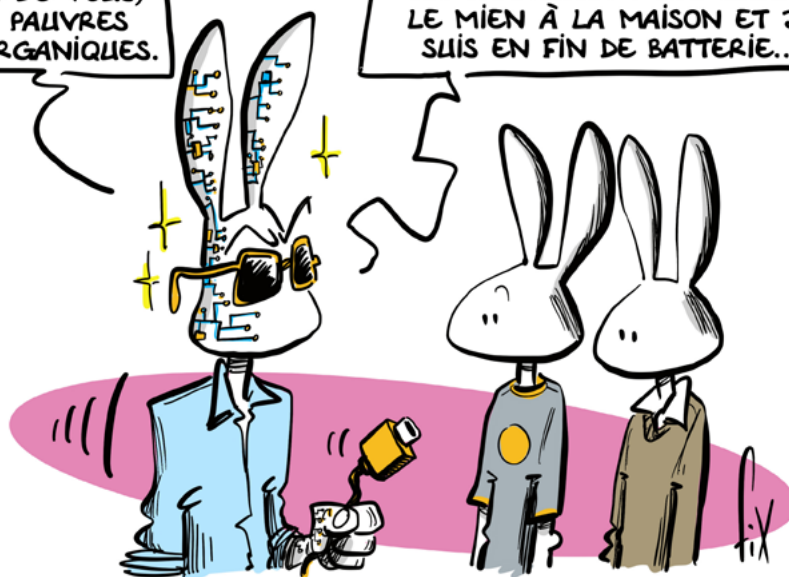
Champ

05 Travail et numérique

SALUT, JE SUIS VOTRE NOUVEAU
COLLÈGUE CYBORG AUGMENTÉ,
BOOSTÉ À L'I.A. ET AUX
IMPLANTS CYBERNÉTIQUES.

HYPER-PERFORMANT,
QUASI-OMNISCIENT,
JE SUIS PLUS PROCHE
DE DIEU QUE DE VOUS,
ESPÈCES DE PAUVRES
CRÉATURES ORGANIQUES.

PAR CONTRE, EST-CE QUE
L'UN D'ENTRE VOUS AURAIT
UN CHARGEUR ? J'AI OUBLIÉ
LE MIEN À LA MAISON ET JE
SUIS EN FIN DE BATTERIE...



Tendances lourdes

Tendance lourde 1. L'intégration en profondeur de l'IA générative dans les activités professionnelles bouleverse les périmètres et l'organisation des postes

Tendance lourde 2. Le décalage entre les besoins en recrutement du secteur IT et les compétences disponibles se maintient et se complexifie

Tendance lourde 3. Les cyberrisques touchant les collaborateurs se multiplient et se diversifient

Tendance émergente

Tendance émergente 1. L'IA agentique remet en question les stratégies traditionnelles de sourcing RH et pourrait favoriser une relocalisation de certaines activités

Incertitudes majeures

Incertitude 1. Le *Shadow AI* pourrait devenir un vecteur d'exfiltration de données sensibles et fragmenter la cohésion au sein de l'organisation

Incertitude 2. La mise à niveau des compétences cognitives pourrait imposer une redéfinition des responsabilités entre l'État et les organisations

Hypothèses de rupture

Hypothèse 1. La démocratisation du « jumeau professionnel » provoque une crise de la propriété intellectuelle et redéfinit le salariat

Hypothèse 2. L'imposition d'un « droit à la non-automatisation » structure le nouveau segment de marché du « Premium Humain »

Hypothèse 3. L'asymétrie cognitive induite par les usages de l'IA provoque une fracture de la capacité de jugement

Tendance lourde 1. L'intégration en profondeur de l'IA générative dans les activités professionnelles bouleverse les périmètres et l'organisation des postes

DE QUOI S'AGIT-IL ?

L'IA générative (IAG) se déploie à un rythme extrêmement rapide dans les organisations, et tend à se substituer totalement à une grande diversité de tâches, pour un large spectre de métiers et de compétences. Alors que s'ouvre la vague suivante de l'IA agentique, cette adoption en profondeur de l'IA générative représente un choc structurel pour les collaborateurs comme pour les organisations, suscitant des incertitudes fortes concernant ses impacts à long terme sur les compétences, la productivité et la rentabilité.

LES DYNAMIQUES À L'ŒUVRE

L'IAG dite « horizontale » est aujourd'hui utilisée par une majorité de collaborateurs pour automatiser certaines tâches routinières ou fastidieuses, comme la recherche d'informations ou la génération de textes. À ce titre, deux tiers des salariés français déclarent utiliser l'IA au travail au moins une fois par semaine, et un quart l'utiliser quotidiennement (*EY*). En parallèle, les IAG « par verticale métier » semblent être utilisées par un tiers des grandes entreprises françaises (*Les Echos*), couvrant une diversité et une spécificité toujours plus grande de processus. Dans les deux cas, les organisations tendent de plus en plus à privilégier le déploiement en interne et la personnalisation de ces outils, pour gagner en efficacité et pour éviter l'exfiltration de propriété intellectuelle sur des serveurs externes. Il n'en reste pas moins que de sérieux décalages peuvent s'observer entre, d'une part, les grandes entreprises qui structurent rapidement leurs usages de l'IA au sein de leurs plans stratégiques, et d'autre part, les plus petites organisations qui l'utilisent de manière plus ponctuelle et sans objectif de pilotage (*Institut Montaigne*).

L'usage professionnel de l'IA générative n'est pas sans conséquence pour la gestion des ressources humaines puisqu'il suscite des enjeux inédits pour les collaborateurs. En effet, la notion de « reconnaissance du travail » (matérielle et symbolique) se trouve fortement interrogée par la délégations importante de tâches aux IA, et s'associe de manière récurrente à un sentiment de dépossession des savoir-faire et de perte d'autonomie cognitive. Plus globalement, l'utilisation systématique des IAG peut entraîner une détérioration des interactions sociales (tout particulièrement intergénérationnelles) au sein des organisations, et bouleverser la valeur ajoutée historique des managers intermédiaires, dépossédés d'une partie de leurs missions au profit du pilotage algorithmique.

L'IAG bouleverse particulièrement les activités cognitives, complexes et non répétitives. La montée en abstraction place malgré tout les collaborateurs au rang d'opérateurs chargés de superviser, vérifier et compléter des matériaux de plus en plus générés automatiquement. Si les impacts sur la productivité globale des organisations n'ont pas encore été massivement démontrés, bien que certaines études les évaluent comme étant légèrement positifs (*Centre for Economic Policy Research*), l'enjeu stratégique réside dans l'exploitation de ces gains de productivité, avec le risque d'une prolétarianisation des cols blancs vers des tâches à plus faible valeur ajoutée immédiate. En ce sens, le rapport *LaborAI* met en avant le « paradoxe

de la performance », selon lequel les gains de productivité obtenus grâce à l'IA entraînent une réduction mécanique de la charge de travail et de l'utilité relative du travail humain. S'y ajoute le « paradoxe de la facilitation », décrivant le fait que la simplification d'une partie du travail peut être une source de frustration, de perte de sens et de réduction de la satisfaction au travail. Avant même les bouleversements promis par les systèmes multi-agents, le recours massif aux outils d'IAG pourrait déjà générer une baisse de la motivation et du bien-être au sein des collaborateurs, non sans effets à terme pour l'engagement personnel, la cohésion opérationnelle et la performance des organisations.

PERSPECTIVES À L'HORIZON 2040

D'ici 2040, les IA génératives seront vraisemblablement devenues un outil de travail incontournable pour une majorité de salariés, au premier rang desquels les collaborateurs de la fonction numérique. Trois types d'impacts principaux pourraient redessiner la matrice des métiers et des compétences.

Tout d'abord, le mouvement de reconfiguration des métiers et des tâches existantes pourrait continuer. L'IA en permettant de recentrer les métiers les plus qualifiés sur des tâches à très forte valeur ajoutée, imposerait une hyper-productivité qui accroîtrait le risque d'épuisement des collaborateurs compte tenu des exigences mentales requises par ces tâches. Pour les métiers moins qualifiés, l'usage de l'IA pourrait se traduire par un recentrage sur des activités de supervision et de contrôle, potentiellement dégradées et moins valorisantes.

D'autre part, cette tendance pourrait entraîner des destructions d'emplois ou des non-crétions d'emplois, à la fois pour des métiers peu qualifiés et pour des professions intellectuelles. Les métiers de l'informatique figurent à ce titre parmi les plus concernés par ce risque (Coface), plus d'un quart des activités étant vouées à l'automatisation. Ce risque de rationalisation technique pourrait tout particulièrement toucher les jeunes collaborateurs. En effet, le renouvellement de leur cursus de formation pourrait ne pas réussir à s'adapter à la vitesse de changement des nouvelles attentes des employeurs, et la rentabilité immédiate des profils juniors pourrait se trouver annulée par la mise en concurrence directe avec les IA, freinant considérablement leur embauche et leur montée en compétence tout en brisant la chaîne historique de transmission de l'expérience.

Troisièmement, le recours à l'IA pourrait augmenter la rentabilité de certains métiers, en améliorant leur productivité et leur créativité grâce à une coopération fructueuse entre l'humain et la machine. La catégorie de métiers augmentables grâce à l'IA pourrait représenter 1,4 million d'emplois rien qu'en France (Roland Berger). Cette évolution organisationnelle devrait également faire émerger de nouveaux métiers, en lien avec la supervision, l'entraînement et l'interprétation des algorithmes, tels que responsable IA, opérateur d'agents, architecte de flux, *designer de workflows* agentiques ou encore *AgentOps*.

Plus globalement, l'IA pourrait bien provoquer une réévaluation profonde de la valeur des diplômes et de leur impact sur les salaires : les formations permettant de valoriser aussi bien la maîtrise technique des outils et l'esprit critique des humanités seront davantage recherchées, avec une répercussion positive sur les salaires. À l'inverse, les rémunérations pourraient s'effondrer pour les métiers et les postes les plus exposés à l'automatisation, actant vraisemblablement une polarisation extrême du marché du travail et un creusement des inégalités selon les postes.

Tendance lourde 2. Le décalage entre les besoins en recrutement du secteur IT et les compétences disponibles se maintient et se complexifie

DE QUOI S'AGIT-IL ?

Le secteur du numérique fait face à une tension majeure entre des besoins de recrutement en hausse régulière et une difficulté à attirer suffisamment de talents. Ce décalage entre les besoins croissants des organisations et la disponibilité limitée de travailleurs qualifiés pourrait encore être accentué et complexifié avec la diffusion de l'intelligence artificielle et l'apparition de nouveaux métiers aux compétences hybrides. Jadis considérée comme une variable d'ajustement, la « compétence » devient aujourd'hui un levier stratégique de stabilité dans un environnement en mutation constante¹.

LES DYNAMIQUES À L'ŒUVRE

Les métiers de l'informatique et des télécommunications sont classés par l'INSEE depuis 2016 dans la liste des métiers les plus en tension pour les recrutements. Fin 2024, 71% des entreprises du numérique confirmaient rencontrer des tensions de recrutement sur certains postes, freinant leur croissance. Certaines compétences restent particulièrement prisées, comme celles qui permettent de travailler à la cyber-résilience, à la gestion des infrastructures cloud ou encore à la gouvernance et à l'analyse de données. La nécessité d'anticiper ces manques à long terme se fait de plus en plus pressante et selon deux ordres. Les tensions peuvent être quantitatives, en raison de l'accroissement des besoins des organisations en capacités numériques ou de la réinternalisation partielle de compétences. Cette pression pour l'acquisition de talents peut également être qualitative, correspondant alors à un besoin d'actualisation rapide des compétences pour s'adapter aux nombreuses évolutions technologiques. En effet, outre un éventuel décalage persistant entre les programmes des formations initiales et les savoirs réellement mobilisés en entreprise, l'obsolescence des compétences est nettement accélérée et se compte parfois même en mois plutôt qu'en années.

Les difficultés de rétention et d'acquisition sont notamment aggravées par la rapidité des transformations de certaines technologies et des compétences associées. À titre d'exemple, les compétences demandées pour les métiers exposés à l'IA évoluent beaucoup plus vite que pour les autres métiers. Les directions numériques tentent donc de faire évoluer régulièrement les compétences de leurs équipes dans ce domaine par des plans de requalification proactifs (*reskilling*) qui puissent anticiper sans effet de mode la couverture réelle de leurs besoins en *prompt-engineering*, *machine learning*, *Forward Deployed Engineer*, supervision multi-agents, sécurité des modèles et conformité IA, FinOps cloud&AI. La complexification des infrastructures et la multiplication des APIs se traduisent, en effet, par un besoin de compétences de supervision, d'intégration et de sécurisation des systèmes distribués, nécessitant des profils capables de garantir la résilience d'architectures de plus en plus fragmentées. Les organisations affrontent ici le paradoxe de « l'invisibilisation de la complexité » par lequel les infrastructures hybrides et l'IA simplifient l'expérience de l'utilisateur final, tout en masquant une complexité technique exponentielle pour la fonction numérique.

¹ Préparer les organisations aux évolutions de compétences des 10 prochaines années, Cigref, 2025

Pour pallier les défaillances du marché, les organisations s'engagent également dans la création « d'Académies du numérique » internes, visant à industrialiser la certification sur-mesure et la reconversion de leurs propres collaborateurs. Cette mue s'accompagne d'un changement de doctrine RH signant l'abandon de la classique Gestion Prévisionnelle (GPEC) au profit d'une approche dynamique (GEPP), centrée sur l'adaptation continue des trajectoires individuelles. Certaines organisations exigent d'ailleurs que le temps de production libéré par l'IA soit sanctuarisé comme un « vide fertile » et obligatoirement réinvesti dans la formation pour générer des profils hyper-spécialisés.

En parallèle, les évolutions des outils numériques et de leurs usages se traduisent par des besoins accrus de compétences hybrides, croisant expertises techniques (cloud, cybersécurité, jumeaux numériques, filières xOps comme DevSecFinOps ou AIOps) et aptitudes comportementales et émotionnelles fines (leadership et influence, gestion de la complexité systémique, intelligence situationnelle et conduite du changement). La maîtrise technique ne suffisant plus, ces nouveaux métiers imposent désormais une hybridation intégrant la stratégie, le droit, l'éthique et le design des interactions homme-machine.

PERSPECTIVES À L'HORIZON 2040

À l'avenir, les tensions sur les recrutements dans le secteur numérique pourraient encore s'intensifier en France et en Europe, sous l'effet de plusieurs facteurs. Le premier, d'ordre démographique, est dû au mouvement de départ à la retraite d'une partie des collaborateurs actuels, qui, combiné au vieillissement des effectifs toujours en poste qui pourrait bien exercer une pression croissante sur le renouvellement du capital humain. L'allongement des carrières pourrait, de plus, imposer la cohabitation inédite de quatre à cinq générations, obligeant les organisations à gérer activement des frictions liées à des rapports différents au travail et à la technologie. Le second résulte de l'évolution de la population active qui devrait commencer à diminuer en France à partir de 2040 (INSEE), alors même que les besoins en compétences pourraient continuer à croître, fragilisant directement la planification stratégique des effectifs (*Strategic Workforce Planning*) des organisations.

Une forte incertitude demeure concernant l'impact de l'IA sur ces besoins, qui pourraient être limités par l'automatisation toujours plus forte de certaines tâches, voire de postes complets. Les effets de l'IA générative sur les créations de postes restent en effet controversés : selon les fonctions concernées, ils pourraient se traduire soit par des remplacements ou non-crénos de postes, soit par des transformations des postes existants (notamment par un déplacement des besoins vers des tâches de supervision à forte charge cognitive). Dans tous les cas, l'ampleur de la transformation en cours déborde complètement le seul champ technologique et touche à la sociologie par sa remise en cause du fondement du travail salarié, de la création de valeur et de la création de richesse. Le renversement de l'étalon « jour-homme » fixant le rapport entre temps de travail et rémunération ou encore la généralisation des interactions « humains - machines évolutives » imposent de s'interroger sur la nature même du travail. Le défi principal sera d'arriver à absorber avec sagesse une avalanche sans précédent d'évolutions techniques apparues en un laps de temps record.

Tendance lourde 3. Les cyberrisques touchant les collaborateurs se multiplient et se diversifient

DE QUOI S'AGIT-IL ?

En l'espace de quelques années, les cyberrisques auxquels les organisations sont exposées n'ont cessé de s'étendre et de se diversifier, devenant multiformes et ciblant de plus en plus les collaborateurs comme points d'entrée privilégiés. Un décalage persistant s'observe entre la rapidité de diffusion de ces attaques et leur impact systémique d'une part, et la capacité des acteurs à les anticiper d'autre part. Le facteur humain, pilier de toute résilience, constitue également l'interface de vulnérabilité principale par laquelle s'opère le contournement des défenses périmétriques.

LES DYNAMIQUES À L'ŒUVRE

Pour la seule année 2025, le Ministère de l'Intérieur a enregistré près de 450 000 atteintes numériques, soit une hausse de 87% en cinq ans. Les deux tiers des attaques ont visé directement des entreprises (fraudes, extorsions, sabotages). Selon le ministère, les attaques sont à la fois plus nombreuses, plus ciblées et plus difficiles à détecter, notamment quand elles s'appuient sur l'IA ou des crypto-actifs. L'IA facilite en effet l'automatisation des attaques et la production des *deepfakes*, rendant l'ingénierie sociale encore plus crédible. On observe une véritable industrialisation de la cybercriminalité, avec des logiques de spécialisation dans les outils et le type d'attaques.

Loin des escroqueries de masse, les cyberattaques exploitent spécifiquement les salariés pour accéder aux actifs critiques de leur employeur. Elles prennent la forme de *phishing* ciblé (*spear-phishing*), de piratage de comptes à hauts privilèges, de compromission des accès distants ou de fraude au président. Le collaborateur est ainsi instrumentalisé à son insu pour faciliter le mouvement latéral des attaquants au sein du réseau de l'entreprise.

Toutes les organisations, publiques et privées, sont désormais touchées par des cyberattaques caractérisées par plusieurs transformations : le ciblage des fournisseurs de confiance eux-mêmes (Microsoft, Fortinet), la sophistication des attaques (qui portent sur la chaîne d'approvisionnement logicielle, ou qui exploitent des techniques d'ingénierie sociale), le ciblage d'infrastructures critiques pour les organisations, et la diversification des surfaces d'attaque (équipements de bordure, API, cloud-SaaS, Shadow IT/IA, convergence IT/OT). Par ailleurs, la dimension géopolitique des cyberattaques s'accroît, orchestrée par des acteurs étatiques agissant seuls ou en partenariat avec des cybercriminels (cyber-proxies). Elles visent parfois des infrastructures ou des organisations stratégiques, à des fins de vol de données, d'espionnage industriel, ou de déstabilisation politique. En 2025, les attaques par déni de service distribué (DDoS) ont ainsi représenté 89% des revendications d'activisme.

L'IA permet d'automatiser et d'améliorer la pertinence des attaques, mais aussi de les multiplier. Selon une enquête menée par le BCG auprès de 500 entreprises dans le monde, 60% d'entre elles auraient subi une cyberattaque impliquant l'IA en 2025. Par ailleurs, on assiste à une croissance des offres de lutte informatique offensive, comme celles proposées par le logiciel espion Pegasus de l'entreprise israélienne NSO Group, faisant peser une menace permanente d'interception sur les terminaux mobiles des dirigeants et des collaborateurs clés.

PERSPECTIVES À L'HORIZON 2040

À l'avenir, la cybercriminalité pourrait assurément continuer à se professionnaliser et à s'industrialiser, à l'image du crime organisé. Son coût pour la communauté mondiale dépasserait déjà 10 000 milliards de dollars par an, selon les estimations de VikingCloud, et il pourrait avoir des conséquences plus grandes sur l'économie réelle, avec des effets bien visibles sur l'évolution du PIB. Le « *cybercrime as a service* » pourrait encore se développer, avec pour conséquence une augmentation du nombre de plates-formes spécialisées proposant des solutions de *malware*, *ransomware* et *phishing* clés en main pour infiltrer les systèmes d'information.

L'IA pourrait rendre les attaques visant les collaborateurs à la fois plus faciles à lancer, de meilleure qualité et de plus en plus difficiles à détecter, grâce à des *deepfakes* ou à « l'empoisonnement » des modèles d'IA professionnels, des appels par ingénierie sociale ou autres attaques ultra-ciblées (imitant des membres du Comité Exécutif, des fournisseurs stratégiques, ou des administrations). La guerre de l'information, champ d'attaque qui vise plutôt le grand public, pourrait alors se déporter directement sur les employés pour manipuler leurs décisions professionnelles quotidiennes. Enfin, l'hyper-délégation des tâches pourrait faire émerger un nouveau vecteur critique. Les agents autonomes ou jumeaux numériques des collaborateurs pourraient devenir de nouvelles sources de vulnérabilités, et être attaqués par d'autres IA pour exfiltrer des données ou saboter des flux métiers sans aucune interaction humaine.

Tendance émergente 1. L'IA agentique remet en question les stratégies traditionnelles de sourcing RH et pourrait favoriser une relocalisation de certaines activités

L'IA agentique se diffuse au sein des directions numériques, démultipliant à court terme leur capacité à internaliser à un coût marginal encore faible des processus entiers. Ce mouvement pourrait se traduire par une diminution drastique du recours à des prestataires externes (*Business Process Outsourcing*, BPO) ou des centres de services implantés à l'étranger. En effet, les agents IA ne se limitent plus à l'assistance et sont déjà capables de se substituer partiellement ou totalement à des tâches complètes aujourd'hui réalisées par des humains sur des opérations de support, d'administration système ou d'interaction client¹. Compte tenu de leurs rapides progrès, ils pourraient évoluer du rôle d'assistants à celui de binômes autonomes à manager². D'ici 2028, près de 40% des grandes entreprises des pays développés pourraient intégrer ces agents autonomes comme des binômes opérationnels à part entière (*Capgemini*).

Dans ce contexte, l'intérêt de recourir à des prestataires externes pour des tâches de *run* ou de support applicatif standard s'effondre. Capables d'opérer 24h/24, nativement intégrés aux systèmes de l'organisation et exempts des contraintes de coordination inter-fuseaux, ces agents videraient de leur substance la valeur ajoutée des prestations *offshore* traditionnelles. Plus de 90 % des décideurs technologiques envisagent d'ailleurs explicitement l'IA agentique comme une alternative stratégique directe aux modèles de sourcing délocalisés (*offshore* et *nearshore*). À mesure que les agents diagnostiquent des incidents, appliquent des correctifs et orchestrent des flux complexes, la pertinence d'une sous-traitance humaine d'exécution se réduit drastiquement avec des effets d'ores et déjà visibles sur le chômage de masse en Inde.

Cette mutation du travail pourrait conduire à une transformation des modèles de sourcing des organisations et plus globalement des chaînes de valeur. Plutôt qu'une opposition entre internalisation et externalisation, les entreprises pourraient privilégier une nouvelle répartition des activités, dans laquelle les tâches d'exécution seraient davantage automatisées, tandis que les fonctions de pilotage, de gouvernance, de cybersécurité et de supervision des agents gagneraient en importance. Cette dynamique pourrait favoriser la relocalisation de certaines compétences, tout en réduisant le nombre de postes consacrés aux tâches les plus standardisées.

Elle n'exclut toutefois pas l'émergence de nouvelles formes d'externalisation, de dépendances et de risques. Certaines organisations pourraient en effet choisir de recourir à des agents d'IA proposés sous forme de services par des prestataires spécialisés. Les enjeux de supervision, de gouvernance, de sécurité des données et de maîtrise des dépendances se déplaceraient alors des équipes humaines vers les agents eux-mêmes. Selon le *Digital Trust Digest*, 69 % des professionnels de la cybersécurité considèrent d'ailleurs que les vulnérabilités propres aux agents d'IA constituent désormais une menace plus importante que leur utilisation malveillante par des acteurs humains.

¹ Do Tank Impacts de l'IA sur les activités d'ingénierie logicielle, « Optimisation du support », Cigref, Janvier 2026

² Do Tank Impacts de l'IA sur les activités d'ingénierie logicielle, « Développeur augmenté & Passage à l'échelle », Cigref, Janvier 2026

Incertitude 1. Le *Shadow AI* pourrait devenir un vecteur d'exfiltration de données sensibles et fragmenter la cohésion au sein de l'organisation

Le *Shadow AI*, qui concerne aujourd'hui près de la moitié des salariés utilisant l'IA, pourrait consacrer l'évasion massive des pratiques professionnelles hors des systèmes d'information contrôlés, au profit des terminaux personnels des collaborateurs. Poussés par une quête d'efficacité immédiate et de confort cognitif, ces derniers s'engageraient dans un « bricolage pragmatique » clandestin pour résoudre les frictions du travail réel.

Cette dynamique souterraine ferait peser un double risque critique sur les organisations. D'une part, un péril sécuritaire et juridique actant la « privatisation par le salarié des gains de productivité, au prix d'une mise en risque des données de l'entreprise ». D'autre part, un risque managérial systémique, où l'usage solitaire et dissimulé de la machine viendrait fragmenter le corps social de l'organisation. Face à cette menace, l'illusion d'une interdiction stricte s'effondrerait : la répression ne ferait que renforcer l'opacité et la fuite des pratiques.

À l'horizon 2040, les directions du numérique devront avoir réussi un dialogue et la mise en place de moyens techniques pour faire émerger des pratiques positives de l'IA (*Citizen AI*), combinant outils personnels et professionnels, tout en déployant des alternatives internes performantes et faciles d'accès.

Incertitudes majeures

Incertitude 2. La mise à niveau des compétences cognitives pourrait imposer une redéfinition des responsabilités entre l'État et les organisations

La démocratisation des technologies d'IA pourrait déplacer la fracture numérique du seul accès aux technologies vers la capacité à les comprendre, les maîtriser et les utiliser efficacement. Cet élargissement de la fracture sur le terrain capacitaire et cognitif pourrait soulever un enjeu macroéconomique majeur, en transformant profondément les conditions de formation, de financement et de maintien de l'employabilité de la population active.

L'incertitude porte notamment sur la répartition de cet effort entre sphères publique et privée. D'un côté, l'État pourrait être sommé d'adapter en urgence le cycle de formation initiale des élèves et de raccourcir les délais d'actualisation des programmes afin d'éviter un déclassement massif d'une partie de la population active. De l'autre, face à une éventuelle inertie de l'appareil public, les entreprises pourraient être amenées à prendre en charge une part croissante de l'adaptation des compétences de leurs collaborateurs, par la création d'académies internes et le déploiement massif de programmes d'*upskilling* et de *reskilling*.

À l'horizon 2040, au-delà du seul effort de formation et d'équipement, la pression réglementaire et réputationnelle pourrait également conduire les organisations à devoir rendre compte de leur capacité à préserver l'autonomie intellectuelle et le jugement critique de leurs collaborateurs face à l'usage croissant de systèmes d'IA. Si aucun équilibre efficace ne parvenait à se structurer entre responsabilités publiques et privées, le marché du travail européen pourrait connaître une polarisation accrue entre travailleurs et organisations capables de suivre cette accélération technologique et ceux qui en seraient progressivement éloignés, au risque d'affaiblir durablement la compétitivité européenne.

Hypothèse 1. La démocratisation du « jumeau professionnel » provoque une crise de la propriété intellectuelle et redéfinit le salariat

D'ici 2040, l'intégration d'une IA personnelle (« jumeau professionnel ») entraînée sur les méthodes, les données et l'environnement de travail de chaque salarié devient la norme. Cet agent autonome ne se contente plus d'assister : il se substitue au collaborateur pour exécuter des flux complexes, interagir avec d'autres systèmes et prendre des décisions opérationnelles. L'apprentissage continu de cette IA engendre un choc de gouvernance majeur. L'appropriation algorithmique des savoir-faire brouille la frontière entre le capital immatériel de l'entreprise et la compétence propre de l'individu. Ce transfert de l'expertise humaine vers la machine impose aux organisations de trancher juridiquement la propriété des connaissances acquises par l'agent, sa portabilité en cas de départ, et la chaîne de responsabilité civile et pénale en cas de décision dommageable. La délégation algorithmique ouvre également la voie au « poly-emploi » automatisé, où les capacités d'un jumeau pourraient être monétisées simultanément auprès de plusieurs employeurs, disloquant le cadre historique du salariat.

Hypothèse 2. L'imposition d'un « droit à la non-automatisation » structure le nouveau segment de marché du « Premium Humain »

D'ici 2040, face à l'industrialisation cognitive et à la standardisation des services algorithmiques, un « droit à la non-automatisation » s'impose de manière réglementaire et commerciale. Loin d'être une simple revendication syndicale, ce principe se transforme en un avantage concurrentiel assumé pour sanctuariser des activités exigeant une responsabilité morale, juridique ou créative (santé, justice, éducation, assistance, création). L'intervention humaine non intermédiée devient un marqueur de rareté et de luxe. Les organisations déploient des certifications « 100 % Humain » qui garantissent l'authenticité, la confidentialité absolue et l'absence de biais. Le marché se scinde alors brutalement entre un service de masse *low-cost*, piloté par l'IA agentique, et un service *premium*, fondé sur l'exclusivité du jugement humain, redéfinissant ainsi la cartographie de la valeur ajoutée.

Hypothèse 3. L'asymétrie cognitive induite par les usages de l'IA provoque une fracture de la capacité de jugement

D'ici 2040, la fracture numérique ne se mesure plus à l'aune de l'accès à l'équipement, mais bascule sur le terrain purement cognitif. L'essor de l'IA générative instaure une asymétrie radicale de la productivité et du discernement. D'un côté, une élite intellectuelle maîtrise l'art de l'orchestration algorithmique, conservant son esprit critique pour auditer la machine, démultipliant ainsi sa valeur sur le marché. De l'autre, une majorité d'individus subit une atrophie de ses compétences analytiques, sombrant dans une dépendance structurelle à des systèmes d'aide à la décision dont ils ne comprennent plus la logique. Cette sous-traitance généralisée du jugement enferme les utilisateurs dans des bulles cognitives dictées par l'algorithme, menaçant la capacité d'innovation autonome des organisations et posant, à terme, la question de la pérennité du libre arbitre professionnel.

Membres du Conseil d'Orientation Stratégique

Membres du Cigref

Lionel Chainé - BPIFRANCE
David Krieff - AÉROPORTS DE PARIS
Pascale Montrocher - SFR
Sandrine Racouchot - ABEILLE ASSURANCES
Emmanuel Sardet - CRÉDIT AGRICOLE

Personnalités qualifiées

Yves Bernaert - ISG & 1001FONTAINES
Nicolas Bouzou - ASTERÈS
Cécile Méadel - UNIVERSITÉ PANTHÉON-ASSAS
Julien Nocetti - CENTRE D'ANALYSE, DE PRÉVISION ET DE STRATÉGIE, MEAE
Arno Pons - DIGITAL NEW DEAL & ASSOCIATION DIGITAL RESILIENCE INITIATIVE

Membres du Conseil d'Orientation Stratégique Jeunes

Formé en 2023, le Conseil d'Orientation Stratégique Jeunes est constitué de collaborateurs de moins de trente ans, issus des organisations membres du Cigref, qui contribuent aux travaux du ROS.

AIOUAZ Selma - FONDATION DE FRANCE
AMMAR Dhia Eddine - CNAM
ASNACIOS Youri - MTE
BARRÉ Logan - SOCIÉTÉ GÉNÉRALE
BERNARDO Christelle - MINISTÈRES SOCIAUX
BINEL Oann - CNES
BRASSEUR Charlotte - SOCIÉTÉ GÉNÉRALE
CAO Caroline - SOCIÉTÉ GÉNÉRALE
CELOSIA Guillaume - SAVENCIA
CHANA Naomi - EIFFAGE
CHAUVIN Etienne - AIR FRANCE-KLM
DELAUNAY Clément - SODEXO
FILICHKINA Alena - SODEXO
GODART Arthur - THALES
GRESSET Erwan - MSA
HENOUNE Asma - SOCIÉTÉ GÉNÉRALE
JOUBERT Chloé - ICADE
LALLEMENT Julie - AG2R LA MONDIALE
MALFARA Elio - FRANCE TRAVAIL
MARTINEZ Tom - AIR FRANCE-KLM
MILLEVILLE Camille - LVMH
MOUNAIX Marion - AIR FRANCE-KLM
PETIT Stéphane - THALES
RAMSAMY Cyril - AIRBUS
ROCHER-MONNIER Vincent - AIR FRANCE-KLM
ROLLIN Guillaume - CNES
SECHIER Hugo - STELLANTIS

Remerciements

Le Cigref souhaite chaleureusement remercier les membres du Conseil d'Orientation Stratégique, du Conseil d'Orientation Stratégique Jeunes et tous les membres du Cigref pour leur contribution riche et stimulante.

Pour la septième année consécutive, nous remercions également l'équipe de Futuribles, partenaire historique du Cigref, pour son accompagnement dans l'élaboration de cette vision prospective.

Ce rapport, destiné tout d'abord aux membres du Cigref, s'adresse également à l'ensemble de l'écosystème du numérique et à toutes les personnes intéressées par les enjeux numériques et une approche multidisciplinaire et prospective de ceux-ci.

Rédaction

Pierre Skrzypczak, Chargé de mission senior, Cigref

En collaboration avec Futuribles

Cécile Désaunay, Directrice d'études

Juliette Guilbaud, Chargé d'études

Contributions équipe Cigref : Aymeric Bourdin, Célia Culi, Lysandre Mazuer

Relecture : **Chantal de Bardies**, Directrice des contenus, Cigref

Direction artistique et Communication : **Émilie Grange**, Chargée de communication, Cigref

Illustrations originales : **Fix** (<https://fix-dessinateur.com/>)

Ce rapport a été réalisé par HandiPRINT, entreprise adaptée qui emploie 120 personnes en situation de handicap, dans la gestion globale de documents imprimés. Plus d'informations : www.handi-print.fr



Cigref
www.cigref.fr
21 avenue de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr