Livre blanc sur le futur des infrastructures numériques et le positionnement des acteurs des secteurs impliqués

CSF infrastructures numériques

Sous-groupe innovation (SGT2)

06/07/2026

1. Les raisons et les objectifs généraux de cette publication

Les évolutions technologiques impactent de façon de plus en plus importante les acteurs traditionnels des chaînes de valeur des infrastructures numériques (équipementiers, opérateurs, producteurs/distributeurs de contenus/applications…)[1]. À titre d'exemple, les nouvelles architectures de réseau, notamment 5G/6G, font appel à des paradigmes issus des écosystèmes *cloud*, lesquels sont largement dominés par des acteurs non-opérateurs et non équipementiers (dont les GAFAM). Ces évolutions offrent de nouvelles opportunités tout en faisant peser une menace existentielle sur certains secteurs, celui des télécommunications bien sûr mais aussi les filières critiques utilisatrices des réseaux (notamment les OIV2), et donc globalement pour certaines sociétés et économies, comme les européennes.

Il s'agit d'un sujet largement débattu mais dont le cadre général et les principaux risques sont insuffisamment identifiés et surtout nécessitent une analyse fine des enjeux et des impacts. Le sujet est souvent abordé sous des angles d'analyse partiels, comme celui d'un type d'acteurs, ou celui d'un type d'impact. Or, l'analyse de l'impact des évolutions technologiques sur les marchés des acteurs des télécommunications, du *cloud* et de l'IA, entre autres, requiert une vision plus globale, d'autant plus que les frontières entre filières s'estompent progressivement.

Les objectifs de ce livre blanc sont de :

- Poser une vision holistique de l'écosystème des infrastructures numériques face à ces évolutions, des acteurs impliqués, de l'impact de ces évolutions et des initiatives de structuration des réflexions qui contribuent à orienter ces évolutions

[1] Il n'existe pas une définition universellement utilisée du terme « infrastructure numérique ». Les diverses définitions existantes se confrontent à des difficultés, souvent générées par les évolutions technologiques et notamment la *softwarisation* généralisée (passage à des solutions essentiellement logicielles) de ces infrastructures, concept que nous introduisons plus tard. Afin de faciliter la lecture en donnant un cadre générique, nous donnons ici une définition adaptée aux objectifs du document, axée sur la différenciation entre les « infrastructures numériques » et les services numériques. Les infrastructures numériques permettent de créer et fournir les services. Elles sont composées de réseaux de communication, de ressources de calcul et de stockage distribuées sur des *data centers* (qui font partie intégrante de ces infrastructures), dans les réseaux (notamment le concept de *mobile edge computing*, MEC, présenté dans le document) et à l'*edge* (au-delà des frontières des réseaux d'opérateur, dans des réseaux et équipements terminaux, notamment des réseaux véhiculaires, des smartphones et autres types d'objets connectés). Ces infrastructures sont également composées de briques logicielles nécessaires à l'orchestration des services numériques. Cela peut concerner des aspects d'opération de ces infrastructures, mais également des briques génériques de sécurité, de facturation, d'orchestration de services, d'orchestration d'agents d'IA, etc.

La difficulté avec une définition d'infrastructures numériques est liée au fait que les diverses briques technologiques qui les composent offrent des services à d'autres briques pour globalement construire ces infrastructures flexibles. Il faut donc identifier, à chaque niveau d'analyse, quels sont les services internes aux infrastructures et les services externes, ces derniers étant créés et fournis grâce aux infrastructures.

[2] OIV – Opérateur d'Importance Vitale

- Analyser les opportunités et les risques pour ces acteurs et comment ceux-ci se traduisent dans des opportunités et des risques plus globaux pour nos sociétés et nos économies
- Faire des recommandations et proposer des actions pour faciliter la construction d'un plan d'action global permettant de tirer parti des opportunités et de mitiger les risques.

Ces recommandations viseront à :

- Renforcer, par le numérique et en particulier par l'IA, le pouvoir de comprendre et d'agir des citoyens et des entreprises (*empowerment*), en garantissant qu'ils disposent et disposeront de tous les outils disponibles, à l'état de l'art international et à l'état global des affaires. Éviter ainsi le risque que les Européens et notamment les Français ne deviennent des citoyens de deuxième zone à l'échelle mondiale, faute d'un accès suffisant aux outils numériques de dernière génération
- Faciliter le positionnement national et international des entreprises du numérique, des grands groupes aux TPE et start-ups, existantes et émergentes, dans un cadre de compétitivité globale
- Faciliter l'innovation et l'émergence de nouveaux services et applications à fort impact sociétal et économique
- Maintenir et développer une recherche académique de haut niveau qui alimente et soutient les processus d'innovation.
- Protéger les citoyens et les entreprises contre toute attaque visant tout objectif : vol de données, perturbations de services, destructions de biens, attaques physiques aux personnes, etc.

Ces enjeux peuvent être résumés ainsi : l'objectif central est d'assurer la souveraineté numérique et d'en faire un levier de souveraineté civile et militaire.

Se pose alors la question de la définition même de la souveraineté numérique visée. Au sens le plus strict, cela pourrait signifier de contrôler toute la chaîne technologique, toutes les infrastructures et tous les services et applications. Ceci est aujourd'hui et à court et moyen terme illusoire, au regard des investissements et du temps nécessaire, même si la France dispose des compétences pour le faire. Il convient donc de préciser le périmètre de la souveraineté recherchée ainsi que le niveau de contrôle visé (souhaité et faisable à divers horizons de temps).

Dans la section suivante nous introduisons les principales transformations en cours dans le large domaine des infrastructures numériques. Puis nous revenons, sur ces bases, sur la chaîne technologique et sur les enjeux de souveraineté associés.

2. Une vision d'ensemble des transformations en cours

Nous traitons ici avec un peu plus de détail, mais avec un regard stratégique, les évolutions technologiques qui sous-tendent les évolutions structurelles induites par le numérique. Ces évolutions technologiques peuvent se caractériser autour d'un nombre réduit de changements de paradigmes, dont la *softwarisation* (fonctionnalités réseaux rendues par du logiciel) et virtualisation des infrastructures, la convergence progressive entre les réseaux et le *cloud*, l'IA (dont l'IA agentique, de plus en plus distribuée et multi-acteurs), les jumeaux numériques, intégrant notamment des *world models (*simulation du modèle physique*),* qui définissent de nouveaux modes d'interaction entre le monde physique et le monde numérique, ainsi que l'ouverture des infrastructures numériques aux acteurs externes. Ce dernier point transforme les infrastructures du numérique dans des plateformes de services, permettant à ces derniers d'être conçus et établis en temps réel, en orchestrant des composants d'acteurs multiples, pour répondre dynamiquement à des besoins spécifiques et évolutifs.

2.1. Réseaux et verticaux, un changement de paradigme

Les générations successives des réseaux mobiles ont historiquement poursuivi comme objectifs majeurs l'augmentation de la capacité, des débits et de la couverture, à des coûts rendant économiquement rentable leur déploiement. Avec l'avènement de la 5G, un changement de paradigme est introduit : la conception partiellement synergétique avec divers secteurs d'activité, tels que les transports et l'industrie du futur (mentionnons par exemple les initiatives *5G Automotive Association, 5G Alliance for Connected Industries and Automation* et *Software Republic*).

De manière simplifiée, nous sommes passés d'une logique où les réseaux étaient conçus et déployés, puis le marché décidait "quoi en faire", à une logique dans laquelle un travail sur les possibles cas d'usage est réalisé très en amont et avec une participation directe de divers secteurs d'activité. Il en ressort des spécifications fonctionnelles et non fonctionnelles mieux adaptées aux besoins réels de ces secteurs.

Ainsi, les divers secteurs d'activité ne se limitent plus à être des utilisateurs des réseaux, mais deviennent des partenaires technologiques de ceux en charge des infrastructures numériques. De nos jours, cela dépasse largement l'identification de cas d'usage pour passer à une co-conception des systèmes. Les réseaux véhiculaires (mobilités route/fer/air), en tant qu'extension d'un réseau d'infrastructure, représentent un exemple bien connu. De manière plus générale, les réseaux dits *à l'edge* (au bord) deviennent progressivement une partie intégrante des infrastructures du numérique.

Nous verrons par la suite que les interactions technologiques entre les réseaux et divers verticaux se diversifient fortement avec les nouvelles générations de réseaux, donnant lieu à des évolutions majeures d'architectures, de services et de modèles économiques. Cela est encore plus significatif dans le cadre des réseaux privés ; ces derniers étant un des atouts clés pour la diffusion de la 5G et des réseaux du futur en général.

Cette interpénétration accrue se traduit par une dépendance fortement croissante des divers secteurs d'activité vis-à-vis des infrastructures du numérique, imposant sur celles-ci de nouvelles contraintes, notamment en termes de sûreté et de sécurité, mais également en termes de flexibilité (création automatique et dynamique de réseaux dans le cadre de systèmes virtualisés) et de latence (notamment dans le cadre du contrôle de sites industriels).

2.2. Convergence réseaux-*cloud*, MEC

En 2012, un groupe de treize opérateurs de télécommunications, dont Orange, a publié un livre blanc[3] qui introduit le concept de virtualisation des fonctions réseau (NFV pour *Network Functions Virtualization*). Ce document a représenté en quelque sorte la validation de concepts qui étaient déjà étudiés, mais dont on doutait fortement de l'acceptabilité massive par ces acteurs.

Historiquement, les équipements de réseau télécoms ont été construits comme des solutions *hardware*, spécifiques à chaque équipementier et utilisés comme des boîtes noires. Ce mode de fonctionnement présente de nombreux inconvénients : les difficultés et délais pour introduire de nouvelles fonctionnalités, le coût élevé et la dépendance technologique (dans un cadre d'émergence d'acteurs majeurs non européens). Certes les réseaux sont depuis des décennies standardisés, mais en fait seules les interfaces entre grands blocs fonctionnels faisaient l'objet de ces standards.

Le document mentionné, partiellement motivé par le grand succès des centres de calcul, capables d'implémenter avec flexibilité une multitude de fonctionnalités, services et applications, préconise le remplacement des équipements dédiés par un *hardware* générique (serveurs informatiques) et l'implémentation logicielle des fonctionnalités réseaux.

La *softwarisation* des réseaux est ainsi formalisée et fortement accélérée.

En conséquence, d'une part, de très nombreuses fonctions réseau sont aujourd'hui offertes en mode *cloud*, y compris pour l'accès radio (*cloud*-RAN) et ce phénomène s'accélère, d'autre part, le *cloud* sort des grands *data centers* pour se déployer jusqu'aux extrémités (le terme *edge* est utilisé dans la littérature) et notamment au niveau du MEC (*Mobile Edge Computing* ou *Multi-access Edge Computing*), permettant la mise en place de nombreuses nouvelles applications, notamment celles sensibles à la latence (temps de réponse) ou nécessitant une protection particulière des données. Ceci joue un rôle central dans les interactions avec les verticaux mentionnés plus haut. Le terme *edge* tel qu'utilisé dans ce contexte fait référence, soit à des points de présence des réseaux proches des clients finaux (bien plus proches que les grands *data centers*), ce qui est le cas du MEC, soit à des équipements côté usager, comme des terminaux, des voitures ou autres objets connectés.

Prises conjointement, ces évolutions permettent de parler de convergence, voire d'interpénétration, entre réseaux et cloud. L'utilisation du paradigme *cloud* dans les architectures de réseau permet à ces derniers d'introduire une très grande agilité et flexibilité,

[3] Network Functions Virtualization - An Introduction, Benefits, Enablers, Challenges & Call for Action.

et le déploiement de ressources *cloud* dans les points de présence des réseaux permet aux *clouds* une grande diversité de nouvelles applications et usages.

Tout cela est possible grâce à la virtualisation des fonctions, qui de ce fait peuvent être ajoutées, éliminées ou déplacées dynamiquement. En effet, les fonctions, devenues purement logicielles et tournant sur du matériel générique, ne sont plus enfermées dans des boîtes noires. Cette virtualisation n'est pas qu'une nouvelle manière de construire un équipement de réseau, elle permet de construire un réseau sur une architecture de type *cloud*, toutes les fonctions réseaux pouvant être implémentées par des briques logicielles portées en mode *cloud* (sauf le câblage et les antennes RF, bien évidemment).

2.3. Ouverture des réseaux

Les évolutions mentionnées plus haut sont un facilitateur majeur pour l'ouverture des réseaux. Cette ouverture se met en place de trois manières principales. D'une part, les architectures des réseaux deviennent potentiellement plus ouvertes permettant à une diversité d'acteurs de proposer des composants de réseau et aux opérateurs de construire leur réseau en déployant et interconnectant des composants de fournisseurs différents. C'est le cas notamment des solutions Open RAN. D'autre part, deux évolutions bien plus structurelles par rapport aux évolutions des filières se mettent en place : d'abord, les réseaux proposent des interfaces qui permettent à d'autres acteurs de contrôler une « partie » du réseau, typiquement celle qui leur est attribuée, puis des acteurs extérieurs peuvent placer dans les systèmes convergents réseau-*cloud* leurs propres fonctionnalités. Ce concept se généralise et introduit de nouveaux changements de paradigme, comme nous le verrons plus bas.

Un élément clé des architectures ainsi définies est l'orchestrateur, l'intelligence qui permet à chaque instant d'identifier les fonctionnalités nécessaires, de les agencer et de leur attribuer les ressources dont elles ont besoin.

Toutes ces évolutions sont en cours, mais sont loin d'avoir abouti malgré leur intérêt certain pour les usagers. Une des raisons est que, même si la technologie répond plutôt bien aujourd'hui aux besoins de convergence mentionnés (dans des cadres restreints qui ne couvrent pas les évolutions à venir présentées plus bas), les filières industrielles concernées se trouvent dans une situation de concurrence de plus en plus forte et de ce fait ont du mal à trouver les moyens et le temps, ainsi que les modèles économiques et d'affaires, pour opérer une plus forte convergence.

2.4. Des services réseaux aux plateformes du numérique

La dernière étape dans l'ouverture mentionnée plus haut consiste dans la possibilité pour des acteurs tiers de déployer leurs propres composants dans les infrastructures convergentes réseau-*cloud*. Ces fonctionnalités, développées par des tiers, portées ainsi par les infrastructures convergentes réseau-*cloud*, sont notamment en lien avec des services (de tout type, pas uniquement services réseau) et des applications fournies également par des acteurs tiers, pas nécessairement les mêmes que ceux qui déploient ces fonctionnalités.

L'ouverture du cœur de réseau pour accueillir de telles fonctionnalités rend même possible l'émergence d'une *marketplace* de ces fonctionnalités déployées sur les infrastructures que nous traitons et ouvre ainsi de nombreuses opportunités et des risques importants.

L'idée générale, posée de manière « caricaturale », serait de voir les infrastructures convergentes réseau-*cloud* comme un environnement PaaS (*Platform as a Service*) qui accueille de nouvelles fonctionnalités, de divers acteurs tiers, permettant de construire dynamiquement, à la demande, de nouveaux services et applications. Toute la chaîne, en partant du réseau lui-même, pouvant être construite à la demande et en temps réel.

Ce type de solutions est aujourd'hui plus prospectif, mais envisageable dans un horizon de 3 à 5 ans. Néanmoins, des verrous sont à lever, notamment dans la conception de nouveaux types d'orchestrateurs, dans la conception de mécanismes de validation des propriétés des composants acceptés dans la *marketplace*, dans la spécification des niveaux de qualité sur divers critères à exiger de ces composants, etc.

2.5. Vers les services multisectoriels

Indépendamment des évolutions que nous venons de mentionner, une autre transformation se met en place. La transformation numérique, qui jusqu'à présent s'est faite en silos, par secteur d'activité, passe à une nouvelle phase, avec l'avènement de services multisectoriels. Dans ce cadre, des acteurs de secteurs d'activité différents collaborent pour développer conjointement des services fortement innovants s'appuyant sur les services et les données de chacun, tout en gardant la maîtrise de leurs données, de leur IA (notamment de leurs agents) et de leurs infrastructures. Selon les modèles économiques choisis, ils peuvent aussi être en « coopétition ». La convergence réseau-*cloud* et l'ouverture des réseaux représentent clairement des facteurs d'accélération de cette tendance émergente.

2.6. L'IA pour les infrastructures numériques

Face à l'explosion de la complexité engendrée par les évolutions mentionnées plus haut, des approches de conception, planification, opération, contrôle, maintenance, etc. basées sur de l'intelligence artificielle et l'utilisation de jumeaux numériques sont en cours d'étude, mais encore dans des stades très embryonnaires.

Nous sommes donc dans un cadre général qui permet de clairement identifier la voie, vu les avantages indiscutables des solutions décrites, mais dont il est très difficile d'évaluer les horizons de temps auxquels des solutions stables seront disponibles.

2.7. Les infrastructures numériques pour l'IA

Quand on parle de ce sujet, le premier réflexe est de penser à l'augmentation des besoins de capacité, notamment de communication. Mais les défis sont bien plus structurels[4]. L'IA devient de plus en plus distribuée, notamment dans le cadre de l'IA fédérative et de l'IA agentique. Ces technologies sont particulièrement intéressantes dans le cadre de collaborations multi-acteurs. Mais ces collaborations requièrent un plan de gouvernance des données et de l'IA et des orchestrateurs d'agents qui interagissent avec ce plan de gouvernance. Ce plan de gouvernance permet de suivre le comportement des agents, tous en « respectant » leur autonomie, mais en garantissant qu'ils ne débordent pas de leur mandat, que les règles d'accès entre eux soient respectées, que les échanges soient bien tracés, etc. Ce plan de gouvernance, qui doit respecter la réglementation (européenne notamment : *Digital Services Act*, *AI Act*, RGPD…) et ses évolutions, doit encore être conçu.

Pourquoi le trafic IA nécessite des évolutions du réseau ?

Nous entrons dans une nouvelle phase où le changement clé n'est pas simplement « plus de trafic », mais un changement dans la « forme » du trafic, de plus en plus alimenté par l'IA. Les applications pilotées par l'IA sont interactives et en rafale, remplaçant les sessions stables par des pics créés par des événements qui peuvent modifier les ratios traditionnels entre liaison descendante et liaison montante à mesure que les utilisateurs ne se contentent pas de « consommer » mais « créent et détectent ». Cette évolution du trafic montant amène une pression particulièrement forte dans le cas des réseaux mobiles. Les moyennes mondiales peuvent n'évoluer que modestement, mais la variance locale s'élargit avec les marchés et les zones à forte demande. La planification des accès devient un défi majeur car le trafic est structurellement modifié par le rythme d'adoption des appareils, la mobilité et les rafales déclenchées par des événements. Les réseaux doivent donc être conçus pour s'adapter à des comportements très variables plutôt que basés sur une évaluation statique des besoins aux heures de pointe. Ce même dynamisme se répercute dans le plan de contrôle, où l'IA interactive augmente la charge de signalisation et le changement de politiques du fait des interactions fréquentes avec des services axés sur le contexte.

« L'IA physique » accélère ces mutations. Les robots, véhicules autonomes et capteurs industriels perçoivent l'environnement *via* la liaison montante et agissent en temps réel sur les décisions. Dans ce monde, le réseau devient moins un « tuyau de contenu » qu'un système nerveux. Les boucles critiques pour la sécurité passent de dizaines de millisecondes à quelques millisecondes, et, dans des déploiements locaux étroitement délimités, vers des régimes inférieurs à la milliseconde. Dans cet environnement, une baisse de fiabilité ou de latence peut devenir un enjeu de sécurité. À mesure que l'IA et le trafic physique d'IA évoluent rapidement, la demande d'adaptabilité, de fiabilité et de réactivité augmente. Les applications natives de l'IA ont de plus en plus besoin de décisions conscientes de l'intention, ce qui, en pratique, nécessite une orchestration coordonnée de l'accès radio

[4] Nous reviendrons sur la question de la capacité, en effet, il y a quand même sur ce sujet un point important : les nouvelles formes d'IA requièrent des capacités symétriques dans les 2 sens de communication.

(RAN), du cœur, de l'accès au transport et du transport plutôt qu'une optimisation domaine par domaine.

2.8. Convergence réseau-*cloud*-IA Ouverture et Hyperscalers, un futur incertain

L'ensemble des évolutions mentionnées dans les paragraphes précédents pose de manière encore plus centrale la question des investissements et du partage de la valeur entre les filières historiques et notamment entre opérateurs de télécommunications et hyperscalers (opérateurs de « *cloud*s » multi-usage, basés sur de très grands *data centers*, souvent eux-mêmes fournisseurs d'applications ou de terminaux). Depuis plus de 20 ans (Google, par exemple, a été créé en 1998 et le premier iPhone date de 2007), cette question du partage de la valeur est soulevée par les opérateurs qui sont les principaux investisseurs dans les infrastructures de réseaux qui supportent les services des hyperscalers. Ils disposent ainsi du contrôle de ces réseaux et des ressources confortables de communication associées. Les évolutions mentionnées risquent de réduire fortement leur positionnement clé dans la chaîne de valeur et faire émerger une concurrence par la fourniture directe de services de communication par des acteurs de type « *hyperscalers* ».

À ceci doivent être ajoutés les investissements des hyperscalers dans des câbles sous-marins de très grande capacité, la croissance forte du marché des réseaux non terrestres (avec notamment les constellations de satellites en orbites basses et moyennes) avec la concurrence accrue qui se dessine dans ce domaine et la multiplicité d'opérateurs de télécommunications en Europe qui se traduit par le fait que les entreprises en question ont un poids financier limité (en comparaison aux autres acteurs mentionnés), les risques existentiels pour les opérateurs de télécommunications, mais aussi pour les équipementiers fournisseurs historiques de ces derniers, sont réels.

Limiter l'impact de ces risques impose une vision holistique des acteurs impliqués, des évolutions technologiques, des nouveaux modèles d'affaires, de la réglementation, etc. Cette vision globale peut se placer dans le cadre du *continuum* numérique. Nous proposons de structurer deux types, complémentaires, de *continuum* numérique : vertical et horizontal

En vertical, le *continuum* part de la couche physique des systèmes de communications (la capacité à transmettre de l'information sur un médium, air, fibre, etc.) à l'IA notamment distribuée, fédérative, agentique, en passant par les architectures des réseaux (intégrant nativement l'IA), la convergence réseau-*cloud*, et l'ouverture des systèmes pour permettre une grande agilité dans la création de nouveaux services. Ce *continuum* vertical est essentiel à traiter, notamment dans un cadre où les interactions matériel (HW) et logiciel (SW) sont en pleine transformation, avec une évolution forte du paysage industriel concerné.

En horizontal, le *continuum* est traité en partant des grands *data centers* et allant jusqu'aux objets connectés, en passant par le *Multi-access Edge Computing (MEC)*, pour une distribution optimale des capacités de stockage et de calcul et des algorithmes et agents d'IA, dans des objectifs de protection de données, d'efficacité dans l'utilisation des ressources et surtout d'adaptation aux contraintes, notamment de temps réel, de très nombreux cas d'usage industriels.

Les décisions sont difficiles : la *softwarisation* des réseaux a des avantages notables pour les opérateurs, mais elle les rend plus vulnérables aux positionnements d'autres acteurs. De même, l'ouverture des réseaux, à la mode Open RAN, est d'intérêt pour les opérateurs, mais met en risque le positionnement des équipementiers, qui néanmoins n'ont pas le choix et doivent suivre. L'IA semble *a priori* un moyen clé pour la maîtrise de la croissance très rapide de la complexité, mais elle a ses propres défis et un risque de ralentissement dans les investissements. Le multi-sectoriel est une voie de forte création de valeur, très probablement la prochaine phase de la transformation numérique, mais la disposition des acteurs pour y avancer n'est pas claire et les modèles économiques pour accélérer les processus sont à définir.

Dans ce cadre, de nouvelles formes d'organisation de l'écosystème pourront éventuellement émerger, ouvrant la porte à des rôles nouveaux, facilitateurs des relations technologiques ou économiques entre les parties prenantes.

Tout ceci accroît de manière notoire les enjeux autour de la souveraineté numérique, voire de la souveraineté tout court étant donnée l'imbrication croissante du numérique avec tous les secteurs d'activité. Une réflexion de fond, globale, multipartite semble s'imposer dans l'intérêt de tous à moyen terme et cela même si la pertinence et les modalités ne semblent pas évidentes à court terme.

3. La chaîne technologique et ses enjeux de souveraineté

Pour avancer dans l'analyse, notamment en termes de souveraineté, nous introduisons dans cette section l'ensemble des éléments de la chaîne technologique, en suivant la logique du *continuum* vertical, tout en indiquant, quand cela est pertinent, le lien avec le *continuum* horizontal.

3.1. Les composants

La chaîne technologique part des composants : électroniques, optiques, quantiques, logiciels. Nous différencions donc ici les logiciels composant des infrastructures, au cœur des nouvelles architectures, comme évoqué dans la section précédente, des logiciels applicatifs.

L'articulation entre les nouveaux composants *hardware* et le logiciel, ce qui inclut entre autres les *firmwares* et les systèmes d'exploitation, est également un sujet clé. À titre d'exemple, nous pouvons citer le constructeur Nvidia, qui conçoit de manière unifiée le matériel et le logiciel, ce qui fait que leur logiciel s'impose dans un objectif de performances maximales. Ceci génère donc des dépendances.

Parmi les composants, nous incluons ceux permettant de mettre en œuvre des liaisons optiques, dont les technologies évoluent et les besoins explosent en volume du fait que les *data centers* en consomment bien plus aujourd'hui que les réseaux de télécommunications. Voir par exemple l'explosion en bourse de Corning Inc. (GLW, + 300 % en 1 an).

Ces composants concernent :

- Les communications : optique, radio, quantique
    - Ces composants sont en pleine évolution du fait de l'émergence de nouvelles technologies de communication (*beamforming*, RIS, Massive MIMO, Cell-Free, augmentation des fréquences…), des défis des réseaux non terrestres, des nouvelles technologies de fibre optique, de nouveaux besoins de communication notamment à l'intérieur des *data centers* ou à l'*edge*, des signaux faibles sur le calcul quantique distribué, etc.
- Le calcul et le stockage pour les *data centers*, le *cloud* en général, l'HPC et l'IA.

L'Annexe VI offre une liste technique, considérée prioritaire, de ces composants.

Composants et souveraineté

Il faut différencier ici

- La conception des briques technologiques, comme des solutions dynamiques de beamforming dont le faisceau radio suit l'utilisateur pour une optimisation de l'utilisation du spectre et de la puissance.
- La conception et la fonderie des composants qui les implémentent.

Recommandation n° 1

La conception des briques technologiques stratégiques est un sujet clé pour la souveraineté, il donne par ailleurs lieu à de la propriété intellectuelle. Le soutien au maintien d'une forte capacité de conception des briques technologiques est indispensable.

La sélection des priorités devrait se faire dans le cadre présenté dans la section Recommandations.

L'innovation dans le domaine de la conception des briques technologiques doit être soutenue à la normalisation, notamment dans le cadre des brevets essentiels aux normes.

Les pouvoirs publics devraient mobiliser les financements, notamment dans le cadre d'une initiative globale académique-industrielle, telle que celles financées par la stratégie d'accélération des réseaux du futur dont l'intérêt est indéniable, mais i) dans le cadre plus global des infrastructures numériques et des convergences progressives technologiques et entre filières présentées dans ce document et ii) davantage axée sur la continuité de la chaîne de l'innovation, de la recherche au marché. Cette initiative devrait être focalisée sur des innovations fortes amenant à des différenciateurs de marché significatifs, tout en facilitant le maintien de l'écosystème global nécessaire à l'émergence de ces avancées. La mobilisation cohérente des outils déjà en place (IRT, ANR, dispositif de la stratégie d'accélération, PUI, BPI et régions) est nécessaire *via* une feuille de route innovation partagée.

La commande publique devrait soutenir les industriels français et européens engagés dans ces évolutions et également favoriser l'émergence d'acteurs compétitifs, en visant le long terme pour éviter des délocalisations notamment vers les États-Unis. Des clauses spécifiques de souveraineté des solutions dans les marchés publics et notamment ceux portés par les opérateurs d'importance vitale (OIV) sont de nature à faciliter l'atteinte cet objectif.

La conception des briques technologiques se base fortement sur des avancées scientifiques. Sous l'impulsion des pouvoirs publics, les industriels et les acteurs académiques devraient renforcer leurs collaborations, développer une stratégie coordonnée d'innovation et de participation aux travaux de normalisation et accroître la production de brevets essentiels aux normes afin de renforcer la souveraineté technologique et l'influence européenne. Les PEPR ont permis d'avancer dans ce sens, mais sans financement dédié, des financements devraient viser spécifiquement ces objectifs, avec une initiative co-pilotée par des acteurs académiques et industriels.

La constitution d'un écosystème de recherche et innovation national, s'appuyant notamment sur les pôles de compétitivité à Paris et en région, et partageant une même feuille de route (*via* les stratégies d'accélération concernées), permettrait d'accélérer le processus. Un plan national « infrastructures numériques souveraines et soutenables », partagé entre les structures d'accompagnement de financement qui guiderait les axes de recherche collaborative des TRL les plus bas aux TRL les plus élevés représenterait un cadre global utile.

NB : Ce document traite de la souveraineté des briques technologiques, mais ne traite pas de la souveraineté des composants matériels qui les implémentent, ce sujet concerne le CSF électronique

3.2. Équipements et infrastructures

Les équipements intègrent les composants qui implémentent les diverses briques technologiques. Ils sont devenus plus flexibles et évolutifs, du fait de la virtualisation et la « programmabilité ».

Ce n'est pas pour autant que les infrastructures sont, elles, devenues plus flexibles, interopérables et ouvertes, bien que les nouveaux paradigmes architecturaux le permettent, à savoir :

- Virtualisation de bout en bout, basée sur des solutions ouvertes, permettant des infrastructures multi-vendeur à niveau fin des composants fonctionnels.
- Convergence réseau-*cloud*-IA et *continuum* numérique, en passant par l'*edge*.

Recommandation n° 2

Les convergences technologiques ne produiront pleinement leurs effets que si elles s'accompagnent de l'émergence de nouveaux modèles économiques adaptés. Les pouvoirs publics devraient donc promouvoir et soutenir, au même titre que les innovations technologiques, la conception, l'expérimentation et la diffusion de modèles économiques innovants permettant de structurer de nouvelles chaînes de valeur, de favoriser le partage des investissements et des risques et un partage équitable des bénéfices globaux, ainsi que d'accroître la compétitivité des acteurs européens des infrastructures numériques.

Cela permettrait une plus grande capacité de création de valeur pour les entreprises de divers secteurs d'activité et un meilleur positionnement des citoyens.

Quelques pistes d'action :

- Lancer des appels à projets centrés autant sur l'innovation économique et organisationnelle que sur l'innovation technologique.

- Adapter, lorsque nécessaire, les cadres réglementaires afin de faciliter les coopérations entre filières.

- Soutenir des démonstrateurs intégrant simultanément innovation technologique et innovation économique.

- Organiser des groupes de travail dédiés aux nouveaux modèles économiques, en s'appuyant sur les pôles, les IRT, etc.

- Orienter les appels d'offres publics pour y inclure des clauses de souveraineté et de résilience.

Tout cela devrait mener à ce que les industriels visualisent de manière concrète le potentiel de mise en œuvre de modèles de co-investissement et de partage des risques et des revenus entre acteurs des différentes filières.

Un équipement réseau, qu'il s'agisse d'une station de base 5G ou d'un routeur de cœur de réseau, intègre des composants matériels et logiciels provenant de dizaines, voire de centaines, de fournisseurs différents, souvent répartis sur plusieurs continents. La souveraineté technologique, dans ce contexte, ne peut être réduite à la seule origine géographique de l'équipement final. Elle doit englober la capacité à contrôler la conception, la fabrication, la sécurité et la maintenance des technologies critiques, ainsi que la protection des données et des communications.

La logique actuelle porte sur des partenariats globaux avec des « partenaires de confiance » comme l'illustre la dernière mouture du *Cyber Security Act* européen. Il est en effet illusoire, dans le contexte actuel, d'imaginer une souveraineté technologique totalement affranchie de toutes dépendances externes, comme un système autarcique derrière les murailles d'un château fort. La souveraineté consistera donc, entre autres, à évaluer, choisir et réduire ses dépendances, en favorisant les interdépendances, nous pouvons être dépendants sur certaines briques technologiques, mais nos partenaires peuvent aussi dépendre de nous sur d'autres briques.

Un « partenaire de confiance » est une entité (entreprise, organisation) avec laquelle un équipementier établit une relation stratégique basée sur des critères rigoureux de sécurité, de transparence, de conformité éthique et réglementaire, et d'alignement stratégique à long terme, ce qui inclut la maîtrise des actifs critiques Cette confiance dépasse la simple conformité contractuelle pour s'ancrer dans une évaluation continue et une collaboration proactive.

Cette dynamique avec des acteurs de confiance peut être une première étape dans la maîtrise de solutions plus globales et alternatives à l'instar des acteurs nord-américains et asiatiques. L'objectif serait d'avoir les moyens d'affirmer sa souveraineté et sa résilience au même titre que les *coopétiteurs*.

Recommandation n° 3

Dans les objectifs réalisables de souveraineté, il est nécessaire d'évaluer les dépendances existantes et de définir des objectifs exigeants mais réalistes, d'évaluer les risques en lien avec les partenaires de confiance et prévoir les moyens pour les réduire, à court, moyen et long terme.

Il est ainsi nécessaire de mettre en œuvre une stratégie de souveraineté fondée sur une gestion dynamique des dépendances critiques. Les pouvoirs publics et les industriels devraient identifier les dépendances technologiques, industrielles et géopolitiques les plus sensibles, définir des objectifs de réduction réalistes et priorisés, et élaborer des feuilles de route à court, moyen et long terme. Cette stratégie devrait s'appuyer sur le développement d'alternatives françaises et européennes dans les domaines les plus critiques (grâce à des avancées technologiques et un travail en écosystème), sur le renforcement des compétences et de la recherche, ainsi que sur un dialogue permanent entre les pouvoirs publics et les acteurs industriels afin d'anticiper les évolutions géopolitiques susceptibles d'affecter les chaînes d'approvisionnement et d'éviter notamment que des partenaires de confiance d'aujourd'hui soient disqualifiés demain pour des critères géopolitiques qui dépassent le cadre décisionnel des entreprises.

Il faudra en particulier :

- Mettre en place une cartographie régulièrement actualisée des dépendances technologiques et industrielles, avec une approche transversale à toute la chaîne technologique et de valeur.
- Définir, dans un cadre multi-filière, des niveaux cibles de réduction des dépendances en fonction des risques. Le cadre holistique multi-filière est le seul qui permettrait des positionnements efficaces dans ce contexte.
- - S'appuyer sur l'Indice de Résilience Numérique (IRN) pour aider les organisations à réfléchir à leurs dépendances en termes de solutions de communication internes et externes.

Pour les PME et les acteurs académiques, il est essentiel d'adopter une méthodologie rigoureuse afin d'identifier des partenaires de confiance et de déterminer le niveau d'exigence associé à chaque type de besoin et de risque. Cette démarche doit s'appuyer sur plusieurs critères clés : la souveraineté des données, la conformité aux réglementations européennes (RGPD, NIS2), la capacité à garantir une sécurité intégrée (notamment contre les cyberattaques et la fraude) comme la certification ANSSI SecNumCloud, ainsi que la maîtrise des aspects techniques liés à la résilience et à la performance des réseaux.

Il est recommandé de privilégier des partenaires qui disposent d'un écosystème ouvert, interopérable et européen, capables d'assurer la localisation des données, la gestion sécurisée des clés, et la traçabilité des opérations.

Enfin, cette démarche doit intégrer une évaluation continue des risques liés à la chaîne d'approvisionnement, notamment en matière de dépendance géopolitique ou énergétique, afin de renforcer la résilience et la sécurité globale des déploiements. En adoptant cette approche structurée, PME et académiques pourront établir des partenariats solides, sécurisés et alignés avec les enjeux de souveraineté numérique européenne.

Certaines initiatives tentent d'identifier des « partenaires de confiance » comme « l'indice de résilience numérique » (IRN, voir aDRI - Indice de Résilience Numérique et adri / aDRI-IRN · GitLab - lien vers grille d'autoévaluation), avec une méthodologie testée notamment par la Caisse des dépôts et qui se base sur le principe de DORA, avec une définition des domaines critiques et l'évitement des interdépendances. La méthodologie est en *open source* sur GitHub, elle permet d'afficher de façon simple un score par rapport à l'indice de résilience de l'entreprise et permet de faire des choix sur la criticité de certains éléments. Une deuxième initiative a été présentée par le Haut-commissariat au plan qui avait demandé les critères de souveraineté et d'autonomie (une définition de l'autonomie stratégique est notamment proposée par l'ANSSI). Travaux d'interopérabilité en Europe, notamment sur les communs numériques, qui encourageraient les pays les plus leaders comme la France et l'Allemagne à développer des solutions en Europe pour maintenir l'interopérabilité.

Rappelons dans ce cadre que le 26 janvier 2026 s'est tenue la première rencontre dédiée à la souveraineté numérique sous l'égide de la ministre déléguée chargée de l'Intelligence Artificielle et du Numérique, Anne Le Hénanff. Cette initiative vient compléter le sommet Franco-Allemand du 18 novembre dernier où avaient été identifiées des thématiques prioritaires : l'intelligence artificielle, le quantique, la cybersécurité et le *cloud*, avec une attention particulière aux solutions certifiées SecNumCloud et sur la nécessaire création des

conditions favorables pour réduire nos dépendances qui nécessite de développer les acteurs français et européens et favoriser une préférence européenne sur les marchés. L'ambition affichée est qu'en 2026, la France et l'Union européenne devront choisir leurs solutions numériques en cohérence avec leurs valeurs, en passant à l'action (voir l'annexe V pour des informations complémentaires, notamment sur l'IRN).

Par ailleurs, la DGA dispose d'outils pérennes utilisés par les militaires sur des domaines super critiques, la phase d'anticipation et la collecte d'information qui permettent de mesurer l'indice de capacité de souveraineté.

Recommandation n° 4

Définir un cadre méthodologique pour aider les entreprises à répondre à des critères de souveraineté dans leurs décisions de conception, d'investissement ou de choix de partenaires de confiance.

Référencer et mettre à disposition les outils méthodologiques existants ou à développer

Développer des méthodes d'évaluation multicritères intégrant les dimensions technologiques, économiques, juridiques et géopolitiques.

Recommandation n° 5

Dans ce document, il a été mis en évidence que les orchestrateurs deviennent des éléments centraux des architectures, en permettant l'adaptation dynamique des infrastructures pour répondre aux besoins des usagers. Faire de l'orchestrateur un levier de pilotage dynamique de la souveraineté des infrastructures numériques. Les orchestrateurs de nouvelle génération devraient intégrer nativement des politiques de souveraineté leur permettant de sélectionner, d'allouer et d'adapter les composants et les ressources (calcul, réseau, stockage, services, données, agents) en fonction du niveau de souveraineté requis par chaque usage. Cette approche permettrait d'assurer le niveau de souveraineté attendu tout en optimisant les performances et les coûts, en évitant le recours systématique à des solutions imposant un niveau maximal de souveraineté lorsque celui-ci n'est pas nécessaire.

Compte tenu du caractère structurant et transversal des orchestrateurs, notamment multisectoriels, il est recommandé de lancer un programme national ou européen de recherche et d'innovation associant technologies, économie et sciences sociales afin de concevoir les architectures d'orchestration, les mécanismes de décision et les modèles économiques permettant la mise en œuvre opérationnelle de cette souveraineté adaptative. Il est également suggéré de soutenir une conception ouverte des orchestrateurs et le développement de composants logiciels pouvant être intégrés dans différents orchestrateurs.

Il ne s'agit pas de se focaliser sur un composant, mais de concevoir les solutions qui permettront de mettre en œuvre et d'articuler les divers composants et les nouveaux modèles économiques, notamment dans un cadre multisectoriel.

Dans le cadre de l'utilisation de composants *open source* dans ces solutions, il faudra s'assurer que les acteurs européens et français sont en position d'être au cœur du processus de décision sur les contenus de ces composants.

Notons que l'Europe dispose d'équipementiers historiques comme Nokia et Ericsson, mais également d'acteurs entrés bien plus récemment dans le marché, positionnées à partir de l'évolution vers la *softwarisation* des réseaux. Nous pouvons citer, sans être exhaustifs :

Amarisoft est une entreprise française, positionnée au niveau mondial sur les piles logicielles 4G/5G (et désormais 6G en prénorme), dont les solutions sont déployées dans la recherche académique, les bancs de test des opérateurs, les réseaux privés industriels et chez de nombreux opérateurs.

Rapid.Space est un équipementier français de télécommunications de bout en bout, opérateur de télécommunications alternatif, qui suit une approche « *hyperopen* » (*open source* incluant le matériel *via* Open Clod Project - OCP). Rapid.Space déploie aujourd'hui des infrastructures virtualisées en Asie, Amérique et Afrique et est référencé chez Airbus, EDF, Thales, Rheinmetall, SANEF, SNCF, Stellantis, Toyota, Nissan, Mitsubishi, Viettel, TDF, MBDA et plus de 1 600 autres entreprises dans le monde.

Nexedi est un éditeur français, impliqué dès le départ de ces innovations dans le concept d'*edge* computing et des réseaux 3C.

SlapOS propose un système d'exploitation distribué et représente ainsi l'une des rares alternatives européennes complètes à Kubernetes/OpenStack pour l'orchestration *edge*.

OpenAirInterface (porté par Eurecom et l'OAI Software Alliance, basée en France) représente probablement à ce jour la seule alternative européenne *open source* aux piles 5G propriétaires ayant réussi une portée mondiale.

srsRAN (Software Radio Systems) est une entreprise irlandaise, : acteur européen majeur du RAN *open source*.

SimpleRAN : alliance européenne d'origine française (Rapid.Space, Amarisoft, Nexedi, etc.) dans le domaine des infrastructures virtualisées.

3.3. Infrastructures et *continuum* numérique vertical et horizontal

Pour commencer, nous rappelons pour faciliter la lecture les deux types, complémentaires, de *continuum* numérique : vertical et horizontal.

En vertical, le *continuum* part de la couche physique des systèmes de communications (la capacité à transmettre de l'information sur un médium, air, fibre, etc.) à l'IA notamment distribuée, fédérative, agentique, en passant par les architectures des réseaux (intégrant nativement l'IA), la convergence réseau-*cloud*, et l'ouverture des systèmes pour permettre une grande agilité dans la création de nouveaux services. Ce *continuum* vertical est essentiel à traiter, notamment dans un cadre où les interactions HW et SW sont en pleine transformation, avec une évolution forte du paysage industriel concerné.

En horizontal, le *continuum* est traité en partant des grands *data centers* et allant jusqu'aux objets connectés, en passant par le *Multi-access Edge Computing (MEC)*, pour une distribution

optimale des capacités de stockage et de calcul et des algorithmes et agents d'IA, dans des objectifs de protection de données, d'efficacité dans l'utilisation des ressources et surtout d'adaptation aux contraintes, notamment de temps réel, de très nombreux cas d'usage industriels.

Recommandation n° 6

Les deux composantes du *continuum* numérique, horizontale et verticale, sont complémentaires et doivent être traitées ensemble dans le cadre de la Recommandation #2. Cela requiert la mise en place du cadre général, multi-sectoriel, figurant dans la section Recommandations.

Mettre en place une gouvernance du *continuum* numérique fondée sur les convergences technologiques, économiques et sectorielles. Cette gouvernance devrait dépasser les approches en silos afin d'assurer la cohérence des politiques de recherche, d'innovation, de normalisation, de régulation et d'industrialisation sur l'ensemble de la chaîne de valeur des infrastructures numériques. Elle devrait s'appuyer sur une coordination renforcée des acteurs y compris des secteurs utilisateurs du numérique.

Des synergies fortes entre les deux agences de programme concernées sont donc absolument nécessaires, avec éventuellement la mise en place d'une cellule de coordination spécifique, garantissant la prise en compte des enjeux technologiques, économiques et sociétaux en lien avec la mise en place de ce *continuum*[5].

3.3.1. Le *Telco Cloud*

Dans ce cadre général, le *Telco Cloud* représente un élément particulier du *continuum*. Il peut être défini de diverses manières et, schématiquement, dans 2 visions complémentaires :

- L'utilisation du paradigme et des technologies du *cloud* pour l'implémentation d'infrastructures réseau. Cette approche est bien avancée avec un pourcentage non négligeable des infrastructures réseaux basées sur ces architectures.
- Le déploiement d'infrastructures convergentes, offrant de manière intégrée des services réseau et des services *cloud*, avec une opération et optimisation unifiées. Cette approche est encore balbutiante au regard du potentiel de création de valeur qu'elle représente.

Ces évolutions offrent des opportunités pour les opérateurs mais peuvent également représenter des risques. Ici, le sujet de la souveraineté doit être traité sur plusieurs angles :

- La garantie de disposer des moyens de communication nécessaires.
- Le fait que des acteurs nationaux/européens puissent garder, voire développer, leur positionnement de marché.

[5] Les recommandations 2 et 6 pourraient être fusionnées, mais leur interprétation nous semble plus simple en les gardant séparées et positionnées dans le cadre de leurs sections respectives, l'une sur les briques technologiques et l'autre sur le *continuum* du numérique.

- Le fait que ces infrastructures soient sûres, ce qui dépend des équipements et composants logiciels déployés.

Le points 1 est fortement lié au point 2, en effet, une perte de positionnement ne permettrait pas de garantir que les investissements futurs nécessaires seront réalisés.

L'ouverture souhaitée, notamment dans le cadre du *Telco Cloud*, engendre des risques majeurs au travers de la facilité et agilité pour déployer de nouveaux composants logiciels.

À titre d'exemple, lorsqu'une opportunité de renouvellement des fonctions réseau se présente, certains opérateurs comme Orange peuvent être amenés à évoluer vers des infrastructures *cloud* conformes aux standards ouverts portés par Sylva, afin de renforcer l'interopérabilité des solutions.

Le côté « *open* » est complexe et ne génère pas nécessaire des externalités positives, citons l'Open RAN qui ne réduit pas forcément ses coûts en partageant certains types d'infrastructures, avec des réserves émises quant à la pertinence de l'ouverture.

Pour un opérateur, la logique pourrait être de promouvoir l'*open source* et l'écosystème attenant. Néanmoins, il faut éviter le risque d'une fragmentation du marché avec une plaque chinoise, américaine et européenne, ce qui représenterait un retour 20 ans en arrière. La stratégie actuelle est de promouvoir les standards et l'*open source*, et de jouer sur la complémentarité, la bonne entente et l'équilibre, notamment entre les acteurs européens.

Il y a beaucoup d'investissements en normalisation et également dans le cadre de la Linux Foundation. Des efforts sont mobilisés pour viser **le cercle européen en premier.**

Recommandation n° 7

Dans le contexte des infrastructures numériques européennes, l'ouverture des réseaux *via* des solutions *open source* constitue un levier stratégique pour garantir l'interopérabilité, accélérer les déploiements et stimuler l'innovation collaborative. En adoptant des standards ouverts, cette approche facilite l'intégration de solutions variées, évite la dépendance à des fournisseurs uniques et permet aux acteurs publics, privés et académiques de développer des architectures compatibles et résilientes.

Toutefois, cette ouverture doit être encadrée par une gouvernance forte pour éviter la fragmentation, gérer la compatibilité entre différentes solutions et assurer la sécurité et la pérennité des systèmes.

Si l'*open source* offre de nombreux avantages en termes de contrôle, de flexibilité et de développement d'un écosystème européen, il comporte également des risques importants, notamment en matière de propriété intellectuelle, où la diffusion libre peut compliquer la protection des innovations et des brevets.

De plus, la gestion des vulnérabilités, la normalisation et la coordination restent des défis majeurs, nécessitant une vigilance constante pour éviter que l'ouverture ne fragilise la sécurité ou n'entraîne une fragmentation incompatible avec la souveraineté européenne.

Ainsi, une stratégie claire d'ouverture, associée à une gouvernance européenne rigoureuse, est essentielle pour bâtir des infrastructures numériques souveraines, résilientes et

innovantes, tout en maîtrisant les enjeux de sécurité, de propriété intellectuelle et de standardisation.

Il est fortement souhaitable d'analyser plus en détail le besoin d'orienter des financements vers des innovations européennes en avance, ce qui est détaillé dans ce document, d'identifier les briques technologiques pour lesquelles l'*open source* constitue un avantage stratégique et d'élaborer une feuille de route coordonnée entre les initiatives nationales et européennes.

Un exemple concret de cette démarche est Sylva, un projet européen *open source* visant à développer une plateforme de gestion d'infrastructures *cloud* souveraines qui a permis de réduire la dépendance aux fournisseurs étrangers, tout en favorisant l'innovation locale et la coopération européenne. Il faut néanmoins rappeler que Sylva est techniquement une distribution intégrée de composants Kubernetes, eux-mêmes développés sous gouvernance CNCF (Linux Foundation). Le cœur technologique — Kubernetes, Cilium, Istio, etc. — n'est pas européen (voir la section *Logiciel libre et gouvernance associée*).

Le projet Sylva fait l'objet de financements publics européens (notamment dans le cadre du PIIEC-CIS) et aide à combler un retard fonctionnel sur des solutions américaines (Google Kubernetes Engine, Red Hat OpenShift).

Il serait souhaitable d'analyser la pertinence d'orienter des financements vers des innovations européennes en avance. Des acteurs européens existent, citons par exemple Nexedi avec sa solution SlapoS.

3.3.2. Convergence des Réseaux Terrestres (TN) et non Terrestres (NTN)

Nous présentons ici quelques concepts structurels concernant la dynamique autour des NTN et nous revenons plus en détail sur le sujet dans la section suivante.

La convergence entre réseaux terrestres et non terrestres représente une opportunité stratégique majeure pour la France et l'Europe, notamment dans le contexte de l'émergence des constellations satellitaires. La complémentarité entre TN et NTN permettrait de proposer un meilleur accès à une connectivité pour l'ensemble de la population ainsi qu'à des contextes spécifiques (mer/montagne). Sur le plan technologique, la mise en œuvre de solutions D2D (*Direct to Device*) *via* la 5G-NTN, intégrant des chipsets compatibles smartphones et des spectres dédiés MSS (Mobile Satellite System), pourrait ouvrir la voie à des services innovants, notamment pour l'Internet des objets, la mobilité ou la connectivité en mobilité (transports terrestres dont le train, maritimes et aéronautiques). Cependant, cette convergence nécessite une régulation adaptée, notamment en Europe, pour garantir l'accès équitable aux spectres MSS, favoriser la standardisation et éviter une dépendance excessive à des acteurs mondiaux non-européens comme Starlink. Par ailleurs, la convergence TN-NTN apparaît aussi comme un levier essentiel pour renforcer la résilience de la connectivité et l'accès au numérique face aux risques et crises climatiques, énergétiques et géopolitiques. Pour accompagner la montée en puissance des usages data et IA et répondre aux exigences croissantes de disponibilité, de sécurité et de souveraineté ainsi que de contrôle de la latence, la France et l'Europe doivent consolider une stratégie cohérente de convergence TN–NTN. L'enjeu est de disposer

d'infrastructures résilientes et compétitives face aux constellations extra européennes et à l'intensification des besoins de connectivité européennes.

Recommandation n° 8

Pour garantir la souveraineté spatiale de la France et de l'Europe sur le volet critique des infrastructures numériques, plusieurs axes doivent être adressés au travers de la formulation d'un programme tendant à :

- Assurer une autonomie dans l'ensemble de la chaîne de valeur, telle que décrite dans ce document
- Valoriser la complémentarité TN-NTN et l'opportunité de la 5G et de la 6G
- Prendre en compte le secteur aval dans la conception des politiques spatiales, en différenciant les divers besoins : large bande, connectivité d'objets, services critiques, etc.
- Appréhender la dualité civil-militaire de l'espace extra-atmosphérique
- Faire du cadre réglementaire de la LOS (Loi sur les Opértions Spatiales) française un avantage compétitif pour l'industrie européenne.

Une analyse des nouveaux modèles économiques est indispensable ; en effet, le risque est que les acteurs ayant pris des positions fortes dans le cadre des NTN absorbent l'intégralité du marché des télécommunications, en s'appuyant sur les réseaux nationaux pour offrir à leurs clients des services globaux.

Remarque : les éléments de cette recommandation sont détaillés dans la section « Les réseaux non terrestres (NTN) ».

3.4. L'IA pour les Infrastructures numériques et les infrastructures numériques pour l'IA.

La complexité croissante des réseaux, avec l'introduction d'une grande diversité de nouvelles technologies et paradigmes de communication, avec la flexibilité introduite par la *softwarisation*, la virtualisation et le placement dynamique des fonctionnalités, avec l'ouverture des réseaux sur diverses formes, avec la convergence progressive réseau-*cloud* et avec l'avènement de services multisectoriels, impose l'utilisation de l'IA à divers niveaux. Côté technologique, nous pouvons citer à titre d'exemple certaines évolutions du RAN : nouveaux systèmes antennaires et RIS, réseaux sans cellules, la convergence communications-*sensing*...). L'utilisation de l'IA concerne toute la chaîne : la conception, la planification, le déploiement et l'exploitation des réseaux. Il faut également prendre en compte l'utilisation de jumeaux numériques alimentés par de l'IA.

Cette importance croissante de l'utilisation de l'IA soulève des questions sur le positionnement des acteurs dans cet environnement en mutation, sur la régulation, sur les certifications qui seront requises pour que les mécanismes d'IA puissent être intégrés dans les infrastructures de réseaux. Nous revenons plus loin dans ce document sur ces questions.

Parallèlement, l'IA évolue. D'une part, l'usage de l'IA orienté texte (avec des requêtes et des réponses sous format texte) évolue vers des contenus multimédias : traduction instantanée,

utilisation des lunettes connectées remontant un flux vidéo, de caméras de contrôle de process industriels avec une analyse IA dans le *cloud*... Beaucoup de ces cas d'usage modifient les ratios de trafic montant et descendant (uplink / downlink) et augmentent aussi de manière plus globale le trafic (tant en uplink qu'en downlink).

Il est à noter que, du fait de l'utilisation massive de l'IA, le trafic machine-machine a dépassé tous les autres trafics en 2026.

L'IA devient de plus en plus distribuée, notamment avec l'essor de l'IA fédérative et de l'IA agentique, ainsi que pour des raisons de protection des données. La question de l'efficacité énergétique doit également être considérée, l'intérêt de ce point de vue de l'*edge* dépendant des cas d'usage. Cette décentralisation de l'ensemble des infrastructures, sortant des grands *data centers*, crée de nouvelles opportunités, notamment grâce au MEC, et génère aussi des risques significatifs. Le débat portera sur les opportunités pour les opérateurs en tant qu'acteurs de confiance, tout en abordant des thèmes transversaux comme la souveraineté, la sécurité, la protection des données, le numérique responsable et les compétences nécessaires à chaque étape de la chaîne.

Comme déjà évoqué, l'IA agentique multi-agents multi-acteurs soulève la question, essentielle au succès de cette dernière, de la mise en place du plan de gouvernance de l'IA (agents, orchestrateurs, etc.) et des données, pour lequel les infrastructures numériques ont un rôle central à jouer. Le plan de gouvernance permet de suivre le comportement des agents, tout en « respectant » leur autonomie, mais en garantissant qu'ils ne débordent pas de leur mandat, que les règles d'accès entre eux soient respectées, que les échanges soient bien tracés, etc. Ce plan de gouvernance, qui doit respecter la réglementation (européenne notamment : *Digital Services Act*, *AI Act*, RGPD…) et ses évolutions, doit encore être conçu.

4. Positionnement des acteurs actuels

Nous allons présenter une catégorisation des acteurs afin de présenter leur positionnement actuel. Mais avant cela, nous introduisons une définition du *cloud* afin d'éviter de mauvaises interprétations dans le reste du document.

Trop souvent les concepts de *cloud* et de *data centers* sont confondus. Les *data centers* ne sont qu'un moyen d'implémentation du *cloud*, certes historiquement presque unique, mais ceci est en forte évolution. Dans l'objectif de traiter le sujet dans le cadre le plus large, en évitant de réduire le spectre des opportunités, nous utiliserons par la suite la définition suivante de *cloud* : L'architecture d'un système numérique est dite « *cloud* » quand il y a découplage entre le service/l'application et le moyen d'y accéder (terminal, réseau, localisation des ressources IT[6], etc.). Ainsi, une architecture *cloud* peut être basée sur des ressources d'IT localisées dans des grands *data centers*, dans des solutions à l'*edge*, sur des constellations de satellites, etc. Du fait de ce découplage, les fonctionnalités sont fournies en mode service (*as a service*). L'IaaS (*Infrastructure as a Service*) consiste à offrir en mode *cloud* des capacités de calcul et de stockage. Le PaaS ajoute dans l'offre un certain nombre de briques génériques pouvant être utilisées pour la création de services ou applications. Finalement, le SaaS (*Software as a Service*) offre en mode *cloud* des applications. Dans ces 3 cas historiques du *cloud* et dans les évolutions qui ont suivi, le commun dénominateur est le découplage mentionné dans la définition proposée. À titre d'exemple, faire une différence entre *cloud* et *edge* n'a pas de sens, l'*edge* (notamment le MEC, *Mobile Edge Computing* / *Multi-access Edge Computing*) est conçu pour pouvoir contribuer avec ses ressources à l'infrastructure *cloud*.

Sur cette base, revenons à l'objectif de cette section, la catégorisation des acteurs.

Nous couvrons dans ce document les acteurs suivants :

- Opérateurs de réseaux de télécommunications terrestres et non terrestres (TN et NTN), publics et privés.
- Opérateurs de systèmes *cloud* (IaaS, PaaS, SaaS).
- Opérateurs de *data centers*, de systèmes MEC, de centres de colocalisation.
- Équipementiers : (Réseau, Serveurs, stockage, virtualisation, orchestration, systèmes de planification et déploiement…) et le rôle de l'*open source*.
- Fournisseurs de solutions de cybersécurité pour les infrastructures numériques et de solutions pour la cybersécurité applicative.
- Fournisseurs de solutions de planification, d'exploitation, de gestion et de maintenance : automatisation, apport des jumeaux numériques (*digital twins*), etc.
- Fournisseurs de solutions d'IA pour les infrastructures numériques.
- Fournisseurs de solutions d'IA s'appuyant sur les infrastructures numériques.

[6] IT : Information Technologies

Nous présentons maintenant le positionnement des acteurs, sachant que les frontières entre les différentes catégories s'estompent progressivement dans le cadre de la convergence réseau-*cloud*-IA ; les catégories ne sont donc pas disjointes.

4.1. Opérateurs de réseaux terrestres et non terrestres (TN et NTN), publics et privés

À l'avenir, presque tous les appareils seront connectés partout et à tout moment. Cela confère au secteur des télécommunications un avantage unique pour conquérir les divers segments de marché que ces appareils et leurs applications représentent. Un prérequis est cependant que les acteurs télécoms démontrent leur capacité à différencier leurs services grâce au(x) réseau(x) et aux fonctionnalités les mieux adaptées aux besoins des applications. Pour relever ces défis, des transformations structurelles sont nécessaires, sur lesquelles nous revenons dans la section « Catégorisation des opportunités ».

Les fournisseurs de réseaux de télécommunications, terrestres et non terrestres (TN et NTN), sont directement concernés par l'essor des usages fondés sur les données et l'intelligence artificielle, qui imposent des exigences accrues de disponibilité, de souveraineté et de conformité (RGPD, NIS2, *AI Act*) à l'échelle nationale et transfrontalière et dans certains cas de latence[7]. Pour y répondre, ils convergent peu à peu vers un *continuum* de connectivité et de calcul combinant des capacités *edge* distribuées (chez le client et dans le réseau) et des ressources *cloud* centrales, orchestrées de bout en bout, y compris lorsque des segments satellitaires NTN sont mobilisés. Ce modèle vise à proposer des garanties harmonisées et des services cohérents en Europe pour des cas d'usage récurrents tels que la fédération intra-groupe et inter-opérateurs des nœuds *edge* (continuité opérationnelle, optimisation de ressources), la mise à disposition en gros (*wholesale*) de capacité de calcul, les services à très faible latence pour la mobilité intelligente et les véhicules connectés, les besoins multi-pays de capacité de calcul et de stockage avec résidence des données locale, la résilience et la sécurité *via* des mécanismes d'entraide entre opérateurs en cas d'incident majeur, et l'optimisation énergétique par traitement local et pilotage temps réel. Les principaux facilitateurs techniques sont la *softwarisation* des fonctions réseau, le *slicing* 5G (possibilité de créer plusieurs réseaux virtuels avec des caractéristiques différentes sur un même réseau physique), l'exposition d'APIs (*Application Programming Interface*) réseau interopérables (par exemple *via* CAMARA/Open Gateway (projets Linux Foundation-GSMA) et une orchestration multi-domaine/multi-opérateur assurant le placement dynamique des charges entre *customer edge*, *network edge* et *cloud* central, avec observabilité et contrôle de la QoS. La connectivité sous-jacente (accès fixe et mobile, transport IP/MPLS, interconnexions inter-*data centers*, intégration TN/NTN) doit garantir des chemins de bout en bout performants,

[7] En ce qui concerne les contraintes de latence, outre des applications de contrôle en temps réel d'usines fortement automatisées, les latences visées pour les nouvelles générations de réseaux peuvent être nécessaires des applications haptiques ainsi que pour certaines applications XR ou IA tems réel. Néanmoins, le nombre d'applications requérant des temps de latence radio extrêmement faibles comme ceux prévus par la 6G sont réduits à court terme ; le potentiel de création de valeur de la 6G se trouve surtout autour de nouvelles approches architecturelles en lien avec le *continuum* numérique.

résilients et sécurisés. Des démarches européennes structurent cette trajectoire, tandis que la mutualisation des ressources et l'alignement des garanties contribuent à limiter la fragmentation du marché, à rationaliser les investissements et à réduire l'empreinte carbone en évitant des infrastructures sous-utilisées.

Néanmoins, là où le nombre d'opérateurs télécom en Chine ou aux Etats Unis se comptent avec les doigts d'une main, en Europe ils dépassent largement la centaine. Cette dispersion limite leur force individuellement dans les nouveaux marchés visés.

Recommandation n° 9

Créer une cellule multidisciplinaire en charge d'analyser les stratégies pour renforcer les opérateurs de télécommunications européens dans leur cœur de métier et dans les ouvertures vers les nouveaux marchés mentionnés dans ce document.

Cela devra passer par une combinaison d'approches : un certain niveau de consolidation, des interactions technologiques plus fortes permettant des fédérations se comportant comme un seul acteur qui passe à l'échelle, notamment dans le cadre de partenariats au niveau européen avec des acteurs d'autres filières : *cloud*, cyber, IA pour des offres consolidées grâce au bon niveau d'interopérabilité technologique et une orchestration dynamique des ressources et des fonctionnalités multi-acteurs, multi-secteurs.

La même cellule devrait analyser le potentiel économique d'une transformation progressive de ces infrastructures convergentes multi-acteurs vers une logique ouverte, de type *Platform as a Service* (PaaS), tel que présenté dans ce document, permettant une bien plus forte création de valeur, à travers l'intégration dynamique de nouveaux composants, proposés par des acteurs tiers, tels que des industriels de divers secteurs d'activité, pour la composition dynamique de nouveaux services. Ces composants pouvant par ailleurs être disponibles sur une place de marché portée par ces infrastructures convergentes.

Cela pourrait enclencher une évolution des infrastructures numériques européennes d'une logique d'infrastructures cloisonnées vers des plateformes ouvertes, interopérables et orchestrées, capables de fédérer des écosystèmes industriels, de soutenir de nouveaux modèles économiques et de piloter dynamiquement des exigences de performance, de résilience et de souveraineté.

Recommandation n° 10

Tel qu'évoqué dans ce document, l'utilisation de l'IA pour la conception, le développement, la planification, l'opération sécurisée et résiliente des infrastructures numériques doit continuer d'être soutenue afin de garantir que la France et l'Europe disposeront des infrastructures nécessaires à permettre le développement socio-économique, du moins à la hauteur de celui prévu dans d'autres blocs. Les outils pour ce soutien existent déjà, il faut pérenniser leur financement.

Au-delà de cela, la France dispose d'atouts permettant le déploiement d'infrastructures disposants de différenciateurs majeurs au niveau global. À titre d'exemple, tel que décrit plus haut, les infrastructures numériques européennes pourraient intégrer un plan de

gouvernance données et IA, ce qui représenterait un différenciateur majeur du fait que cela permettrait un déploiement beaucoup plus pertinent et rapide de l'IA agentique distribuée, y compris multi-acteurs, y compris pour la mise en place de services multisectoriels, tout cela représentant un accélérateur majeur du développement économique.

La gouvernance des données et de l'IA, dont le besoin est aujourd'hui de plus en plus admis comme élément clé pour réaliser tout le potentiel de l'IA agentique, deviendra ainsi une fonction d'infrastructure numérique, transversale donc, au même titre que le calcul, le stockage ou la connectivité. Le lien avec notre recommandation #5 sur les orchestrateurs pour la souveraineté est direct.

Cette piste doit être explorée rapidement, par exemple en créant une cellule multi-filière (réseaux, *cloud*, IA, verticaux) et multidisciplinaire (technologie, économie) et en cas de conclusions positives (ce qui semble évident), la formulation d'une feuille de route pour permettre d'avancer dans un domaine où un leadership global est encore possible.

4.1.1. Les réseaux non terrestres (NTN)

Un réseau NTN est un système de télécommunication utilisant des infrastructures non terrestres, telles que :

- Satellites (caractérisées par différentes orbites : LEO, MEO, GEO),
- Ballons stratosphériques,
- Stations à haute altitude (HAPS)
- Drones ou plateformes aériennes.

Aujourd'hui, les seuls réseaux NTN commerciaux existants sont les réseaux NTN utilisant des satellites de télécommunication et notamment des constellations de satellites en orbite basse ou moyenne. Ils peuvent fournir l'ensemble des services de télécommunications, et notamment des communications critiques (sécurité, défense, urgence).

Tout comme dans le cas des réseaux terrestres, les réseaux non terrestres évoluent vers une convergence réseau-*cloud*-IA. Ainsi, les Chinois ont été les premiers à embarquer une capacité de calcul et de l'IA dans leurs constellations de satellites.

Les constellations de satellites jouent également un rôle clé dans l'observation de la terre. De ce fait, la capacité à prendre de décisions directement au niveau des satellites pour donner suite aux observations et mesures réalisées par ces derniers peut apporter des avantages décisifs, notamment dans le cadre militaire.

Ici encore les enjeux de marché et de souveraineté sont évidents.

Un autre point clé dans ce domaine est la convergence technologique entre les TN et les NTN. Il ne s'agit pas uniquement de les faire interopérer, par exemple dans le cas de l'utilisation d'un réseau NTN comme back-up, mais de concevoir et déployer des réseaux qui utilisent les deux approches. Du point de vue du marché, cela pourra se baser sur des acteurs qui se fédèrent ou sur des approches plus disruptives.

Par ailleurs, la complémentarité des réseaux NTN est déjà commerciale puisque les grands opérateurs terrestres (Orange, DT, Telefonica, etc.) sont également redistributeurs des ressources fournies par les opérateurs satellitaires. Ce modèle de complémentarité des acteurs TN et NTN est remis en cause par la volonté d'intégration verticale de Starlink, qui se positionne directement en concurrent des opérateurs terrestres.

Les systèmes convergents NTN-TN s'appuieront sur les mêmes bandes de fréquence. L'avenir du spectre TN et NTN est désormais de plus en plus interconnecté (e.g. Usage de spectre NTN pour des usages TN et vice-versa sous étude dans le cadre WRC-27[8]). Au-delà des bandes de fréquence, des aspects architecturaux de cette convergence seront traités dans le cadre des systèmes 5G-NTN et 6G-NTN. L'utilisation prochaine de 5G-NTN permettra une intégration plus facile et complète (par ex : un seul cœur réseau 5G, un seul terminal avec plusieurs antennes, *handover* transparent pour l'utilisateur). L'utilisation du standard 3GPP est aussi un garant d'un écosystème industriel ouvert, à l'opposé d'un système propriétaire qui ne permet pas l'entrée de nouveaux arrivants.

Les usages de connectivité satellite se multiplient faisant passer d'un marché d'initiés à un marché grand public, qu'il s'agisse de « B2B » (entreprise) ou de « B2C » (consumer). Cet aspect est renforcé d'abord par la réduction considérable de prix du service sous l'impulsion de Starlink et aussi, par l'adoption progressive du standard 3GPP.

La mise en service de constellations à orbite basse est un changement radical de l'écosystème, passant d'un marché historiquement tourné sur de la diffusion *broadband* à partir de satellite GEO, à de la connectivité à faible latence, globale, potentiellement pour des terminaux utilisateurs de facteur de forme réduit (mais plus complexes). Concernant les services *broadband* (hautes fréquences), deux constellations de satellites LEO sont actuellement opérationnelles :

- La constellation Starlink (USA), avec un modèle économique agressif pour capter le marché, et génère toutefois un risque de dépendance à une solution américaine propriétaire.
- La constellation OneWeb d'Eutelsat (FRA), qui offre une solution alternative souveraine. Bien qu'il s'agisse aussi d'une solution propriétaire, c'est un actif stratégique, soutenu en particulier par l'Agence des Participation de l'État afin de garantir un accès indépendant à la France et à l'UE à cette infrastructure (critique) ainsi qu'une autonomie stratégique.

Les deux constellations envisagent une transition vers de la 5G NTN pour capter le potentiel de croissance du marché.

[8] Studies on possible new allocations to the mobile-satellite service for direct connectivity between space stations and International Mobile Telecommunications (IMT) user equipment to complement terrestrial IMT network coverage

De plus, de nombreuses autres constellations de satellites LEO sont déjà lancées ou annoncées pour le court terme : Amazon LEO (anciennement nommé Kuiper - USA), Guowang et Thousand Sails (Chine), Lightspeed de Telesat (Canada), IRIS² (Europe).

Cependant, au vu des droits orbitaux et des fréquences qui y sont liées, il n'y aura pas de la place pour plus de 5 ou 6 constellations.

Avec ces constellations, il est attendu une évolution des constellations vers une plus forte intégration aux réseaux terrestres et vers le *cloud* (en particulier Amazon LEO).

Des constellations visant la connectivité des objets se déploient également, en évitant une concurrence frontale avec les grands acteurs des constellations offrant des services large bande ; citons par exemple Kinéis (France).

Concernant les soutiens d'état, IRIS² est mis en œuvre au travers d'un partenariat privé-public qui assure le financement et la fourniture de services de connectivité devenus essentiels aux gouvernements, à la croissance des économies et aux citoyens, est d'aider les acteurs de la chaîne de la valeur à être compétitifs et de munir l'Europe d'une infrastructure indépendante.

Le défi est de faire en sorte que les compétences de plusieurs acteurs impliqués (institutionnelles – comme l'UE avec la Commission Européenne et ses agences, ainsi que l'ESA, les industriels membres du consortium et les Etats membres) puissent contribuer de façon synergétique et efficace à la réussite du projet.

Aux États-Unis, les pouvoirs publics ont financé un nombre limité de projets et apporté leur support à l'un d'entre eux : Starlink. Les 4 caractéristiques majeures de leur approche sont les suivantes :

- Un soutien par des financements publics considérables et souvent « duaux » (notamment liés à la défense et au renseignement (programme starshied ~2.7B$) sans compter le financement indirect lié au soutien à SPACEX/TESLA (38B$))
- La maîtrise d'une intégration verticale pour maximiser ses gains de compétitivité : Starlink a une chaîne de la valeur complétement intégrée, l'Europe n'a pas ce genre de champion, qui serait considéré comme anti concurrentiel.
- Des effets d'échelle immédiats quant à la taille du marché.
    - D'où l'effort européen pour supprimer des barrières européennes handicapant les acteurs économiques dans leur recherche de taille critique (Draghi, Letti),

Principaux défis des méga-constellations

La montée en puissance des méga-constellations (Starlink avec + 10 000 satellites actuellement et 42 000 prévus, GuoWang 13 000 satellites prévus, Amazon LEO + 3000 satellites prévus), et la faible durée de vie de ces satellites (~5 ans), posent de nouveaux problèmes :

- Risques de saturation d'orbite : risques de collisions (syndrome de Kessler), coordination des trajectoires, conflits de fréquences (interférences en cas de non-respects de la réglementation)

- Pollution (métaux nécessaires à la fabrication des satellites et en brulant lors de leur retombée dans l'atmosphère), nous revenons plus largement plus bas sur l'impact environnemental des constellations.
- Pollution lumineuse, réduction de la visibilité notamment dans le cadre de la recherche astronomique.
- Modèles économiques incertains (coûts d'investissements colossaux, stratégie agressive pour empêcher la concurrence)

Le projet Européen IRIS² vise à répondre en partie à ces défis en proposant une constellation de satellites avec un nombre de satellites réduit d'environ 290 (sur le même modèle que OneWeb, avec une orbite à 1200 km, plus haute que ses concurrents).

Les enjeux de souveraineté et de résilience sont désormais centraux dans l'espace. Ils sont devenus majeurs comptes tenus du contexte géopolitique. Il devient crucial pour les États de disposer d'un accès autonome à l'espace et de capacités souveraines, afin de garantir leur indépendance stratégique. Cette autonomie conditionne non seulement la continuité des services critiques en toutes circonstances, mais également la capacité des nations à protéger leurs infrastructures, maîtriser leurs données et préserver leur liberté d'action dans un environnement spatial de plus en plus contesté. Ainsi, certains acteurs auront à cœur de se fournir auprès de plusieurs constellations pour réduire leur dépendance (plutôt avec un prisme géopolitique en général mais les risques de panne peuvent également entrer en jeu) à une seule constellation. De même, pour l'Europe, le traitement du trafic intra-européen par une constellation non européenne peut soulever un certain nombre de questions sur la sécurité et l'intégrité des données (ne serait-ce que l'interception légale).

Impacts environnementaux des solutions NTN

Les infrastructures NTN et satellitaires présentent aujourd'hui des impacts environnementaux significatifs qui devraient être intégrés dès la phase de planification industrielle. L'empreinte carbone de la filière spatiale française atteint environ 1,8 $MtCO_2e$ (2023), dont près de 70 % proviennent des lanceurs et du segment spatial pour les missions télécoms. Les constellations NGSO (Non-Geostationary Orbit) devraient afficher un impact climatique supérieur à celui des systèmes GSO (même si encore en phase d'évaluation), notamment en raison du nombre élevé de satellites LEO, de leur durée de vie plus courte et des opérations de désorbitation. Par ailleurs, le segment spatial concentre environ 50 % de son empreinte carbone dans les phases d'Assembly, Integration and Test (AIT) et de production d'équipements, tandis que le transport des satellites, des équipements et des équipes représente près de 30 %, constituant un levier d'optimisation non négligeable. Enfin, l'absence de standardisation xG entraîne la fabrication d'équipements spécifiques supplémentaires, aggravant l'empreinte globale, alors que pour les systèmes GSO l'impact est davantage lié aux terminaux utilisateurs.

Plusieurs leviers structurants peuvent toutefois réduire ces impacts tout en soutenant le déploiement des NTN. La convergence *via* la standardisation 3GPP entre réseaux terrestres et satellitaires permet de mutualiser les terminaux et les chaînes industrielles, limitant la

production d'équipements dédiés. L'optimisation des architectures de constellation, notamment par l'usage d'OISL (Optical Inter-Satellite Links), réduit la dépendance au segment sol et le nombre de stations passerelles, diminuant ainsi les émissions et l'impact associés. La mise en place d'un référentiel carbone commun à la filière est essentielle pour objectiver les choix technologiques et orienter les investissements. Enfin, la décarbonation des processus industriels (énergies bas-carbone pour l'AIT et la production, éco-conception des satellites, optimisation logistique et recours à des transports décarbonés) constitue un levier prioritaire. Ces actions combinées permettent d'aligner la trajectoire de développement des NTN avec les objectifs climatiques tout en renforçant la compétitivité et la soutenabilité de l'écosystème

4.1.2. Principales recommandations sur les NTN

Nous détaillons ici les recommandations formulées dans la section précédente.

Pour dépasser les problématiques évoquées précédemment dans le domaine satellitaire, et pour garantir la souveraineté spatiale de la France et de l'Europe sur le volet critique des télécommunications, plusieurs axes doivent être adressés :

- 1) Assurer une autonomie dans l'ensemble de la chaîne de valeur
- 2) Valoriser la complémentarité TN-NTN et l'opportunité de la 5G et de la 6G
- 3) Prendre en compte le secteur aval dans la conception des politiques spatiales
- 4) Appréhender la dualité de l'espace extra-atmosphérique
- 5) Faire du cadre réglementaire de la LOS française un avantage compétitif pour l'industrie européenne.

1) **Assurer une autonomie dans l'ensemble de la chaîne de valeur**

La France a l'ambition de rester une puissance spatiale. Pour ce faire, l'autonomie dans la chaîne de valeur apparaît essentielle. Cela supposera notamment de dépasser certains verrous techniques. Or aujourd'hui, deux segments posent des problèmes :

Le segment spatial :

- La forte **hausse de la puissance de calcul embarquée** (*On Board Processing*) pour
    - Répondre aux contraintes d'implémentation de la 5G/6G à bord du satellite, tout en respectant les contraintes énergie et thermique du satellite. Nous avons déjà évoqué l'importance de ceci, notamment dans le cadre de la convergence TN-NTN
    - Embarquer de l'IA.
    - Remarque : Les États-Unis sont extrêmement en avance avec une solution mature notamment grâce à l'entreprise Xilinx. L'Europe n'est pour le moment pas en mesure de proposer une solution pouvant concurrencer celle de Xilinx. Il y a donc à la fois un problème de compétitivité et de souveraineté dans ce domaine. Enfin le coût de cette solution reste très élevé.

- **L'émergence d'antennes actives et d'antennes de grandes tailles** pour augmenter la capacité, améliorer le bilan de liaison et réduire les contraintes sur les terminaux utilisateurs.
- Le développement des communications optiques spatiales inter-satellite pour le routage et sol-satellite pour dépasser les limitations des liens radios classiques.
- Le déploiement de constellations dédiées pour le « ***direct to phone*** » ou pour **l'Internet des Objets** (IoT).

Le segment sol :

- Les **lanceurs** : leur disponibilité pourrait être un problème pour le lancement des projets européens de constellation et représentent aujourd'hui une limitation claire dans la capacité de l'Europe à avoir accès à l'espace vis-à-vis des autres puissances, notamment américaine et chinoise.
- Les **terminaux** satellitaires + modem (chipset) + antenne. En particulier, le gain en performances des antennes électroniques, en particulier des **antennes utilisateurs** qui nécessitent une réduction du coût de revient et une maîtrise de la chaîne d'approvisionnement. De manière générale, le développement d'antennes électroniques toujours plus performantes. En particulier, pour répondre aux nouveaux besoins : voiture connectée, trains, aéronautique, sécurité et services d'urgences … **Aucun des programmes à l'échelle européenne comme nationale ne s'attaque entièrement à la question de la conception et de la production des terminaux satellitaires,** secteur dans lequel notre dépendance vis-à-vis des Etats Unis et d'Israël (si l'on écarte les solutions chinoises) est considérable. Or, l'Europe ne peut prétendre développer une autonomie stratégique notamment dans les télécommunications sécurisées en conservant une telle dépendance. C'est un sujet qui mérite qu'une réflexion soit menée et des moyens mis en œuvre très vite. L'antenne étant un élément clé pour fournir des services par satellite, il est important que l'Europe se dote d'un nombre suffisant de fabricants pour couvrir les différents cas d'usages avec des prix et des performances compétitifs - face à la concurrence chinoise par exemple. Aujourd'hui il y a plusieurs petits fabricants, qui ne peuvent pas assurer des gros volumes et qui n'ont pas la possibilité de financer des chipsets RF dédiés pour améliorer les performances.

Jusqu'en 2024, la situation européenne favorisait une dispersion des financements, dont l'impact restait limité. Une approche plus efficace aurait reposé sur une vision stratégique à l'échelle européenne, structurée autour de financements ou de commandes publiques de grande ampleur, concentrés sur un nombre restreint de projets hautement ciblés, à l'image du modèle américain.

La crise du COVID et la guerre en Ukraine sont deux facteurs qui ont contribué à une prise de conscience de l'UE se traduisant sur la nécessité de recouvrer ou préserver une souveraineté dans des secteurs stratégiques, dont le spatial. Cette prise de conscience se manifeste au niveau Européen par deux réponses :

- Un **budget spatial européen aujourd'hui en croissance** : UE : 14,5 Mds € pour les 6 ans de la période 2021-2027, budget qui pourrait doubler pour la période 2028-2034.

L'ESA s'est vu attribuer un budget « historique » de plus de 22 milliards d'euros voté à la Conférence ministérielle de novembre 2025, avec une perte de position de la France devenue moins contributrice que l'Allemagne (passage de 23 à 15 % du budget global entre 2020 et 2025).

- Le **programme de constellation IRIS², programme dual en PPP, de grande envergure et structurant, en réponse à l'approche US de *space dominance***. Une commande publique dans ce domaine est vitale, si l'Europe veut pouvoir être un acteur du marché des constellations : aucun projet de constellation purement commerciale ne s'est avéré viable à ce jour :
    - Starlink est largement subventionné,
    - OneWeb a fait faillite avant d'être repris en 2020 avec l'aide du gouvernement britannique,
    - Telesat n'arrivait pas à boucler son financement : il semblerait qu'ils aient reçu une aide de 2,4 milliards de dollars par le gouvernement canadien.

À noter : les récents développements de l'administration Trump et les déclarations d'Elon Musk que ce soit sur le Canada, l'Ukraine ou le Groenland, ouvrent une fenêtre d'opportunité pour le secteur français/européen. **Cependant, sans soutien massif étatique, il sera difficile de rivaliser avec les USA ou très prochainement la Chine.**

Recommandation n° 11

Construire une autonomie stratégique européenne sur l'ensemble de la chaîne de valeur des réseaux non terrestres (NTN), ce qui inclut l'embarquement de l'IA.

Pour ce faire, la France et l'Europe doivent soutenir l'émergence des technologies critiques nécessaires aux NTN, et renforcer leur capacité à produire des briques technologiques matérielles clés à ces systèmes : processeurs embarqués, antennes, lanceurs, terminaux et chipsets, technologies optiques inter-satellites (OISL), modems 5G/6G NTN, plateformes matérielles pour l'embarquement simplifié du calcul et de l'IA, etc. Toutes ces technologies ne sont pour le moment pas suffisamment matures en Europe et la dépendance envers les États-Unis, la Corée du Sud ou Taïwan est extrêmement importante. La conception et le savoir-faire technologique doivent donc être préservés et renforcés, et les chaînes de valeur doivent être sécurisées et diversifiées, d'autant plus que, outre les acteurs historiques, des jeunes entreprises se positionnent avec un fort potentiel dans ce secteur, y compris pour l'IA embarquée.

Pour ce faire, la mise en place de programmes spécifiques, notamment en matière de R&D, avec un soutien financier important permettrait de rattraper le retard en la matière et bâtir une réelle autonomie stratégique européenne. Ainsi, il semble essentiel d'assurer une connexion forte avec les initiatives européennes existantes que sont le *Semiconductor Act* et le *Chip Act* afin de capitaliser sur les avancées.

L'Union européenne et la France doivent renforcer leur soutien politique, financier et industriel au programme IRIS². Ce dernier constitue un levier stratégique majeur pour garantir une infrastructure souveraine de télécommunications par satellites. Soulignons

l'importance d'infrastructure souveraine pour le besoin *broadband* comme *narrowband* (IoMT, D2D, D2H - *Gov/Defense*). Afin d'éviter la fragmentation des financements, l'Union européenne doit éviter la multiplication de constellations nationales concurrentes au profit d'un programme commun porté par l'écosystème industriel européen dans une optique de souveraineté stratégique, technologique et industrielle et de compétitivité européenne.

Par ailleurs, des outils pour la conception, la planification et le contrôle optimal de ces systèmes doivent être conçus, la France disposant d'une avance certaine dans ce domaine. Ces outils doivent permettre non seulement d'optimiser certaines fonctions clés, comme l'embarquement de l'intelligence ou le routage inter-satellite, mais doivent également permettre d'évaluer les risques de saturation et de collisions, impactant la résilience et la production de déchets dans l'espace, ainsi que d'autres risques écologiques liés notamment à la faible espérance de vie des satellites en orbite basse ou à la pollution visuelle affectant les travaux des astronomes.

2) **Valoriser la complémentarité TN-NTN et l'opportunité de la 5G**

Il s'agit de donner plus de place aux solutions satellitaires dans le développement des infrastructures de télécommunications et dans les stratégies d'usage de ces infrastructures développées par les pouvoirs publics :

- Les solutions spatiales sont par nature des compléments des réseaux terrestres auxquels elles procurent une résilience sans équivalent ;
    - Ex : gestion des catastrophes naturelles,
    - Ex : recours aux capacités d'opérateurs satellitaires privés de confiance pour les besoins de défense, en plus de l'usage des capacités patrimoniales des satellites militaires, qui ne suffisent pas à apporter une couverture géographique mondiale,

De plus, cette recherche de résilience pousse à l'adoption des standards afin de permettre, grâce à l'interopérabilité, l'accès à une pluralité de réseaux de connectivité, il apparaît donc important de favoriser l'interopérabilité des terminaux terrestres et satellitaires, en favorisant **l'adoption par le monde du satellite de solutions standardisées**. En particulier, la norme 5G, définie par le 3GPP est reconnue comme une technologie mondiale majeure, et adoptée par les opérateurs terrestres. La 5G est un changement de paradigme profond car elle initie la convergence des réseaux terrestres et satellitaires et l'émergence de normes. L'ouverture du standard 5G au NTN (requise pour la constellation IRIS²) permettra au monde du satellite de sortir d'un marché de niche, lui donnant l'opportunité de s'ouvrir à l'écosystème de la 5G, en faisant bénéficier l'industrie satellitaire des effets d'échelle de la connectivité terrestre. La chaîne d'approvisionnement dans son intégralité pourrait accéder à une meilleure efficacité de ses coûts, indispensable pour la pérennité des acteurs dans le cadre d'un développement de marché de masse. De plus, l'adoption de solutions standardisées permet l'interopérabilité des solutions, et ne contraint plus les utilisateurs à dépendre de solutions propriétaires. À terme, le déploiement de terminaux satellitaires 5G puis 6G, permettra le passage d'une infrastructure à l'autre de manière fluide et transparente (ex : terminaux voitures et avions).

Il s'agit donc de **positionner l'Europe et en particulier la France comme leader naturel des capacités 5G NTN spatiale** à l'échelle mondiale. Il faut donc agir maintenant afin de pouvoir influencer les évolutions du standard nécessaires à nos besoins spatiaux ainsi qu'à l'ensemble de l'écosystème. Dans le même temps, il est fondamental de **développer les briques technologiques les plus critiques** afin de répondre à ces évolutions. Pour le marché des communications par satellites, cela signifie aussi la **nécessité de s'insérer dans un écosystème d'acteurs beaucoup plus puissants** afin de s'assurer d'une bonne prise en compte du segment spatial dans les normes telles que celles travaillées au sein du 3GPP.

Recommandation n° 12

Les réseaux satellitaires et non satellitaires doivent être interopérables pour renforcer résilience, couverture et services critiques. Le passage aux standards 5G NTN (requis pour la constellation IRIS²) et plus tard 6G est un levier majeur pour garantir l'interopérabilité TN/NTN, réduire les dépendances aux solutions propriétaires, et ouvrir le satellite à un marché de masse grâce aux effets d'échelle de la 5G.

La France et l'Europe doivent donc s'impliquer davantage dans la normalisation (notamment 3GPP) et l'ensemble de la chaîne technologique doit être soutenue.

Les initiatives de la stratégie d'accélération, telles que le PEPR réseaux du futur pour la recherche, France6G sur l'implication dans les standards ou FRAMExG pour développer des portefeuilles de brevets essentiels aux normes peuvent être des solutions, si comme souhaité, elles perdurent dans le temps.

La rencontre en mai 2026 entre le Président Macron et le groupe Science 7 (S7) du G7 a souligné l'importance de renforcer la recherche dans le domaine des réseaux non terrestres (NTN) et de consolider davantage les synergies entre les mondes académique et industriel. S'il y a consensus sur le fait qu'une maîtrise scientifique et technologique de ces réseaux est absolument nécessaire aux pays du G7, et en particulier en Europe, au vu des enjeux géostratégiques, il y a aussi consensus sur le fait que la régulation du domaine, et en particulier l'attribution des orbites, est un sujet critique qui requiert de nouvelles bases scientifiques pour la prise de décision[9]. Ces concepts sont détaillés dans le document « Large Satellite Constellations: Perspectives and Challenges ».

La France dispose, dans ce domaine, d'atouts majeurs ainsi que de résultats scientifiques et technologiques différenciants qu'il convient de valoriser pleinement. Les actions menées dans le cadre du PEPR Réseaux du Futur s'inscrivent pleinement dans cette dynamique et méritent d'être pérennisées au-delà de l'échéance du programme afin de consolider les acquis et d'amplifier leur impact.

[9] Notamment en fonction de l'évaluation de la capacité de support de ces ressources orbitales (problème des collisions), de l'évaluation des interférences optiques et radio (astronomie, communications terrestres), et de l'évaluation des transformations de la chimie de la haute atmosphère qui découle des lancements et des rentrées de satellites.

3) Prendre en compte le secteur aval dans la conception des politiques spatiales

Dans le cadre de la conception de la politique spatiale, il semble essentiel de suffisamment **prendre en compte la parole des opérateurs spatiaux**, qui :

- Ont un contact direct ou étroit avec la demande finale des utilisateurs[10]
- Assument une part essentielle du risque financier.

Le dialogue avec les industriels est indispensable et pour l'instant insuffisant.

Au-delà des opérateurs, c'est la voix de **tout le secteur aval** qui doit être écoutée par l'ensemble de la filière pour développer et opérer des solutions économiquement viables répondant aux usages mais aussi aux contraintes de souveraineté et de résilience, de sorte que les financements et les commandes ne soient plus uniquement orientés principalement vers les activités amont. Même si l'infrastructure est indispensable, l'actualité montre que la valeur ajoutée se crée essentiellement dans les services et les applications, et que la donnée spatiale est devenue centrale. Ce phénomène ne doit pas être mis de côté, au risque de faire prendre encore plus de retard à l'ensemble du secteur spatial français et européen.

Recommandation n° 13

Au niveau politique, les opérateurs et autres acteurs aval (services, IoT, applications) doivent être intégrés à la conception des politiques spatiales, afin d'éviter un déséquilibre entre investissements industriels amont et besoins réels du marché. Au niveau économique, il est essentiel de rééquilibrer la répartition des revenus entre les acteurs qui financent et déploient les infrastructures et ceux qui en génèrent de la valeur, de manière à garantir un modèle durable et équitable pour l'ensemble de la chaîne.

4) Appréhender la dualité de l'espace extra-atmosphérique

L'espace est passé d'un champ concurrentiel à un champ de confrontation :

- La conception des architectures militaires et commerciales sont proches et liées
- Les militaires ne pourront pas seuls financer et maintenir opérationnelles des constellations
- Par ailleurs, ce maillage de réseaux est très coûteux et n'est pas à la portée des start-ups ou PME

L'avenir du spatial est donc dans la dualité. Ce côté dual apparaît de manière éclatante aujourd'hui :

- Les Ukrainiens utilisent des moyens commerciaux/civils à des fins militaires
- Les Russes attaquent et brouillent les capacités commerciales

Afin de gagner en compétitivité, il s'agit de favoriser un projet global englobant à la fois le civil, le commercial, le scientifique et le militaire, afin de ne pas disperser les ressources. Par

[10] Les contraintes sur les terminaux mentionnées plus haut sont à débloquer pour permettre le développement des usages et services.

exemple, les solutions *multi-tenancy*, permettant de porter plusieurs usages duaux, publics et privés sur la même infrastructure satellitaire (avec des segments sols potentiellement spécialisés par usage), pourrait permettre de répondre à cet objectif. Pour gagner en compétitivité face aux États-Unis, (où l'Etat aide ses acteurs à travers de PPP duaux, cf. Space X), une vision globale et duale et transverse s'impose. Les architectures doivent être optimisées, et permettre la permanence. Enfin, la résilience passera par la diversité et par le nombre (dans les orbites et dans les missions).

Recommandation n° 14

Les frontières entre usages civils, commerciaux et militaires des applications spatiales s'estompent : les constellations commerciales sont utilisées à des fins militaires, et sont régulièrement ciblées ou brouillées. Pour rester compétitive, l'Europe doit adopter une approche duale et intégrée, afin d'optimiser l'utilisation des ressources civiles et militaires, en favorisant les constellations à double usage et en s'appuyant sur des partenariats public/privé puissants, comme le font les États-Unis.

Il faudrait mettre en place un pilotage stratégique européen, éventuellement de type PPP (comme 6GSNS) dual civil/défense qui soit en charge de la gestion du projet, de l'émergence des standards nécessaires, de l'organisation des programmes de R&D nécessaires et de la stratégie de partage public/privé des usages, de la vision de bout en bout (segments sols inclus).

5) **Faire du cadre réglementaire de la LOS française un avantage compétitif pour l'industrie européenne.**

La France est un des rares pays à s'être doté d'une Loi sur les Opérations Spatiales (LOS) en 2008 :

- La LOS fixe, pour les opérateurs français comme Eutelsat, un cadre très exigeant en termes de prévention et de gestion des débris spatiaux.
- Les opérations associées à cette gestion des débris sont coûteuses, chronophages et complexes.
- Or, les opérateurs étrangers, y compris au sein même de l'Union européenne[11] ne jouent pas avec les mêmes règles du jeu, mais se voient pourtant accorder un accès aux marchés français et européen.

L'UE réfléchit au sujet et entame des travaux pour définir une réglementation européenne en la matière (*EU Space Act*), l'intérêt de la France et des opérateurs français est d'obtenir :

- Une harmonisation des règles de gestion du trafic spatial (*Space Traffic Management*), à l'échelle européenne puis internationale, sur la base des exigences du modèle français.

[11] Tandis que le Luxembourg se contente d'un cadre très simplifié et peu contraignant, l'Allemagne elle, ne s'est pas encore dotée d'une loi spatiale nationale.

- Conséquence attendue : la garantie que chaque entrant sur le marché français et européen ait une obligation de respecter un niveau d'exigence identique en matière de durabilité des activités spatiales.

Cette mesure, bien que d'ordre réglementaire, contribuerait à renforcer la compétitivité des opérateurs français pour l'accès à ces marchés, dans la logique de ce que le RGPD représente pour les entreprises européennes dans le domaine de la protection des données personnelles.

Recommandation n° 15

Le futur cadre européen (*EU Space Act*) doit harmoniser au sein de l'Union le niveau d'exigence de la LOS française en matière de prévention et de gestion des débris spatiaux, de gestion du trafic spatial, et de durabilité des activités spatiales, afin d'interdire les pratiques de « *dumping* » réglementaire, de garantir des conditions de concurrence équitables entre acteurs, et donc de renforcer la compétitivité des opérateurs français. L'accès au marché européen par des opérateurs extra-européens doit par ailleurs être conditionné au respect des mêmes normes.

Synthèse des recommandations concernant la convergence TN-NTN

La France et l'Europe doivent :

- **Augmenter, coordonner et concentrer les investissements et le soutien public** dans les briques critiques de la chaîne de valeur TN-NTN, notamment en R&D.
- **Assurer l'interopérabilité TN/NTN** en accélérant l'adoption des standards 5G/6G NTN en renforçant la participation française et européenne au sein des instances de normalisation (3GPP) et en soutenant les industriels développant ces technologies.
- **Intégrer les capacités satellitaires souveraines** aux stratégies nationales et européennes de connectivité critique : continuité de service, gestion de crise, défense, etc.
- **Impliquer le secteur aval** (opérateurs, IoT, services, données) dans la conception des politiques spatiales, par exemple par consultations des acteurs concernés.
- **Mieux répartir les investissements et la valeur qui en est générée** sur toute la chaîne de valeur
- Structurer une **approche duale civil/défense** : soutenir des constellations duales, mutualiser les investissements, développer des architectures multi-usages, lancer des PPP comparables au modèle américain.
- **Soutenir fermement IRIS²** comme infrastructure centrale européenne : garantir son financement, accélérer son déploiement, en faire la référence européenne pour les services de télécommunications critiques et sécurisées. S'opposer à la fragmentation des financements, et l'émergence de projets nationaux concurrents d'IRIS², fragilisant l'ensemble de la filière
- **Harmoniser le cadre réglementaire européen sur le modèle de la LOS française**, en imposant un cadre normatif strict en matière de prévention et de gestion des débris spatiaux, de gestion du trafic spatial, et de durabilité des activités spatiales. Conditionner l'accès au marché européen au respect de ces exigences par tous les opérateurs, y compris extraeuropéens.

4.1.3. Acteurs clés français et européens des NTN

La France joue un rôle de leader dans le secteur spatial européen et dans la connectivité par le segment satellite, grâce à de nombreux acteurs tels que :

- CNES – Agence spatiale française
- Eutelsat Group – opérateur de satellites GEO et LEO, et fournisseur de connectivité pour les différents marchés
- Airbus Defense & Space – constructeur de satellites, intégrateur systèmes bout en bout et opérateur.
- Thales Alenia Space – constructeur de satellites et de systèmes « *baseband* »
- EasiIC – constructeur de chipsets DVB-S2
- Greenerwave – start-up constructeur d'antennes électroniques
- Kineis – opérateur IoT
- Fort écosystème spatial : Ternwaves, 3ZA, Exotrail, Leanspace, U-SPACE, SpaceLocker, Enensys, NanoExplore, etc.

En Europe, on peut citer :

- ESA – Agence spatiale européenne
- Opérateurs satellitaires : SES (Lux), Inmarsat (UK)
- Acteurs des télécommunications : Nokia, Ericsson

À noter que les principaux fabricants de puces électroniques pour la 5G ne sont pas Européens : Qualcomm (USA) et MediaTek (Taïwan).

4.2. *Cloud* (IaaS, PaaS, SaaS ; *data centers – edge*, centres de colocalisation)

Les fournisseurs de services *cloud* (IaaS, PaaS, SaaS), d'hébergement en *data centers* et de capacités à l'*edge* sont au cœur du futur des infrastructures numériques nécessaires aux usages fondés sur les données (collectées et traitées en temps réel ou différé) et l'IA (citons par exemple les jumeaux numériques pour l'opération d'usines et d'infrastructures critiques, de plus en plus interdépendantes, la vision par ordinateur utilisée dans les process industriels (usine4.0/5.0), l'agriculture de précision, la maintenance prédictive ou l'apprentissage fédéré.), car ils contribuent fortement à la création d'un *continuum* capable de placer dynamiquement les charges de travail en fonction des contraintes de confidentialité, de souveraineté, de latence, de coût et d'empreinte carbone.

Ceci est particulièrement important dans le cadre de l'IA multi-agents multi-acteurs et pour la mise en place de plans de gouvernance de l'IA et des données. Les agents seront souvent déployés à l'*edge* pour des raisons de sécurité (pas nécessairement au MEC, mais dans des mini *data centers* localisés et souverains).

Comme déjà évoqué, dans de nombreuses applications en lien avec des services d'observation de la terre, les agents pourront être embarqués dans des constellations de satellites (les cas d'usage sont nombreux, notamment dans le cadre militaire).

L'essor de l'IA et tout particulièrement de l'IA générative et les LLM, a imposé le déploiement massif d'accélérateurs dans le *cloud* (GPU/TPU/NPU) et de piles logicielles spécialisées, ainsi qu'un ordonnancement adapté aux traitements temps réel comme aux traitements batch (y

compris des logiques d'allocation "temps/job"), adossés à des capacités de DevOps et d'observabilité, de FinOps/GreenOps et de mesure carbone.

La connectivité intra *data centers* est devenue un facteur critique, nous avons déjà mentionné l'explosion du marché des fibres optiques pour ce besoin. À titre d'exemple, Microsoft aujourd'hui conçoit et déploie ses propres fibres à cœur creux pour des besoins d'optimisation de latences inter data centres (- 33 %) et de réduction des coûts (moins de répéteurs) avec une ambition de 15 000 km à terme !

La sécurité et la conformité structurent les choix d'architecture : options de « *cloud* de confiance », résidence et gouvernance des données, chiffrement et gestion de clés, exécution confidentielle, posture Zero Trust, alignement avec les cadres RGPD/NIS2/*AI Act* et référentiels nationaux/UE. Pour limiter la fragmentation et éviter les dépendances excessives, l'écosystème privilégie standards ouverts et *open source*, expose des APIs interopérables.

Dans l'Annexe I nous présentons une synthèse sur le positionnement des grands acteurs du *cloud* aujourd'hui, notamment des GAFAM. Face à l'évidence du faible positionnement Européen, la question des trajectoires pour la souveraineté des infrastructures numériques se pose. Pouvoir concurrencer frontalement les grands acteurs du *cloud* « générique » (GAFAM et équivalents chinois) est un objectif inatteignable à court ou moyen terme.

En revanche, la France et l'Europe peuvent se positionner en leader dans un cadre de *continuum* vertical (voir plus haut), en forte interaction technologique et d'affaires entre les acteurs des infrastructures numériques et ceux de divers verticaux où l'Europe est forte. Côté IA cela passe par des investissements dans les petits modèles de langage adaptés à ce *continuum* vertical, à la mise en place de plans de gouvernance de l'IA agentique comme cela a été décrit plus haut et, surtout, à la mise en place d'une stratégie inter-filières.

4.3. Équipementiers

Les acteurs traditionnels des réseaux de télécommunications (équipementiers comme opérateurs) doivent s'adapter aux évolutions majeures (*cloudification*, convergence matérielle et logicielle avec le monde IT, évolutions vers l'*edge*, utilisation d'*open source*, impact de l'IA dans les solutions et pour les solutions). Tout ceci induit des transformations profondes, comme cela peut être observé dans le cas de Nokia, avec l'investissement de Nvidia dans NOKIA, avec une réorganisation importante du positionnement de l'entreprise et de sa R&D. À titre d'exemple, nous présentons la synthèse de l'interview à M. Thierry Gruszka, Head of Cisco Innovation Labs France, Strategy Corporate Development & Incubation.

Le cas CISCO : le routage devient une commodité, l'avenir est au logiciel de supervision des réseaux

CISCO considère deux types de marchés avec des dynamiques et des spécificités en termes de vitesse d'appropriation des nouveaux concepts.

- Ainsi Côté opérateurs de télécommunications : Cisco constate un recul relatif du marché, marqué par la virtualisation des réseaux et la transformation des routeurs

en serveurs. Cisco se repositionne sur des segments à plus forte valeur ajoutée : cœur de réseau, optique (switchs, transceivers), sécurité et software.
- Côté entreprises : la virtualisation est moins adoptée qu'attendu. Beaucoup de DSI restent attachés aux équipements physiques. Cisco unifie donc LAN, Wi-Fi et sécurité autour de dashboards en mode SaaS centralisés (Meraki, rachat de Splunk[12]).

Il existe cependant des évolutions transverses à ces deux marchés :

- Forte montée de la cybersécurité, de l'observabilité et de l'intégration IA (notamment *via* le rachat de Splunk et le développement de modèles IA dédiés aux réseaux).
- L'arrivée des tableaux de bord (*dashboard*) pour simplifier les plateformes de gestion dans le *cloud* avec une dimension de *dashboard* régionaux (Europe, US, ASIE) pour des besoins de souveraineté.

Finalement, Cisco interroge sur l'avenir des infrastructures 5G/routeurs à faible marge et se désengage du LORA en revanche il s'attend à une valorisation plus sur le software (dont le SW de gestion des infrastructures (en lien avec les data model associés), l'orchestration et la sécurité plutôt que sur le *hardware*. Il faut enfin noter que CISCO est aussi développeur de serveurs et pour eux du fait des besoin de l'IA le HPC devient la norme (80 % du marché).

En ce qui concerne les technologies clés, pour CISCO, l'optique (photonique) (et notamment en lien avec les futurs réseaux quantique) mais aussi les besoins de technologies de refroidissement des *data centers* sont considérés comme majeurs.

4.4. Cybersécurité des infrastructures et solutions pour la cybersécurité applicative

Comme déjà évoqué, la 6G consacre la **« *softwarisation* »** intégrale, la 5G était déjà voulue comme *« cloud native »*, les fonctions réseau ne sont plus uniquement des matériels physiques mais des micro-services virtualisés distribués spatialement et dynamiquement de bout en bout.

Il s'agit donc de considérer la Sécurité tout au long du cycle de vie des logiciels, la virtualisation et le code devenant aussi critique que le matériel. Les défis spécifiques résidant dans la gestion des mises à jour et de la traçabilité de la chaîne d'approvisionnement dans un environnement multi-acteurs.

Les futures infrastructures numériques ne sont pas seulement convergentes dans la réutilisation de technologies logicielles, elles doivent intégrer des capacités de calcul distribué qui amènent aussi une surface d'attaque spécifique, héritée du *cloud* historique centralisé, mais augmentée par la nature distribuée. Cela impacte significativement les phases de détection et réponse lorsque des attaques surviennent nécessitant coordination et coopération entre différents segments/parties.

[12] Cisco finalise l'acquisition de Splunk pour 28 milliards de dollars.

Recommandation n° 16

La France dispose de compétences au meilleur niveau international dans le domaine de la cybersécurité et d'acteurs bien positionnés sur certains secteurs. Ceux-ci doivent être soutenus dans leurs efforts d'innovation pour répondre aux changements de paradigme évoqués dans ce document et maintenir un positionnement fort.

Il est donc nécessaire d'intégrer les acteurs du secteur dans les diverses initiatives proposées dans les recommandations précédentes.

Les transformations mentionnées dans ce document représentent une opportunité pour l'émergence de nouveaux acteurs, ce qui requiert également une stratégie nationale et un soutien fort, notamment en lien avec la croissance des budgets militaires.

Des acteurs de la sécurité intérieure et de la sécurité extérieure doivent donc également intégrer les initiatives proposées.

La France est également forte dans le domaine du quantique, que ce soit dans l'utilisation de quantique pour la distribution des clés (QKD) ou sur la sécurité post quantique (PQC, comment sécuriser les systèmes à l'ère où le quantique peut affaiblir considérablement les méthodes de cybersécurité actuelles).

Deux sujets d'innovation sont ici à soutenir particulièrement dans les programmes à venir : la conception jointe QKD-PQC et les réseaux quantiques (sujet qui par ailleurs dépasse largement la cybersécurité et qui couvre en particulier le calcul quantique distribué).

Les IA : sécuriser leurs usages, les utiliser pour la sécurité

L'infrastructure convergée est le socle de déploiement de l'IA et intersecte largement l'état de l'art en matière de sécurité d'IA. Il faut distinguer ce que l'infrastructure permet à des applications tierces et les usages propres pour des futures infrastructures dites « *AI-native* ». Une partie commune pour les aspects d'apprentissage sera la maîtrise des cycles de vie des données depuis leur collection, stockage, maintenance d'un niveau de qualité, traçabilité, conformité à la régulation… Autres aspects communs les orientations liées au paradigme *« zero trust »* et sécurité centrée sur la donnée (DCS) qui conviendra de projeter au sein des futures architectures.

Un pan prometteur se fait jour au-delà de l'IA statistique (ou hybride) en la matière de l'IA agentique. Les opérations de sécurité d'une infrastructure convergée, très souvent biaisée par des approches historiques (*cloud* ou réseau) peuvent trouver une cohérence et interopérabilité grâce à l'IA agentique. Une approche multi-agent pouvant typiquement faciliter les interactions dans une approche fédérée et appliquer des politiques « intelligente » pour assurer sécurité et résilience. Un danger majeur ici serait de laisser des acteurs puissants imposer leurs politiques avec la réintroduction d'une couche chapeau elle-même propriétaire.

Recommandation n° 17

Promouvoir une action européenne pour éviter le risque de l'émergence d'une couche de cybersécurité propriétaire, pilotée par les grands acteurs du *cloud* et de l'IA générative et traduire dans les divers *« Act »* cette vision non-propriétaire de la cybersécurité des infrastructures numériques.

Standards et régulations

La sécurité est traditionnellement marquée par une démarche d'évaluation, la complexité des systèmes et services, la dynamique temporelle impose de revisiter l'état de l'art. Les enjeux sont ici stratégiques pour différencier les solutions méritantes au sens du respect de la souveraineté et l'information légitime dont devraient bénéficier les utilisateurs.

4.5. Opération, gestion, maintenance : automatisation, apport des jumeaux numériques

Dans un contexte de montée en complexité, l'exploitation, la gestion et la maintenance des réseaux évoluent vers des opérations fortement automatisées. Sur le plan des fondations, la démarche requiert des pipelines de données gouvernés, une observabilité de bout en bout corrélant métriques, logs et traces sur plusieurs couches, et une posture Zero Trust. Elle suppose également l'intégration multifournisseurs au sein des OSS/BSS, en contexte hétérogène. Certains standards comme le TM Forum définissent des modèles d'automatisation (*Autonomous levels* - ANL) et de modélisation de l'architecture (*Open Digital Architecture* - ODA) permettant de créer un cadre commun.

4.5.1. De nouvelles capacités d'exploitation-maintenance grâce à une utilisation d'IA

La supervision et l'exploitation des réseaux (6G et/ou de transport) évoluent fortement avec le déploiement de solutions d'automatisation et l'usage croissant de l'IA. Les réseaux mobiles et fixes évoluent également dans leur standardisation et leur conception vers des solutions plus automatisées intégrant de plus en plus des capacités de raisonnement, c'est-à-dire des fonctionnalités cognitives.

Cette évolution a vocation à réduire les coûts d'exploitation, améliorer les performances, développer la flexibilité, accélérer la mise en œuvre de solutions innovantes, etc. Il est également utile de noter que cette automatisation associée à l'IA permet de mettre en œuvre des approches basées sur l'intention, associant par exemple des critères de performances à des objectifs d'efficacité énergétique.

Ce nouveau type d'exploitation/maintenance (OAM) est rendu possible par l'essor rapide des agents intelligents (*AI Agents*), dont l'impact devient particulièrement visible en 2025, notamment au sein des différents organismes de standardisation des télécommunications (3GPP, ITU-T, etc.).

Du point de vue des besoins en termes de latence, l'OAM occupe une position unique, comme illustré dans la figure suivante.

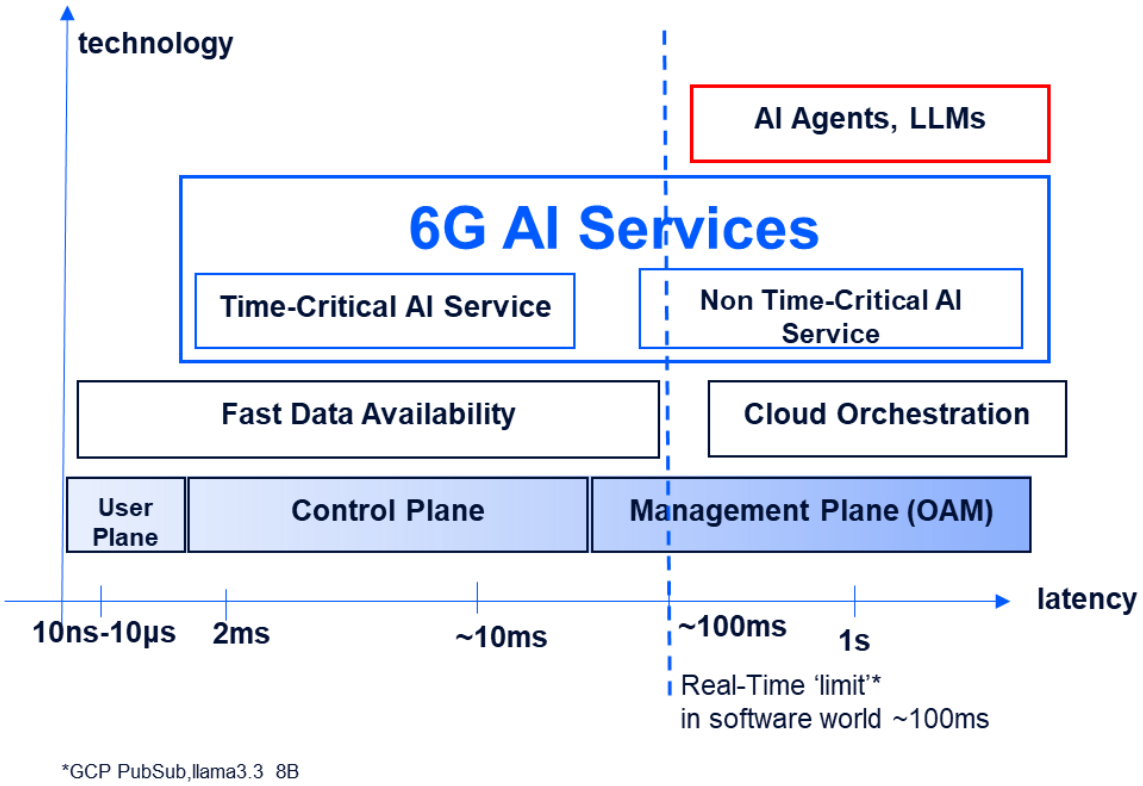


Fig. 1 : Latences des différentes technologies dans les réseaux informatiques et la 6G

Bien que l'OAM puisse atteindre des latences en temps réel, ses fonctions principales opèrent généralement à des niveaux de latence supérieurs à ceux des plans utilisateur et contrôle. Cette caractéristique rend l'OAM particulièrement adapté à l'intégration des technologies agentiques, c'est-à-dire des agents intelligents capables de raisonnement, dont les latences opérationnelles sont proches de celles de l'OAM et des modèles de type LLM (comme le montre la figure).

De plus, les latences des services IA en 6G et de l'orchestration *cloud* sont également compatibles avec les opérations OAM. Cela place l'OAM dans une position stratégique en tant que précurseur de l'adoption des agents intelligents dans les opérations télécoms, ouvrant la voie à une gestion de réseau entièrement personnalisable et autonome.

4.5.2. Des jumeaux numériques pour les réseaux

L'introduction de jumeaux numériques de réseau permet de simuler topologies et politiques et d'évaluer en amont les impacts (fréquences, allocation, migrations/rollback) afin de sécuriser les changements.

Un jumeau numérique est défini, selon Analysys Mason[13], comme une réplique numérique d'un actif physique, d'un système, d'une construction logique, d'un processus, d'un service ou d'un client qui reflète son homologue réel en temps réel. Il doit avoir des capacités d'apprentissage automatique/intelligence artificielle pour tester, optimiser et prédire les futures défaillances ou problèmes de résilience. Les jumeaux numériques doivent prendre en charge un flux de données bidirectionnel pour les tests hors ligne et l'application de nouvelles configurations.

Le paragraphe suivant fournit une catégorisation des principaux acteurs dans le domaine des jumeaux numériques[14].

1. *Jumeaux numériques de clients*

Ils simulent les expériences individuelles des clients et prédisent leurs comportements. On peut citer Amdocs et Pega comme acteurs. Amdocs est largement reconnu pour ses logiciels et services destinés aux fournisseurs de services de communication, de médias et de services financiers. Pega est connu pour ses logiciels d'engagement client et d'automatisation des processus numériques.

2. *Jumeaux numériques d'infrastructures*

On peut distinguer sous cette catégorie trois types de jumeaux numériques, à savoir ceux dédiés aux réseaux, ceux dédiés aux entreprises et enfin ceux dédiés aux data-centres.

a) *Jumeaux numériques de réseaux*

Ils modélisent les éléments logiques et physiques du réseau, le trafic et les services. On peut citer Nokia, Ericsson, et Netcracker comme exemple d'acteurs fournissant des jumeaux numériques pour les réseaux. Nokia et Ericsson sont des équipementiers traditionnels quand Netcracker, filiale de NEC est plus connu pour développer des solutions de transformation numérique (réseaux & IT) à base d'agent IA.

b) *Jumeaux numériques d'entreprises*

Ces jumeaux fusionnent les données provenant des objets connectés (IoT) pour une vue d'ensemble des actifs et des processus. On peut citer AWS et Siemens comme acteurs dans ce domaine. AWS (Amazon Web Services), connu pour ses services de *cloud computing* robustes, propose des solutions IoT qui incluent des capacités de jumeau numérique, permettant aux entreprises de créer des représentations virtuelles de systèmes physiques. Siemens est un leader dans l'automatisation industrielle et la numérisation, il propose des solutions complètes de jumeaux numériques largement utilisées dans divers secteurs pour optimiser les opérations et améliorer la productivité.

c) *Jumeaux numériques de data-centres*

[13] Digital twins in telecoms: a framework for understanding the opportunity and ecosystem. Analysys Mason. 16 Avril 2025.

[14] Digital twins in telecoms: a framework for understanding the opportunity and ecosystem. Analysys Mason. 16 avril 2025.

Ces jumeaux, quant à eux, permettent de représenter les data-centres, leurs environnements, et les configurations de leurs ressources. On peut citer comme acteurs dans ce domaine, EkkoSense et Sunbird. L'acteur EkkoSense est connu pour son accent sur l'optimisation des *data centers* grâce à la technologie des jumeaux numériques, offrant des solutions de surveillance et de gestion en temps réel. Quant à Sunbird, il propose des solutions de gestion de l'infrastructure des *data centers* (DCIM) qui intègrent des capacités de jumeaux numériques pour améliorer l'efficacité opérationnelle.

Ces différents jumeaux numériques nécessiteront des données de trafic pour réaliser les simulations permettant par exemple de tester la pertinence d'un nouveau paramétrage. Ces données peuvent être réelles ou synthétiques, mais leur qualité n'est pas acquise et sera un élément clé.

4.6. IA pour les infrastructures numériques et infrastructures numériques pour l'IA.

L'IA est largement utilisée dans la conception et l'exploitation des réseaux de télécommunication. Ce qui est également notable est qu'en général l'efficacité énergétique est un critère clé d'évaluation de la performance et pertinence de l'usage de l'IA. Des protocoles radio, par exemple, (comme l'estimation de canal, c'est-à-dire l'évaluation des conditions de propagation radio pour optimiser les paramètres d'envoi des paquets d'information) peuvent être basés sur l'IA, mais ils ne seront retenus que s'ils s'avèrent plus performants que les modèles actuels. Ceci est également valable pour les autres cas d'usage comme la maintenance prédictive ou l'optimisation du réseau.

Il est au moins aussi important de noter que l'usage de l'IA amènera de nouvelles contraintes sur les performances des réseaux. L'objectif de performances d'un réseau mobile est un objectif qui évolue avec le temps et le développement de nouveaux usages. Ce qui était optimal peut se révéler insuffisant après quelques années et l'introduction par exemple de nouveaux usages. Pour l'IA, les contraintes seront évidemment fortes sur le temps de latence, la fiabilité, la capacité et le débit si les données sont traitées dans le *cloud*. Les premiers usages IA laissent également penser que les besoins sur le canal ascendant (uplink) vont se développer largement.

Concrètement, l'IA pour les réseaux désigne l'usage d'algorithmes prédictifs et génératifs pour automatiser, optimiser et sécuriser les infrastructures de télécommunications sur l'ensemble de leur cycle de vie (conception, déploiement, exploitation, maintenance), tandis que les réseaux pour l'IA recouvrent l'ensemble des capacités de transport, de calcul et d'orchestration permettant d'exécuter l'IA au bon endroit du *continuum device-edge-cloud*.

4.6.1. Infrastructures numériques pour l'IA

Selon une étude publiée en décembre 2024 par « Digital Marketing PME.ch »[15], Amazon Web Services (AWS), Microsoft Azure, Nvidia, Intel et Qualcomm sont considérés comme les acteurs leaders spécialisés dans les infrastructures numériques pour l'IA. Dans d'autres

[15] Les principaux acteurs du marché de l'IA en 2024, Digital Marketing PME.ch, 27 décembre 2024.

études, comme celle de BDM[16], on peut aussi trouver Google Cloud parmi ces acteurs principaux.

a) Fournisseurs d'infrastructure cloud

AWS, MS Azure et Google Cloud offrent une large gamme de services *cloud* permettant l'hébergement, le traitement et la gestion des données et applications d'IA à grande échelle. Leur positionnement est stratégique, car ils fournissent l'infrastructure essentielle pour la majorité des acteurs de l'IA, facilitant l'intégration et le déploiement rapides des solutions. Ils jouent également un rôle dans la standardisation en proposant des plateformes compatibles avec diverses technologies et en participant à des initiatives de normalisation pour assurer l'interopérabilité.

b) Fabricants de matériel

Nvidia se distingue par ses processeurs graphiques puissants, optimisés pour l'apprentissage automatique et l'entraînement de modèles d'IA. Intel et Qualcomm investissent dans des technologies visant à améliorer la performance des systèmes d'IA. Les composants matériels qu'ils offrent permettent leur positionnement stratégique pour la fourniture d'infrastructure matérielle nécessaire pour exécuter des algorithmes complexes et traiter de grandes quantités de données. Leur contribution à la standardisation concerne le développement de composants matériels (*hardware*) compatibles avec les environnements d'exécution (*frameworks*) d'IA, favorisant une certaine uniformité dans l'écosystème.

c) Implication dans la standardisation

Ces acteurs participent à des consortiums et à des initiatives visant à établir des normes pour l'interopérabilité, la sécurité et la performance des infrastructures d'IA. La standardisation est essentielle pour assurer une compatibilité entre différents systèmes, réduire les coûts et favoriser une adoption plus large des technologies d'IA.

4.6.2. IA pour les infrastructures numériques

Quant aux acteurs fournissant des solutions d'intelligence artificielle (IA) pour les infrastructures numériques, on retrouve des entreprises technologiques majeures, des startups spécialisées, ainsi que des fournisseurs de services *cloud*.

a) Fournisseurs d'équipements de télécommunication

Parmi les acteurs principaux, on peut citer Nokia, qui utilise l'IA pour optimiser les réseaux de télécommunications, améliorer la gestion des infrastructures et offrir des solutions de sécurité avancées. Nokia est bien positionnée dans le domaine des télécommunications grâce à son expertise en réseaux et à sa contribution aux standards du secteur. Ericsson et Huawei sont d'autres exemples.

b) Fournisseurs d'équipements réseau

[16] Cartographie : quels sont les acteurs du marché de l'IA en 2024 ?, BDM, 9 avril 2024.

Un autre exemple d'acteurs est Cisco, qui intègre l'IA dans ses solutions de réseau pour améliorer la gestion et la sécurité des infrastructures. Cisco est un leader dans le domaine des équipements réseau et participe activement à la standardisation des technologies de réseau.

c) Fournisseurs de solutions logicielles spécialisées

IBM propose à son tour des solutions d'IA *via* sa plateforme Watson, qui est utilisée pour l'analyse de données et l'optimisation des infrastructures numériques. IBM est également impliqué dans la standardisation des technologies IA. Il est à noté que Mistral a signé un partenariat avec IBM/Watson.

d) Startups et entreprises spécialisées

De très nombreuses entreprises offrent aujourd'hui des solutions d'IA spécifiques pour, par exemple, l'automatisation des processus ou l'analyse prédictive. Ils apportent souvent des innovations et influencent les tendances du marché.

e) Fournisseurs de technologies cloud

On peut citer à nouveau les fournisseurs d'infrastructures *cloud*, comme de Google Cloud, AWS, et MS Azure qui proposent des services et solutions d'IA pour l'analyse de données et l'optimisation des infrastructures numériques. Ce sont des acteurs majeurs dans le domaine du *cloud* computing et contribuent à la standardisation des technologies IA. La filière française se développe, avec notamment les offres d'OVH Cloud, Scaleway, Dassault Outscale, Clever Cloud, Cloud Temple.

Ces entreprises participent souvent à des consortiums et des groupes de travail pour développer et promouvoir des standards ouverts dans le domaine de l'IA et des infrastructures numériques. Leur positionnement sur le marché est généralement lié à leur capacité à innover, à offrir des solutions évolutives et à collaborer avec d'autres acteurs pour établir des normes communes.

5. Les principales évolutions technologiques à considérer

Dans cette section nous revenons, avec plus de détails, sur les évolutions technologiques et architecturales des infrastructures numériques, réseau-*cloud*-IA.

Le processus de *softwarisation* et de virtualisation des réseaux de télécommunications, initié au début des années 2010, s'est fortement accéléré les cinq dernières années, notamment dans le cadre du déploiement de la 5G. On se trouve donc face à une convergence de plus en plus forte des technologies utilisées dans ces réseaux et de celles utilisées dans le *cloud*, les réseaux étant de plus en plus implémentés sur des infrastructures du type *cloud* et le *cloud* se disséminant en dehors des grands data centres, et en particulier à l'*edge* et sur le MEC (*Mobile Edge Computing).* En même temps, l'IA devient essentielle aux nouvelles architectures réseaux et les réseaux deviennent critiques pour soutenir les nouveaux besoins de l'IA, notamment sa distribution dans le cadre de l'IA fédérée.

Ces transformations ont un impact majeur sur le positionnement des acteurs et la constitution des filières ; ce qui se traduit par des opportunités et des risques, notamment en ce qui concerne la souveraineté des pays.

Dans cette section nous revenons sur :

- Les évolutions des architectures des infrastructures numériques, réseau-*cloud*-IA, et les types de convergences envisagées. Cela couvre notamment les aspects 3C (*Communicating Collaborative Computing*) et ceux liés à l'ouverture des infrastructures numériques[17].
- Les impacts potentiels sur le positionnement des acteurs existants et émergents et sur la constitution des filières, l'identification des opportunités et des risques, notamment en ce qui concerne la souveraineté de la France et de l'Europe.

Cela nous permettra, dans la section suivante, de présenter de manière consolidée les diverses recommandations figurant dans ce document, en faisant référence quand nécessaire aux aspects technologiques mieux détaillés ici.

5.1. Virtualisation des réseaux et *Telco Cloud*

Avec la virtualisation, et même la *cloudification* des fonctions réseaux, le secteur des télécommunications vit une transformation en profondeur qui, grâce à la désagrégation *hardware* et *software*, ouvre la porte au réseau intégralement programmable. Ce changement de paradigme repose sur un *cloud* performant, sécurisé et une conception des réseaux 100 % *cloud native,* que l'on désigne sous le terme *« Telco Cloud ».* On pourrait être tenté de définir le *Telco Cloud* comme l'utilisation d'architectures ou services *cloud* pour l'implémentation des réseaux. Mais ceci serait fortement réducteur vis-à-vis des enjeux actuels liés notamment aux diverses formes de convergence en cours, déjà présentées dans ce document, et aux choix stratégiques de positionnement des acteurs. La définition du *Telco Cloud* peut partir d'une

[17] Ce qui, dans les projections à moyen terme, dépasse largement le simple accès à des services.

architecture de réseaux qui utilise nativement les technologies du *cloud*, mais doit intégrer l'évolution vers ces convergences et ouvertures qui transforment le paysage industriel du secteur. C'est le seul moyen de bien considérer les opportunités et les risques qui découlent de ces évolutions, notamment ceux liés aux potentielles dépendances vis-à-vis de solutions « *cloud* clés en main » ou de briques technologiques constitutives de ces architectures non maîtrisées par les acteurs européens et/ou nationaux.

Il est nécessaire de garder le contrôle sur les architectures pour avoir toute la flexibilité que l'on souhaite (référence aux travaux communs Intel/Google qui vont dans le sens contraire, en définissant la couche HW/SW se trouvant en dessous de la virtualisation).

5.2. 3C Network (Connected Collaborative Computing) European initiative

Dans la continuité des travaux menés dans le cadre de l'IPCEI-CIS, et d'autres appels à projets européens comme le 6G SNS visant à soutenir les efforts des acteurs européens en vue de construire des solutions de *Telco Cloud* fiables, innovantes, et indépendantes, le **projet « 3C Networks »** (*Connected - Collaborative - Computing*), fait partie de l'initiative européenne « Horizon Europe » et constitue une étape clé dans la stratégie de passage à l'échelle. En effet, le projet « 3C Networks » est un projet de recherche et d'innovation, visant à tester des solutions techniques innovantes à petite échelle, sur quelques nœuds réseau existants. Ce pilote permettra de démontrer la faisabilité, d'évaluer l'efficacité, et d'affiner les cas d'usage prioritaires avec les clients et acteurs du marché. Il contribuera aussi à affiner la notion de souveraineté qui est encore à définir d'un point de vue réglementaire à l'échelle européenne[18].

Dans son document « Q&A: Connectivity package », la Commission européenne définit le concept 3C ainsi : *« The 3C Network is a future* ***ecosystem that spans over the entire computing continuum****, from semiconductors and radio technologies to connectivity infrastructure, data management, and applications »*. Ce *continuum* s'appuie notamment sur les diverses formes de convergence déjà mentionnées et sur le rôle de l'*edge* computing (dont le MEC). Le *continuum* couvre les usages et interactions technologiques avec les filières utilisatrices de 3C (énergie, mobilité, industrie…). Les enjeux sont multiples, de performance temps réel, d'adaptabilité et de scalabilité, d'interopérabilité, de sécurité et confiance (de bout en bout), d'impact environnemental (dont optimisation énergétique). Les verrous associés d'orchestration décentralisée, de gestion de la complexité algorithmique de qualité de service (QoS) dynamique des IN, de résilience aux défaillances et de modélisation formelle de la collaboration, pour ne citer que les plus étudiés à ce jour.

Pour tirer le plus grand profit de l'écosystème envisagé, une dimension clé est la capacité à réaliser dynamiquement une interconnexion sur mesure des espaces d'exécution distribués. L'approche habituelle des acteurs du *cloud* est de gérer la connectivité entre clusters en overlay (e.g. Nebula, Liqo, Cilium, Open SDN, …) ou par service mesh (Istio, Kuma, …), mais

[18] Large-scale pilots for supply end-to-end infrastructures integrating device, network computing and communication capabilities for Telco Edge Cloud deployments, as a basis for Connected Collaborative Computing Networks (3C networks) (RIA)

cela requiert la majeure partie du temps la connaissance d'adresses IP statiques et est peu compatible pour gérer la flexibilité et le dynamisme des ressources *edge*. Il est donc intéressant de rechercher des solutions qui intègrent la dimension réseau de manière plus fine de façon à former un *continuum* réseau-calcul (*« network-compute continuum »*) qui forme une abstraction à la fois des ressources de calcul distribuées mais aussi des différentes technologies et segments réseau les interconnectant, au sein et entre les espaces d'exécution. La gestion d'un tel *continuum* réseau-calcul se doit donc d'être particulièrement souple pour pouvoir déployer à la fois les fonctions réseaux (NF), des fonctions/charges applicatives et des fonctions/charges d'intelligence artificielle, tout en assurant leur possible migration durant le cycle de vie des services et au gré des déplacements des utilisateurs.

Ce *continuum* réseau-calcul extrêmement multiforme et distribué inclut trois dimensions différentes qui doivent être prises en compte au niveau de l'orchestration ([UNEXT_ECS] :

- Une dimension géographique bien sûr, qui idéalement ne va pas uniquement de l'*edge* au central *cloud*, mais pourrait aussi intégrer des ressources d'extrémités telles que les derniers points d'accès réseau ou même des équipements utilisateurs (UEs) à « l'extrême *edge* » ;
- Une dimension multi-acteurs induite par cette dimension géographique extrêmement étendue, puisque les ressources adressables du *continuum* peuvent naturellement être fournies par différents fournisseurs (réseau d'accès, réseau de transport, *cloud* provider, entreprises, voire des particuliers dans le cas extrême *edge*) ;
- Et enfin, une dimension technologique pour prendre en compte la très grande hétérogénéité des ressources *hardware* et *software* (CPUs, GPUs, …)

Les enjeux et cas d'usage résultant de la convergence réseau-capacité de calcul dans ce nouveau *continuum* sont multiples :

- Dans un premier temps, il permet de répondre à la problématique actuelle de « silotisation » du *cloud* en permettant une approche multi-cloud plus dynamique où l'orchestration du *continuum* réseau-calcul va permettre d'exposer, de négocier et de connecter sans couture des ressources de *clouds* privés et publics répondant en particulier à la dimension multi-acteurs précédente, et d'automatiser le déploiement ou redéploiement des charges en fonction de critères choisis par le client (performance en terme de qualité de service, d'empreinte énergétique, de « *privacy* », etc.) ;
- L'intégration de l'extrême *edge* ou des terminaux (UEs) dans ce *continuum* permet aussi d'envisager à la fois les cas d'usage de décharge (« *offloading* ») des UEs sur des ressources *edge* du *continuum* (que ce soit pour des critères d'économie de batterie pour l'UE ou de performance pure sur UE contraint, e.g. application AR/XR gourmande ou exécution d'une charge IA), ou inversement de sous-traitance de l'exécution d'une charge applicative sur l'UE, de manière à utiliser de manière opportuniste toutes les ressources de *compute* qui peuvent être à proximité d'un utilisateur ; cette exposition et utilisation de ressources de *compute* à l'extrême *edge* permet aussi de faire émerger des solutions très innovantes et participatives potentiellement bas coûts [Akash] tout en soulevant des problématiques techniques intéressantes pour prendre en compte leur hétérogénéité et leur volatilité ;

- L'inclusion de *compute* de tout type, y compris pour de l'accélération matérielle, dans le *continuum* réseau-calcul permettrait aussi non seulement d'intégrer de manière plus profonde l'intelligence artificielle partout dans le réseau y compris dans le RAN, que ce soit pour le RAN ou pour faire tourner des charges d'AI de manière plus distribuée [Nvidia]. Cela pourrait aussi faire apparaître une nouvelle source de revenu pour les opérateurs en exposant leurs propres ressources de compute lorsqu'elles sont sous-utilisées pour y exécuter des charges d'acteurs tiers ;
- Ainsi, différents niveaux d'exposition et d'intégration entres les deux types de ressources peuvent envisagés, que ce soit par l'utilisation d'APIs où le réseau et/ou le *cloud* exposent leurs caractéristiques à l'acteur en charge de l'orchestration (opérateur, *cloud provider* ou tiers), ou bien même par la diversification d'un opérateur incluant lui-même des ressources de compute pour offrir des services à valeur ajoutée intégrant finement du compute dédié au son offre réseau pour de la performance [NTT].

L'intégration des ressources réseau et compute et leur orchestration conjointes prenant en compte les diversités géographiques, technologiques et d'acteurs ouvrent une perspective particulièrement riche. Pour prendre en compte toutes ces différences et pouvoir envisager un passage à l'échelle, une approche mêlant de plus en plus des mécanismes de décentralisation et de gestion autonomique est probablement nécessaire |UNEXT]

Références :

- Extended compute services for a unified networking experience
- Five Takeaways from NVIDIA 6G Developer Day 2024
- Navigating the Akash Network: Unraveling How It Works
- Inclusive Core: Integrative and Cooperative Network Architecture for the 6G/IOWN Era (white paper)
- UNEXT – A unified networking experience

5.3. Edge Computing et Mobile / Multi-access Edge Computing

Les nouveaux usages, avec des contraintes fortes en termes de performances, de résilience et parfois de latence, par exemple liées au traitement de données dans des applications de mobilité (véhicule autonome…) ou de processus industriel (souvent avec des interactions avec des algorithmes d'IA), poussent au développement de solutions d'*edge* computing/MEC. Évidemment des questions demeurent encore sur l'architecture associée et plus spécifiquement sur la granularité de la couche d'*edge* computing (densité de déploiement des solutions d'*edge* computing)

Les enjeux et verrous se rapprochent de ceux du thème précédent mais dans un scénario où la possible confrontation entre acteurs télécoms et *cloud* est directe et où des solutions et modèles économiques permettant de débloquer les opportunités de création de valeur jointe sont nécessaires. On y retrouve les enjeux de la réduction de la latence, l'allégement du réseau central, la confidentialité locale, la scalabilité / performance, le support de la mobilité (MEC), les services xG temps réel (MEC), la résilience locale des équipements à la périphérie et les verrous technologiques d'orchestration distribuée, de prise en compte de l'hétérogénéité des équipements, de la cybersécurité des équipements Sécurité à la périphérie, de support à la

protection des données en limitant leur dissémination, de capacité de déploiement et de maintenance, l'impact des procédures mobiles (*handover* et continuité de service inter opérateurs), le couplage complexe avec les architectures NFV/SDN déployées. Il ne faut pas non plus négliger les impacts des modèles d'affaires (surcoût de déploiements dispersés, qui paye quoi, qui est responsable de quoi…). Il est important d'identifier quel est le facteur qui va induire l'avantage de la distribution : la protection des données ? les performances ? l'impact environnemental ? Cela dépend du cas d'usage. Par ailleurs les demandes des clients varient.

5.4. Open Networks

Les Open Networks désignent l'ensemble des architectures réseau qui reposent sur des interfaces ouvertes, des standards publics, des composants désagrégés et programmables, souvent basés sur : SDN (Software Defined Networking), NFV (Network Function Virtualization), Open RAN, Open Optical Networking, Open Core / Open Packet Core, Open APIs / Service orchestration. Le tout est souvent piloté par des initiatives comme l'O-RAN Alliance, ONF (Open Networking Foundation), TIP (Telecoms Infra Project), Linux Foundation, etc. Les Open Networks ne sont pas une technologie en soi, mais un principe transversal.

Ils se placent souvent mais pas toujours dans la logique *cloud native*, agile, souveraine et automatisée. Les enjeux des Open Networks sont liés à l'interopérabilité (multi fournisseurs), l'agilité et l'innovation dans la programmation réseaux (nouveaux services), une réduction des coûts, la contribution à une souveraineté numérique (réduction de la dépendance aux équipementiers, nouveaux entrants. Les verrous ne sont pas négligeables : la complexité de l'intégration, l'interopérabilité est parfois incomplète avec une maturité inégale des composants, la Sécurité (augmentation de la surface d'attaque), la Gouvernance des briques *open source* et le modèle économique et le besoin de nouvelles compétences dans les organisations.

Les réseaux ouverts sont fondés sur des interfaces standardisées, la désagrégation, des APIs programmables et des socles *open source* robustes, afin d'accélérer l'innovation, réduire le verrouillage fournisseur et renforcer la résilience industrielle européenne. Parmi l'écosystème des télécommunications, Orange s'appuie sur un écosystème piloté par la Linux Foundation (Sylva pour le *Telco Cloud* cloud-native, CAMARA/Open Gateway pour l'exposition sécurisée de capacités réseau, Nephio/Anuket pour l'automatisation et les référentiels).

5.5. Open RAN

La notion d'Open RAN, voire sa dénomination, est en train d'évoluer. On parle peut-être un peu moins d'Open RAN tout en projetant une évolution des réseaux (vers la 6G) s'appuyant sur les principes associés à l'Open RAN, comme la virtualisation, l'ouverture des interfaces, la *cloudification* et l'automatisation.

Open RAN est une architecture de réseau d'accès radio mobile qui vise à ouvrir et désagréger les éléments traditionnellement fermés et propriétaires des réseaux RAN (Radio Access Network). Elle repose sur trois piliers : désagrégation des fonctions RAN (CU, DU, RU), interfaces ouvertes (standardisées par l'O-RAN Alliance), virtualisation / *cloudification* des

fonctions RAN (vRAN). Elle a pour objectif de conduire à une innovation accélérée. Ces architectures ouvertes permettent donc d'associer des solutions d'équipementiers différents. Néanmoins dans certaines configurations, l'opérateur peut s'appuyer plus fortement sur un équipementier et voir cette architecture ouverte comme une forme d'assurance si son équipementier de référence lui faisant défaut sur certaines configurations.

Elle présente cependant des enjeux liés à l'interopérabilité multi-vendeurs (intégration complexe, manque de standardisation concrète), les coûts et l'ouverture des marchés à de nouveaux entrants, le risque d'immaturité des solutions et de performance inférieure aux RAN propriétaires (Latence, synchronisation, QoS difficiles à garantir), des défis de sécurité rehaussée du fait de l'ouverture du code mais aussi le besoin en nouvelles compétences tech et devops chez les opérateurs notamment.

Les enjeux de performances de bout en bout sont cruciaux, et il est souvent attendu qu'un acteur puisse prendre ces engagements, et avoir une vue globale d'une solution en partie hétérogène en termes d'équipementiers.

Ces nouvelles architectures doivent aussi permettre d'optimiser les coûts tout en facilitant et accélérant les cycles d'innovation. Elles peuvent répondre à un enjeu de souveraineté numérique par une moindre dépendance vis-à-vis de fournisseurs traditionnels.

5.6. Services de cybersécurité

La sécurité est un sujet clé. Il ne s'agit pas uniquement de la sécurisation des infrastructures numériques mais également de l'offre par ces dernières de services de sécurité évolués. Les évolutions mentionnées ouvrent de très nombreux nouveaux défis de sécurité qui requièrent notamment des solutions distribuées (bien au-delà des concepts type parafeux), intelligentes, automatisées et autoconfigurées. Ce sujet s'accentue avec l'avènement des nouveaux paradigmes, tels que l'IA agentique, nécessitant de nouvelles approches pour le contrôle d'accès[19] (voir notamment le positionnement de CyberArk, racheté en 2026 par Paolo Alto)[20]. Nous avons en France des acteurs dans le domaine des services de sécurité et également sur les autres domaines à traiter ; il est nécessaire de mettre en place un lien, via une fédération ou d'autres approches, pour devenir compétitifs au niveau global. Des clients peuvent préférer des solutions venant d'ailleurs pour se protéger en cas de problème parce que considérées comme plus sûres au sens large, choix qui leur donne une « couverture » en cas de problème, par rapport au cas où ils auraient choisi un acteur plus petit ou plus local. La création d'un acteur type NIST pour valider les performances de solutions locales pourrait devenir un facteur déterminant de succès pour des acteurs nationaux.

[19] Voir par exemple les concepts introduits dans la section « *Cloud* (IaaS, PaaS, SaaS ; *data centers – edge*, centres de colocalisation) »

[20] CyberARK est une société israélienne leader des fonctionnalités de PAM (Privileged Access Management= gestion des accès à privilèges). CyberArk évolue vers une approche plus large de type plateforme (Identity Security Platform) qui intègre l'IAM (gestion des identités), les fonctions PAM, la gestion des secrets et globalement la sécurité machine-to-machine

Au-delà d'un acteur de type NIST européen pour la validation des solutions de cybersécurité. Et, bien que des fournisseurs de services de sécurité européens existent, les logiciels sur lesquels leurs infrastructures de gestion de la sécurité se reposent (i.e. IAM, EDR, NDR, XDR, MDR, SIEM, SOAR et les OS sous-jacent permettant l'administration des plateformes etc.) sont souvent développés par des sociétés nord-américaines ou depuis l'Amérique du Nord). Pour des questions de souveraineté technologique européennes, il serait souhaitable de favoriser des solutions logicielles développées et maintenues par des entreprises européennes, sur le territoire Européen, au lieu de se reposer sur des éditeurs logiciels ou des capacités de développement nord-américains (e.g. CrowdStrike, GAFAM etc.). De même, la sécurité de la chaîne d'approvisionnement aussi bien matérielle que logicielle pour les plateformes de services de sécurité gérées est critique. Cela nécessiterait probablement un contrôle plus strict, ainsi que l'anticipation sur des solutions en cas de compromission.

Avec le développement rapide des approches d'apprentissage (i.e. *Machine Learning, ML*), d'intelligence artificielle (i.e. *Artificial Intelligence, AI*), en particulier les modèles génératifs (i.e. *Large Language Model, LLM*), ainsi que les capacités d'entraînement autant locales que déportées en nuage, de nouvelles opportunités d'amélioration les services de cybersécurité autant que de nouvelles menaces émergent. Les modèles génératifs pourraient par exemple aider les experts sécurité dans la synthèse des informations provenant de la veille sur les menaces ainsi, qu'au traitement des sources de données permettant la détection des attaques (e.g. flux réseaux, traces systèmes, comportement utilisateurs, etc.) afin de faire des recommandations ciblées de remédiations plus pertinentes et rapide. Néanmoins, des questions se posent autant sur leur résilience vis-à-vis des attaques adverses (i.e. *Adversarial Attacks*) contre les modèles, en particulier dans leur phase d'entraînement, ainsi que sur la sécurité de leur exécution déportée, la traçabilité, la maîtrise des données d'entraînement, l'explicabilité et la confiance dans les résultats produits. Il serait ainsi important de développer les capacités de recherche sur les algorithmes d'apprentissage et de l'intelligence artificielle dans ces différentes directions (i.e. sécurité, traçabilité, protection des données d'entraînement, confiance et explicabilité). Un renforcement ou de nouveaux moyens d'améliorer la collaboration entre acteurs académiques de la recherche et entreprises de pointe européennes est probablement souhaitable dans ce domaine. De plus, des capacités d'exécution des algorithmes d'apprentissage et d'intelligence artificielle, maitrisées par des acteurs européens seraient aussi une garantie de souveraineté pour l'utilisation de ces approches dans des secteurs critiques (e.g. défense, télécommunications, énergie, bancaire, étatique etc.).

La Convergence *cloud*-réseau : une surface d'attaque étendue

La 6G consacre la *« softwarisation »* intégrale, la 5G était déjà voulue comme *« cloud native »*, les fonctions réseau ne sont plus uniquement des matériels physiques mais des micro-services virtualisés distribués spatialement et dynamiquement de bout-en-bout.

Il s'agit donc de considérer la Sécurité tout au long du cycle de vie des logiciels, la virtualisation et le code devenant aussi critique que le matériel. Les défis spécifiques résidant dans la gestion des mises à jour et de la traçabilité de la chaîne d'approvisionnement dans un environnement multi-acteurs.

La 6G n'est pas seulement convergente dans la réutilisation de technologies logicielles, elle doit intégrer des capacités de calcul distribué qui amènent aussi une surface d'attaque spécifique, héritée du *cloud* historique centralisé, mais augmentée par la nature distribuée. Cela impacte significativement les phases de détection et réponse lorsque des attaques surviennent nécessitant coordination et coopération entre différents segments/parties.

Les IA : sécuriser leurs usages, les utiliser pour la sécurité

L'infrastructure convergée est le socle de déploiement de l'IA et intersecte largement l'état de l'art en matière de sécurité d'IA. Il faut distinguer ce que l'infrastructure permet à des applications tierces et les usages propres pour une 6G dite « AI-native ». Une partie commune pour les aspects d'apprentissage sera la maîtrise des cycles de vie des données depuis leur collection, stockage, maintenance d'un niveau de qualité, traçabilité, conformité à la régulation… Autres aspects communs les orientations liées au paradigme « zero trust » et sécurité centrée sur la donnée (DCS) qui conviendra de projeter au sein des architectures 6G.

Un pan prometteur se fait jour au-delà de l'IA statistique (ou hybride) en la matière de l'IA agentique. Les opérations de sécurité d'une infrastructure convergée, très souvent biaisée par des approches historiques (*cloud* ou réseau) peuvent trouver une cohérence et interopérabilité grâce à l'IA agentique. Une approche multi-agent pouvant typiquement faciliter les interactions dans une approche fédérée et appliquer des politiques « intelligente » pour assurer sécurité et résilience. Un danger majeur ici serait de laisser des acteurs puissants imposer leurs politiques avec la réintroduction d'une couche chapeau elle-même propriétaire.

Standards et régulations

La sécurité est traditionnellement marquée par une démarche d'évaluation, la complexité des systèmes et services, la dynamique temporelle impose de revisiter l'état de l'art. Les enjeux sont ici stratégiques pour différencier les solutions méritantes au sens du respect de la souveraineté et l'information légitime dont devraient bénéficier les utilisateurs.

5.7. Accès aux services offerts par les Infrastructures numériques (IN)

Il est nécessaire de garder le contrôle sur les formes d'accès aux services, même dans les contextes des architectures multi-acteurs qui se dessinent. Il faut garder le contrôle sur le « guichet d'accès », autrement dit sur le client final (en référence aux approches Amazon vis-à-vis des fournisseurs d'applications). Ceci est notamment important pour permettre aux petits acteurs de se positionner. La question est centrale à l'approche PaaS présentée dans l'Annexe I. Amazon vend de la 5G privé, mais comme une boîte noire, sans possibilité de savoir ce qui y est intégré.

Le fait de travailler sur des infrastructures en utilisant des APIs réseaux standardisées et ouvertes associées à un système permettant de garantir la sécurité, l'identification, la chaîne de responsabilité et la non-cannibalisation des infrastructures numériques est un élément clé de pérennité des infrastructures numériques.

5.7.1. Fédérations des acteurs

Ce n'est pas la même chose d'ouvrir un réseau par des APIs que de se positionner au centre du paysage en articulant le reste. Il faut essayer de maîtriser la chaîne, par exemple en mettant en place les fédérations pertinentes et intégrer les autres acteurs selon nos règles.

À titre d'exemple, concernant les travaux 3C Networks (Connected Collaborative Computing), il ne semble pas possible que les opérateurs de télécommunications puissent avancer seuls dans cette direction. Il faut pouvoir fédérer les acteurs, notamment du *cloud*. Il faut un « endroit » et des acteurs pour ce faire.

Il faut valoriser la composante réseau, sans laquelle le numérique n'existe pas. Un service ça se paye, ça se monitore, il offre une qualité d'expérience et de service. Ceci est rendu possible quand le service est offert en local. Mais il faut pouvoir exposer la différence entre cela et le Best Effort fourni au bout du monde et aujourd'hui on n'a pas les outils. Cela inclut la sécurité.

Il manque un stratum qui permette, sur une diversité de fournisseurs d'infra réseau/*cloud*/services, de donner une vision intégrée de bout en bout vis-à-vis des clients finaux. Ce stratum pouvant être mis en place par une fédération d'acteurs qui ont décidé de s'allier. La stabilité de ces alliances représente un élément clé, qui dépend de modèles économiques à concevoir. Ce stratum doit fournir la visibilité en termes de qualité de service, de robustesse, de résilience, etc. mentionnés dans le précédent paragraphe.

5.7.2. Logiciel libre et gouvernance associée

Les évolutions des réseaux vers l'utilisation de logiciels libres (*open source*) bénéficient des principes et outils de gouvernance mis en place au cours du temps par les acteurs de l'informatique et du développement logiciel et notamment *via* la Linux Foundation.

La Linux Foundation est une organisation à but non lucratif qui vise à soutenir le développement collaboratif de logiciels libres et ouverts, en particulier autour de l'écosystème Linux et des technologies critiques pour l'industrie numérique. Ses principaux objectifs sont :

- Favoriser l'innovation ouverte en fournissant une gouvernance neutre et un cadre juridique clair pour le développement collaboratif.
- Accélérer la standardisation et l'adoption de technologies interopérables, en évitant la fragmentation.
- Offrir des ressources communes (infrastructures de test, outils, formations) pour mutualiser les coûts de R&D et faciliter l'industrialisation des solutions *open source*.
- Fédérer les acteurs industriels et académiques afin de constituer des écosystèmes internationaux autour de projets stratégiques (réseaux, *cloud*, *edge*, IA, cybersécurité, etc.).

Dans les télécommunications, la Linux Foundation joue un rôle central à travers des initiatives comme LF Networking (LFN) et LF Edge :

- Virtualisation et *cloudification* des réseaux : soutien aux projets de NFV (*Network Functions Virtualization*) et SDN (*Software Defined Networking*), avec des plateformes comme ONAP (*Open Network Automation Platform*) et OpenDaylight, permettant l'automatisation et la programmabilité des réseaux

- Interopérabilité et standardisation : création de cadres ouverts favorisant la compatibilité entre équipements multi-constructeurs et opérateurs, réduisant la dépendance aux solutions propriétaires.
- *Edge* et 5G/6G : contributions majeures à l'architecture distribuée des réseaux, *via* des projets *open source* pour le *Multi-access Edge Computing* (MEC), le *slicing* 5G et l'orchestration *cloud native*.
- Écosystème collaboratif : mise en relation des opérateurs de télécommunications, fournisseurs de technologies, start-ups et organismes de recherche pour codévelopper les briques logicielles qui structurent les futures générations de réseaux.

En résumé, la Linux Foundation qui apporte une infrastructure collaborative, ouverte et neutre doit permettre à l'industrie des télécommunications de construire des réseaux plus souples, interopérables et innovants, adaptés aux besoins du *cloud*, de la 5G/6G et de l'*edge* computing.

Il faut néanmoins rappeler que

- La Linux Foundation est une organisation américaine de droit du Delaware (501(c)(6)), à but non lucratif mais gérée comme une entreprise classique, dont le financement provient majoritairement de membres américains et asiatiques.
- La création en 2022 de « Linux Foundation Europe » (où Sylva est hébergé) est précisément une réponse à cette critique de souveraineté. Mais il s'agit d'une filiale, dont le contrôle stratégique, juridique et financier reste à Linux Foundation US. Héberger un projet européen dans une filiale d'une fondation américaine n'est pas équivalent à exercer une souveraineté européenne sur sa gouvernance.
- Plusieurs des projets cités dans ce document (Nephio, ONAP, OpenDaylight…) sont pilotés ou co-pilotés par des entreprises américaines (Google Cloud pour Nephio, AT&T pour ONAP à l'origine, etc.).

5.7.3. *Open source* et souveraineté

L'*open source* est ainsi un élément clé pour avancer vers une souveraineté numérique, mais comme évoqué dans d'autres sections de ce document, la stratégie *open source* doit être placée dans un cadre bien plus large.

Plusieurs travaux européens récents proposent précisément une telle approche, en intégrant l'*open source* comme l'un des critères fondamentaux de la souveraineté logicielle, sans le confondre avec elle :

- Le projet de critères LOTEC (Legal, Operational, Technological, Economic, Cultural Sovereignty)[21] publié en 2024 dans le cadre de l'EuroStack Directory Project, définit cinq piliers complémentaires de la souveraineté numérique. L'*open source* y figure à plusieurs niveaux — licences ouvertes (pilier juridique), code auditable et standards ouverts (pilier technologique), réversibilité et portabilité (pilier opérationnel) — mais

[21] S. Fermigier, Drafting European Sovereignty Criteria for Software and Digital Systems, EuroStack Directory Project, 12 septembre 2024.

toujours articulé avec d'autres critères : résidence des données, contrôle juridictionnel, propriété intellectuelle sous juridiction européenne, indépendance de la chaîne d'approvisionnement, etc.

- Le livre blanc *« Deploying the EuroStack: What's Needed Now »* (mai 2025)[22], co-signé par une vingtaine de contributeurs représentatifs de l'industrie européenne, organise sa stratégie autour de trois axes — *« Buy European »*, *« Sell European »*, *« Fund European »* — où l'*open source* est traité comme un levier transverse de visibilité, d'interopérabilité et de rupture des verrous propriétaires.
- Le document *« A Proposed Framework for a 'Buy European' Regulation of Strategic Digital Procurement »* (septembre 2025)[23] propose un cadre opérationnel pour la commande publique stratégique. Il définit un *« Sovereign European Provider »* selon le *framework* JOTED (Jurisdictional, Operational, Technical, Economic et Data Sovereignty), cinq dimensions hiérarchisées : Juridiction & Gouvernance comme prérequis pass/fail, Souverainetés Technique, Opérationnelle et des Données comme garanties cœur, Souveraineté Économique comme différenciateur. L'usage prédominant de logiciels libres (sous licence approuvée par l'OSI) y figure explicitement comme critère technique (Criterion 2.1), aux côtés de la transparence architecturale et de la réversibilité opérationnelle. L'assise juridique repose sur l'exception *« essential security interests »* de l'AMP de l'OMC (Article III) et l'Article 346 TFUE — ce qui rend ce dispositif compatible avec le droit international en vigueur.

5.8. IA pour les réseaux, les réseaux pour l'IA

La complexité croissante des réseaux, avec l'introduction d'une grande diversité de nouvelles technologies et paradigmes de communication, avec la flexibilité introduite par la *softwarisation*, la virtualisation et le placement dynamique des fonctionnalités, avec l'ouverture des réseaux sur diverses formes, avec la convergence progressive réseau-*cloud* et avec l'avènement de services multisectoriels, impose l'utilisation de l'IA à divers niveaux. Côté technologique, nous pouvons citer à titre d'exemple certaines évolutions du RAN : nouveaux systèmes antennaires et RIS, réseaux sans cellules, la convergence communications-sensing...). L'utilisation de l'IA concerne toute la chaîne : la conception, la planification, le déploiement et l'exploitation des réseaux. Il faut également prendre en compte l'utilisation de jumeaux numériques alimentés par de l'IA.

Cette importance croissante de l'utilisation de l'IA soulève des questions sur le positionnement des acteurs dans cet environnement en mutation, sur la régulation, sur les certifications qui seront requises pour que les mécanismes d'IA puissent être intégrés dans les infrastructures de réseaux.

[22] EuroStack Industry Initiative, Deploying the EuroStack: What's Needed Now, version du 19 mai 2025

[23] EuroStack Industry Initiative, A Proposed Framework for a "Buy European" Regulation of Strategic Digital Procurement, 29 septembre 2025

Dans le RAN, l'introduction de GPUs et autres accélérateurs matériels disponibles crée une opportunité d'améliorer l'efficacité du RAN et de créer de nouveaux services grâce à l'IA. L'AI-RAN Alliance étudie les questions d'intégration d'infrastructures, de partage de ressources et de la sécurité des données dans ce cadre. D'éventuels changements d'architecture pourraient potentiellement rebattre les cartes entre les différents acteurs.

Parallèlement, l'IA devient de plus en plus distribuée, notamment avec l'essor de l'IA fédérative et pour des raisons de protection des données. La question de l'efficacité énergétique doit également être considérée, l'intérêt de ce point de vue de l'*edge* dépendant des cas d'usage. Cette décentralisation sur l'ensemble des infrastructures, sortant des grands *data centers*, crée de nouvelles opportunités, notamment grâce au MEC, et génère aussi des risques significatifs. Le débat portera sur les opportunités pour les opérateurs en tant qu'acteurs de confiance, tout en abordant des thèmes transversaux comme la souveraineté, la sécurité, la protection des données, le numérique responsable et les compétences nécessaires à chaque étape de la chaîne.

Les systèmes multi-agents connaissent un second souffle dans le cadre de l'IA basée sur des agents équipés de grands modèles de langage (LLM) - « Agentic AI » comme moteur de raisonnement central. Ces agents possèdent souvent une mémoire, un ensemble d'outils et peuvent interagir de manière programmatique, transformant ainsi les LLM de prédicteurs de texte en composants logiciels fonctionnels. Pour collaborer et se connecter aux données et outils utilisés par les agents, de nombreux frameworks logiciels et protocoles comme MCP ou A2A ont récemment émergé. Les architectures logicielles, notamment de gestion de réseaux, doivent maintenant évoluer pour profiter de ces évolutions. Le développement de modèles embarqués et souverains est également souhaitable pour limiter la dépendance aux hyperscalers.

5.8.1. Questions clés IA et réseaux

L'IA est intéressante, pertinente, et même nécessaire pour les réseaux, dans toutes les phases, de la conception jusqu'à l'opération (voir la section suivante). Elle est développée par les opérateurs eux-mêmes, mais également par divers autres acteurs. Elle est portée par les infrastructures des opérateurs, mais également par celles de divers autres acteurs, notamment dans un cadre de passage à l'échelle.

- Quel usage de l'IA pour les réseaux ?
- Quelle IA est utilisée et quel niveau de maîtrise les opérateurs ont-ils sur cette IA ?
    - Qui conçoit et développe les algorithmes d'IA déployés dans les réseaux ?
- Positionnement sur l'utilisation des IA génériques, de solutions spécifiques ou les deux ?
- Quelles infrastructures supporteront cette IA ?
    - Les opérateurs déploieront-ils leurs propres infrastructures ou utiliseront-ils celles de tiers ?
    - Comment l'IA sera-t-elle distribuée sur les infrastructures ?
    - Notamment dans un cadre de placement dynamique des fonctions, même inter- acteurs, et d'échanges de données.
- Quelle prise en compte des aspects énergétiques ?
- Les jumeaux numériques seront-ils utilisés pour consolider et faciliter l'opération ?

5.8.2. Défis associés à l'IA et éléments de réponses aux questions clés

L'IA est utilisée pour la conception, la planification et l'opération des réseaux ; nous citons ici quelques exemples : l'automatisation (citée très souvent en premier dans les enquêtes sur le sujet), l'évaluation de la qualité de service offerte (*service assurance*), la gestion plus efficace des inventaires, la maintenance prédictive, l'exploitation efficace des technologies avancées (e.g. nouvelles technologies radio), l'augmentation de résilience. Dans l'opération, elle permet d'automatiser la gestion du spectre, l'optimisation des ressources (y compris énergétiques) face à un trafic de plus en plus dynamique et hétérogène, le placement dynamique des fonctions, ainsi que la compréhension en temps réel de la qualité d'expérience et de service et la détection des sources des problèmes. L'IA permet aussi de réagir instantanément et d'assurer une allocation flexible et optimale des ressources disponibles y compris énergétiques. Enfin, elle facilite la maintenance, en particulier la maintenance prédictive. Cette liste sera bien sûr à compléter dans le rapport.

Le principal défi des opérateurs, quel que soit leur niveau d'avancement, est d'automatiser la configuration et l'exploitation des réseaux. En permettant de traiter davantage de données et de prendre en charge des tâches répétitives auparavant scriptées manuellement, l'IA répond à la complexité croissante et aux besoins d'efficacité.

Après 2-3 ans de POC dispersés, bien que le processus soit encore en réflexion, les opérateurs ont l'objectif de consolider tout cela pour passer à l'échelle.

Lors de la conception d'un réseau chez un opérateur, des documents de référence sont rédigés pour configurer le réseau. Actuellement, des initiatives explorent comment l'IA pourrait aider à rédiger ces documents. Cela n'implique pas une automatisation complète, mais l'IA pourrait générer un premier brouillon, que les ingénieurs et architectes de réseau pourraient ensuite ajuster. Cela permettrait de gagner du temps, en particulier dans un contexte où les cycles de conception sont devenus plus courts, passant d'une planification annuelle à un flux continu, en raison de la *softwarisation* des réseaux. Les grands modèles de langage et l'IA générative peuvent être utilisés pour faciliter la recherche d'information sur l'état, les fonctions et les modalités de configuration du réseau, sur le diagnostic de dégradation, de manière plus efficace qu'une recherche manuelle dans une documentation.

Par ailleurs, l'IA c'est aussi beaucoup de travaux sur l'amélioration de la qualité de service, à commencer par le *« root cause analysis »* : l'IA va permettre d'ingérer beaucoup de données, voire détecter des signaux faibles pour anticiper un futur dysfonctionnement ou une baisse de performance de telle entité du réseau. Et donc, c'est un peu comme une base de connaissances qu'on alimente au fil du temps et qui va permettre non seulement d'anticiper ou même de comprendre plus rapidement la cause du problème.

L'impact de l'IA sur les réseaux soulève de nombreuses questions chez les opérateurs. Leur métier consiste à gérer et anticiper le volume et la typologie du trafic, qu'ils connaissent bien, notamment celui des GAFAM. Cependant, avec l'essor de l'IA et la transition vers des modèles plus distribués, ils s'interrogent sur la croissance et la localisation de ce nouveau type de trafic. Ces incertitudes compliquent la planification des investissements en infrastructures, un processus long qu'ils cherchent à anticiper malgré le manque de visibilité actuelle.

Dans l'exploitation des réseaux, les solutions OSS fournies par des éditeurs de logiciels, sont des outils permettant de configurer et gérer les réseaux et qui intègrent souvent des

technologies d'IA, appliquées à différents secteurs et sous-ensembles. Il existe de nombreuses solutions IA, souvent *open source*, qui reposent sur des frameworks personnalisables, permettant d'adapter les modèles aux besoins spécifiques de chaque opérateur.

On évoque également le concept de « service assurance », qui consiste en un suivi systématique de la performance des services au sein des réseaux. L'IA permet d'analyser rapidement des volumes de données bien plus importants que ce qu'un humain pourrait faire, et ce, dans des délais beaucoup plus courts.

La question de l'hébergement est liée à celle de la souveraineté, ainsi qu'à la manière d'entraîner les modèles. Les modèles publics, souvent proposés par les hyperscalers, sont généralement généralistes, car entraînés sur une diversité de cas d'usage qui ne reflètent pas nécessairement les besoins spécifiques des opérateurs de télécommunications. Actuellement, on observe une tendance à privilégier des modèles de plus en plus spécialisés pour répondre à ces exigences particulières.

Pour des cas relativement simples, les opérateurs peuvent se contenter de solutions généralistes comme ChatGPT ou d'autres outils similaires. En revanche, pour des besoins plus spécifiques (optimisation des infrastructures dans un cadre d'intégration de nouvelles technologies radio, déploiement d'architectures d'IA agentique pour la mise en place automatique des services requérant une orchestration entre divers acteurs, etc.), ils privilégient des modèles d'IA spécialisés, qu'ils déploient sur leur propre infrastructure ou sur une partition de *cloud* public dédiée exclusivement à leur usage. Les opérateurs de télécommunications (Orange, Vodafone, AT&T, Deutsche Telekom, etc.) ont massivement intégré l'IA dans leurs feuilles de route réseau, avec des usages désormais assez convergents. Ils utilisent l'IA pour de l'exploitation quotidienne et visent l'automatisation complète des réseaux (vision "autonomous networks") :

- Supervision intelligente et détection d'anomalies pour remplacer les systèmes de monitoring classiques par des systèmes prédictifs incluant maintenance prédictive pour anticiper les défaillances avant qu'elles ne surviennent, automatisation des opérations (AIOps) pour réduire voire supprimer l'intervention humaine.
- Optimisation des réseaux telle que l'optimisation radio (RAN intelligent) en temps réel de la performance du réseau mobile ou la gestion dynamique du trafic et du cœur de réseau pour allouer les ressources réseau de façon optimale,
- Amélioration de l'expérience client (QoE) pour passer d'indicateurs techniques (QoS) à l'expérience réelle utilisateur.
- Sécurité réseau (AI for security) pour faire face à des menaces de plus en plus complexes.
- Efficacité énergétique (Green AI for networks) pour réduire la consommation énergétique des réseaux

Les opérateurs convergent vers un objectif commun : les réseaux autonomes. Actuellement les réseaux sont partiellement autonomes (L2) avec des décisions assistées par l'IA (L3) l'objectif affiché est une autonomie élevée d'ici 2030 (L4).

Cela implique que la solution optimale consiste à conteneuriser et entraîner les modèles pour des usages particuliers.

Par exemple Ericsson intègre de l'IA dans ses technologies et disposent d'un portefeuille de solutions couvrant la transmission radio, le cœur de réseau aussi bien pour le fixe que pour le mobile, et essaie de développer et d'entraîner des solutions d'IA spécifiques à chaque ligne de produits. Afin que le modèle fournisse des réponses précises, il doit être adapté à l'environnement de la radio, en opposition à d'autres éléments du réseau qui présentent des problématiques différentes.

Le choix entre infrastructures propres ou externalisées se fera au cas par cas, vu que l'exploitation des réseaux soulève rapidement des problématiques de souveraineté : les directions de sécurité des opérateurs sont fortement opposées à l'idée de confier ces opérations à l'extérieur de leur infrastructure, où elles pourraient être gérées par des entités externes à leur environnement et à leur organisation. Et à côté de ça, se pose la question du fait que, quand il faudra passer à l'échelle, il faut voir si on a les compétences qui ont les GAFAM.

Les GAFAM cherchent à développer leurs activités en se rapprochant des opérateurs pour les inciter à migrer leurs workloads vers des infrastructures *cloud*. Ils tentent de les convaincre qu'ils y gagneront, en bénéficiant d'un niveau de performance équivalent à un coût nettement inférieur. En conséquence, les opérateurs sont plus ou moins enclins à s'orienter ainsi.

En France, il existe déjà des solutions de fonctions réseau *cloud natives* qui sont déjà opérationnelles. Cependant, elles ne sont pas réellement déployées sur le *cloud*, mais sur des technologies *cloud* au sein des infrastructures des opérateurs.

En Allemagne, Telefonica a récemment communiqué sur sa solution de cœur de réseau data achetée chez Nokia, et déployée sur une infrastructure AWS. C'est assez rare, mais c'est intéressant de le noter, Telefonica Allemagne étant un opérateur représentatif. En tout cas, aujourd'hui, en France, ce n'est pas le cas. Les Google, Microsoft et AWS aimeraient bien devenir les fournisseurs, mais pour l'instant, ce n'est pas encore une réalité.

Les hyperscalers ont des philosophies qui ne sont pas forcément équivalentes : au-delà de la localisation des *data centers*, Google et Microsoft par exemple, permettent aux opérateurs et à tous types de clients, d'avoir des technologies *cloud* qu'ils ont développées pour eux-mêmes et qu'ils vendent maintenant à l'ensemble du marché, permettant de les avoir de façon complètement privée et containerisée. C'est-à-dire qu'on peut acheter auprès de Google de la technologie et être en complète maîtrise de cette technologie sans Google, et idem Microsoft,

En revanche AWS n'est pas en principe sur ce type de logique, mais sur l'idée de privatiser une partie du *cloud*, où l'accès est exclusif au client, tout en conservant une part de gestion de l'exploitation de l'infrastructure par le fournisseur.

Les opérateurs se posent de nombreuses questions, notamment du côté des directions de sécurité. D'un côté, les opérationnels veulent adopter ces technologies, et de l'autre, les hyperscalers financent des projets *via* des POC, avec toute la retombée sur les activités autour de ce POC. Cela fait que, pour les hyperscalers, au moment où ça passe à l'échelle, l'option *cloud* devient l'évidence.

Le concept de jumeau numérique ne décolle pas à pleine vitesse du fait de la complexité de créer un modèle conceptuel d'un réseau de télécommunications et en particulier un modèle de données unifié et homogène. C'est le rêve des opérateurs, car ça leur permettrait de jouer des scénarios de trafic de l'IA, parmi d'autres, et de voir l'impact que ça a sur le réseau et comment ils devraient soit reconfigurer le réseau, rajouter de la ressource, ou créer des catalogues de services, de dédier des ressources réseau au trafic de l'IA, en mode slice, par exemple, sur un réseau mobile, ou pas. L'IA va aider à faire émerger les jumeaux numériques.

5.8.3. Aspects réglementaires

Un des enjeux de la réglementation, concernant le numérique, porte sur la capacité à intégrer les enjeux d'innovation et en particulier à ne pas brider ex ante les axes d'innovation des acteurs. Cela peut concerner par exemple le développement de nouvelles offres 5G basées sur le *slicing* et la différenciation de la QoS, pour lesquels un cadre réglementaire trop strict peut tuer l'innovation dans l'œuf, avant même que son bénéfice, et la matérialité des risques aient pu être évalués.

Il faudrait avoir une analyse de ce que la réglementation propose, car c'est un sujet structurant.

Où tourneront les algorithmes dépendra de la réglementation et sera basée sur la nature des données :

- Données de l'IA qualifiées de froides (conception théorique avec des données froides) : des données complètement détachées que l'on extrait à un moment donné pour analyse ;
- Données de l'IA qu'on va analyser en temps réel et qui ne vont pas avoir d'action sur le réseau ;
- Données de l'IA qui vont avoir une action sur notre réseau, par exemple pour éteindre des composants ou pour corriger des problèmes.

Concernant le développement des algorithmes, on peut envisager un écosystème varié d'intervenants, avec des objectifs différents, où les opérateurs n'ont pas forcément besoin de développer des solutions transverses qui impliquent plusieurs fonctions réseau parallèles. Ils pourraient développer des algorithmes, pour des optimisations bien précises. En revanche, plus logiquement, les éditeurs et les constructeurs (Nokia, Ericsson, etc.), pourraient travailler sur du transverse.

À l'Arcep, lors d'une démarche qui s'appelle « Réseaux de futur », un travail a été réalisé sur l'informatisation des réseaux, qui va se poursuivre avec l'analyse de l'IA et les réseaux. Une vingtaine d'acteurs échangeront sur ces aspects d'évolution des réseaux grâce à l'IA, notamment sur les cadres réglementaires existants et comment ça va déjà façonner leurs développements, et identifier s'il y a d'autres sujets à penser et des actions à mener.

Le sujet de la cybersécurité et de la résilience est clé, l'utilisation de l'IA ouvre la porte à de nouvelles formes d'attaque.

La protection des données doit être traitée, en effet, les opérateurs collectent énormément de données qui sont extrêmement utiles aux opérateurs eux-mêmes, mais également à d'autres acteurs[24].

L'harmonisation du cadre réglementaire européen peut aussi permettre aux opérateurs de s'appuyer sur une dynamique collective plus forte et des effets d'échelle plus significatifs. Cette harmonisation doit donc, entre autres, permettre le lancement de nouvelles offres de service innovantes, et créatrices de valeur.

Nous pensons en particulier aux offres dédiées avec des éléments de différenciation de la qualité de service. Les exemples sont nombreux et peuvent porter par exemple sur un accès prioritaire pour les terminaux de paiement carte bleue, qui peuvent rencontrer des difficultés à accéder au réseau mobile lorsque le réseau est très chargé, comme lors de la mi-temps d'un évènement sportif, alors qu'ils nécessitent un débit faible mais avec une fiabilité élevée. D'autres services seront évidemment plus exigeants en débit, voire permettront à des flux différents de cohabiter sur le même accès radio (comme l'accès fixe sans fil et le haut débit mobile, pour lesquels il est souhaitable qu'aucun ne cannibalise l'accès au détriment de l'autre). Ces nouvelles offres ne peuvent pas être développées sans cadre, et la réglementation sur l'internet ouvert est clé, néanmoins, une approche harmonisée et plus ouverte à l'innovation peut permettre de stimuler le marché (l'incertitude actuelle pousse les acteurs à une certaine prudence).

La politique spectrale est également un aspect pour lequel l'harmonisation serait bénéfique en créant également des dynamiques plus fortes. Nous entendons aussi que le spectre est un élément de souveraineté et que cette harmonisation peu aussi prendre des formes plus souples.

5.8.4. Les réseaux pour l'IA

L'IA devient de plus en plus distribuée, notamment *via* l'*edge* computing et en particulier le MEC, pour des raisons de latence et de protection des données, entre autres facteurs.

Une question importante est de savoir si les infrastructures sur lesquelles l'IA fonctionne doivent être constamment opérationnelles ou non. En effet, la *softwarisation* des réseaux permet d'activer et de désactiver les fonctions à la demande. La forte dynamique du trafic généré par l'IA requiert cela.

Un point clé avec le déploiement massif de l'IA est son empreinte carbone significative, qui ne diminue pas avec l'*edge*. Le fait de déployer massivement des ressources de calcul et de stockage à l'*edge* peut avoir un impact bilan carbone négatif important pour celui qui déploie les ressources, mais par rapport aux cas d'usage, ça peut amener, au niveau des verticaux, une réduction significative de l'impact environnemental. Et donc la question est de regarder le

[24] Se pose par ailleurs la question de l'ouverture sous conditions de ces données à la communauté des chercheurs afin d'accélérer certaines innovations. À titre d'exemple de bonne pratique, la DGA met à disposition, à des équipes de recherche mais aussi à des industriels, des données qui sont plus orientées cyberdéfense.

bilan, pour que ça ne pèse pas sur les opérateurs, mais au contraire, qu'ils deviennent des fournisseurs de solutions vis-à-vis du développement durable.

L'usage intelligent de l'IA implique une approche globale, probablement multi-opérateurs, et une mutualisation des ressources pour des déploiements responsables. Concernant les verticales et l'*edge*, la difficulté est de trouver des cas d'usage complémentaires aux usages réseaux pour partager les ressources dynamiquement entre les divers besoins.

Il est possible d'imaginer à terme un co-investissement sur ces ressources, qui serait fait par les opérateurs et par des acteurs de divers verticaux. Les opérateurs ont des points de présence où déployer ces ressources et cela est une valeur indiscutable aujourd'hui. Et d'autres acteurs pourront amener sur ces endroits-là la capacité de calcul et de stockage.

Les problématiques de mutualisation des infrastructures et de mutualisation des investissements, sont communes à de nombreux enjeux européens aujourd'hui. Dans le cadre du développement des réseaux de communication et des convergences déjà évoquées, aucun acteur ne souhaite prendre seul le risque ; les montants requis pour le passage à l'échelle requis étant trop importants. Seule la mise en commun des compétences et des moyens permet de résister à des menaces de compétition importantes qui viennent des États-Unis ou de la Chine. On a besoin de bâtir des propositions pour avoir des moyens qui soient à la hauteur, que ce soit sur des plans nationaux ou européens. Il est nécessaire que chacun y trouve sa place dans la chaîne de valeur en termes de positionnement. Il faut concevoir et implémenter de nouveaux modèles d'affaires, permettant à chaque acteur de garantir son développement de marché et de trouver des différenciateurs. Airbus, par exemple, soutient ces réflexions et ces initiatives, puisque ce sont les seules façons que l'on voit d'avancer.

L'entraînement et l'exécution de grands modèles de langage (LLM) dans les *data centers* présentent des défis importants, notamment la demande massive en puissance de calcul et en bande passante, ainsi que la complexité de la gestion de l'infrastructure. Dans le domaine du HPC, historiquement tourné vers le calcul scientifique, les besoins réseau étaient bien moindres par rapport à l'IA générative.

Cela ouvre aussi des opportunités considérables pour les équipements. L'augmentation exponentielle des données nécessite des interconnexions GPU haute performance pour accélérer les communications inter-GPU, cruciales pour l'efficacité de l'entraînement distribué. Des technologies comme NVLink, offrant une bande passante très élevée à faible latence entre GPU d'un même serveur, et UEC (Ultra Ethernet Consortium), visant à étendre les capacités d'Ethernet pour les interconnexions entre serveurs, sont essentielles pour relever ces défis. L'optimisation de ces interconnexions est clé pour améliorer la vitesse d'entraînement et réduire les coûts énergétiques, ouvrant la voie à des modèles LLM plus grands et plus performants. L'interconnexion des *data centers* et des serveurs avec des composants optiques, co-packaged optics, est désormais indispensable pour répondre aux besoins de communication. Dans le domaine des clusters pour l'IA, il y a quelques entreprises dites « full-stack » (Nvidia, Huawei) qui ont des solutions allant du réseau au traitement, de nombreux intégrateurs et des fournisseurs de composants spécialisés (cartes réseaux, switch et routeurs, serveurs, logiciels).

Afin d'anticiper et de suivre l'évolution du trafic IA sur les réseaux et les changements de modèles de trafic, Orange a initié un observatoire de trafic et son développement à plus large échelle *via* un groupe de la GSMA *« AI Traffic Observatory »*.

5.8.5. Vision des standards

Comme décrit dans les recommandations de l'ITU-R [1], l'intelligence artificielle (IA) est considérée comme un pilier fondamental des systèmes 6G, capables de fournir des services pour des applications intelligentes et de répondre aux moteurs environnementaux, sociaux et économiques de la 6G.

Dans le contexte des systèmes 6G pilotés par l'IA, deux concepts sont anticipés comme étant essentiels pour façonner les systèmes futurs : **l'IA pour le système 6G** et **le système 6G pour l'IA**.

- **L'IA pour le système 6G** fait référence à l'utilisation des capacités de l'IA pour soutenir le réseau et les dispositifs dans la fourniture des services 3GPP.
- **Le système 6G pour l'IA** se concentre sur la manière dont le système prend en charge et permet les applications d'IA en exploitant les fonctionnalités du système 6G pour fournir différents services.

Dans cette section, nous analysons les cas d'usage 6G du groupe SA1 de la 3GPP soutenant ces deux concepts (présentés dans le document [2]), afin de tirer des conclusions préliminaires sur l'impact des technologies d'IA dans la 6G.

RÉSUMÉ DES CAS D'USAGE

Cette section présente un résumé des différents cas d'usage liés à l'IA, regroupés par thématique, issus du document TR 22870 [2].

Une première thématique commune à plusieurs cas d'usage peut être identifiée comme L'***AI as a Service*** **(AIaaS)**. Selon les sources récentes disponibles, cette thématique concerne à la fois les concepts de « l'IA pour le système 6G » [3] et de « le système 6G pour l'IA ». Le système 6G agit comme une plateforme, fournissant ces services d'IA et les outils correspondants dans le cadre de ses capacités « au-delà de la communication » (« beyond communications »).

L'AIaaS est capable de prendre en charge des consommateurs externes (fonctions d'application tierces, AFs, équipements utilisateurs, applications verticales, etc.) en exploitant les ressources du système 6G (comme les ressources de calcul, de stockage, de réseau), mais elle prend également en charge des cas d'usage où l'IA est utilisée pour soutenir les fonctionnalités du réseau, l'automatisation et l'auto-organisation des différents éléments et processus du réseau [3].

Plusieurs cas d'usage du TR 22870 concernent également les **agents IA**. Dans certains cas, l'AIaaS est soit demandée par un agent IA, soit un agent IA est fourni dans le cadre de l'AIaaS demandée, soit l'agent IA participe à la supervision de l'AIaaS fournie.

Sujet	Sous-sujet	Description	Cas d'usage associés

AIaaS	*AI Training as a Service*	L'entraînement des modèles d'IA est délégué par des entités externes (par exemple les équipements utilisateurs : UEs, AFs, les tiers : « 3rd party ») au réseau 6G, notamment afin de s'appuyer sur les données du système 6G.	6.1, 6.11, 6.20, 6.24, 6.26, 6.28, 6.29, 6.31, 6.34, 6.35, 6.36
	AI Inference as a Service	Des entités externes sollicitent des inférences à partir de modèles pré-entraînés hébergés dans le réseau 6G, permettant une exécution de l'IA à faible latence et haute performance.	6.1, 6.2, 6.4, 6.8, 6.9, 6.12, 6.13, 6.14, 6.16, 6.17, 6.18, 6.19, 6.20, 6.22, 6.24, 6.28, 6.29, 6.30, 6.31, 6.32, 6.33, 6.34, 6.35, 6.36, 6.38
AI agent	Agent IA exposé par le réseau 6G	Un agent IA spécifique est exposé par le réseau 6G et fournit des capacités d'IA (par exemple, analyses, prédictions, décisions) à des entités externes *via* des interfaces.	6.12, 6.30, 6.31, 6.38
	Collaboration entre agents d'intelligence artificielle au niveau des applications	Plusieurs agents IA intégrés dans des applications (par exemple sur les équipements utilisateurs : UEs, dans le *cloud* ou à la périphérie : « *edge* ») interagissent et collaborent pour accomplir les tâches ou objectifs des utilisateurs.	6.5, 6.6, 6.8, 6.22, 6.28, 6.37
	Collaboration entre l'agent d'intelligence artificielle au niveau de l'application et les fonctions du réseau	Les agents IA dans les applications ou les équipements utilisateurs (UEs) exploitent les informations fournies par le réseau.	6.2, 6.7, 6.10, 6.13, 6.16, 6.19, 6.20, 6.22, 6.29, 6.30
AI Native	AI Native	L'IA est profondément intégrée au réseau 6G ou aux fonctionnalités réseau, sans nécessité spécifique d'agents IA.	6.3, 6.6, 6.7, 6.13, 6.14, 6.15, 6.17, 6.18, 6.19, 6.20, 6.21, 6.22, 6.23, 6.25, 6.27, 6.28, 6.29, 6.32, 6.33, 6.34, 6.35, 6.37, 6.38, 6.39

DÉFINITION DE L'AIAAS

*L'**AIaaS (AI as a Service)** peut être décrit comme une fonctionnalité du réseau 6G permettant la création, la configuration et la supervision de services d'IA, proposée à différents utilisateurs (par exemple à un équipement utilisateur (UE), à une application tierce, etc.). Ces services sont déployés dans le cloud ou le réseau de l'opérateur, à un emplacement personnalisable. Ils exploitent les données disponibles à l'intérieur et à l'extérieur du réseau 6G.*

En analysant les cas d'usage de l'IA présentés dans le document [2], on observe le rôle central et multifacette de l'AIaaS dans la fourniture de services d'IA dans les systèmes 6G. Notamment, les deux types d'AIaaS proposés dans la taxonomie sont représentés à travers des cas d'usage, ce qui confirme la pertinence de cette taxonomie.

- ***AI Training as a Service*** et ***AI Inference as a Service*** apparaissent fréquemment dans les scénarios impliquant le déport de l'entraînement et de l'inférence des modèles d'IA, en particulier pour les utilisateurs externes tels que les UEs et les applications tierces.

Ces observations renforcent l'idée que l'utilisation d'IA dans la 6G constitue un écosystème riche et structuré — couvrant la création de services d'IA, leur dynamique, leur intelligence, leur personnalisation et leur capacité de raisonnement — et que la taxonomie proposée offre un cadre robuste pour comprendre les services activés par l'IA dans la 6G.

5.8.6. Considérations préliminaires sur l'impact de l'IA sur l'architecture réseau

Les contributions continues des entreprises et des opérateurs à la 6G, illustrées par les cas d'usage du TR 22870 [2], montrent le rôle important que l'IA jouera dans la nouvelle génération de réseaux.

Environ 60 % de tous les cas d'usage sont **agentiques**, ce qui signifie que les agents IA sont la technologie centrale, moteur de l'évolution du réseau. Les tâches d'étude récemment adoptées par le groupe SA2 mentionnent la capacité de **raisonnement** comme un objectif du réseau. Le groupe SA5 prépare également son étude (en août 2025) et considère les fonctionnalités **agentiques** et **AI/ML**. De plus, de nombreux cas d'usage supposent que le réseau peut être précisément personnalisé selon les besoins de l'utilisateur, ce qui est sans précédent dans les réseaux informatiques.

L'IA et les agents IA mèneront probablement à l'introduction de nouvelles fonctionnalités dans le cœur du réseau et dans l'OAM (Opérations, Administration et Maintenance), organisées pour soutenir la capacité de raisonnement du réseau. Ces possibilités sont actuellement à l'étude chez Nokia et chez d'autres acteurs.

L'architecture réseau pourrait évoluer pour inclure une nouvelle fonctionnalité spécialisée dédiée au support de l'IA, **permettant à la fois l'hébergement d'agents IA ou de modèles de langage (LLM) et la fourniture de services AIaaS, dans le cadre de l'intelligence embarquée du réseau.**

Par ailleurs, l'organisation actuelle du réseau en plans de contrôle, de gestion et d'utilisateur ("control, management and user plane") pourrait évoluer pour intégrer davantage d'automatisation basée sur l'IA, ainsi que des capacités de diffusion de données à haut débit et à faible latence (nécessaires pour l'IA) entre les différents domaines du réseau. Les principaux défis de cette évolution sont les suivants :

1. La latence des agents IA (les latences de traitement des modèles de langage de grande taille – LLMs, dépassent 150 ms) ;
2. La nécessité de maintenir la compatibilité avec les standards 3GPP existants ;
3. Le défi pour les opérateurs de réseau, qui doivent maîtriser les technologies *cloud*, y compris le MLOps et le "data engineering" (indispensables pour supporter un réseau centré sur l'IA) ;

4. La nécessité de définir les standards 3GPP en cohérence avec les meilleures pratiques des standards (ou “de-facto standards”) liés à l’IA, en évolution rapide (par exemple MCP, A2A, etc.).

References:

[1] Recommendation ITU-R M.2160-0 : Framework and overall objectives of the future development of IMT for 2030 and beyond.

[2] TR 22870, SA1 3GPP, 2025 (Specification # 22.870)

[3] NGMN, “6G USE CASES AND ANALYSIS”, v1.0, www.ngmn.org

5.9. Monétisation dans la 6G

La 6G promet une révolution technologique sans précédent, ouvrant la voie à des applications et services radicalement nouveaux, bien au-delà des capacités de la 5G. Pour exploiter pleinement ce potentiel et assurer la rentabilité des investissements massifs nécessaires au déploiement de la 6G, une plateforme de monétisation robuste et évolutive est indispensable. Cette plateforme permettra non seulement de gérer efficacement les différents modèles de tarification et de facturation des nouveaux services utilisateurs directs de ressources réseau (y compris les réseaux privés ou dédiés usages dans des approches de type *« multi tenancy »*), mais aussi de stimuler l'innovation et l'adoption de la 6G en offrant des mécanismes de partage des revenus et en facilitant l'accès au marché pour les développeurs d'applications et les fournisseurs de services. Sans une telle plateforme, le potentiel économique de la 6G risque de rester largement inexploité.

Quelques exemples de services permettant de valoriser le réseau

- Ouverture du réseau pour devenir une plateforme de services, telle qu‘évoqué précédemment dans ce document.
- Mise en place dans le réseau d’un plan de gouvernance pour l’IA agentique distribuée multi-acteurs.
- Solutions pour les réseaux non terrestres et la convergence terrestre/non terrestre.
- Évolutions vers des applications immersives, à 6 degrés de liberté, embarquant de la réalité virtuelle, augmentée et mixte, et leurs applications dans divers cadres : jumeaux numériques industriels avancés, interactions distantes hommes-machines, télémédecine, etc.
- Mise en œuvre dans le réseau de solutions de sécurité avancées en mode service, notamment de protection des données et de protections des individus (détection automatique et estampillage de circulation de fake news).
- Validation des performances, fonctionnalités et de résilience aux attaques des applications
- *Slicing* différencié offrant des garanties de service, autrement dit, partitionnement virtuel du réseau avec un passage à l’échelle en quantité de réseaux virtuels et avec une adaptation dynamique de chaque réseau aux besoins spécifiques des services et applications qu’il supporte, à terme dans un cadre de réseau orienté objectifs.
- Mesure et prédiction de l’efficacité énergétique des applications utilisant le réseau

- Optimisation de la localisation des traitements (équipement utilisateur, *edge* ou serveur du fournisseur) pour l'IA générative multimodale (texte, audio, vidéo) ou la réalité augmentée en fonction de la localisation de l'utilisateur, des besoins de latence, de la charge des processeurs et du réseau : *« Off loading as a service »* des applications du terminal sur le réseau, *« inference as a service »* à l'*edge* …
- Place de marché pour des applications d'une entreprise ou d'une infrastructure telle qu'un port ou un réseau électrique (pour la maintenance, la sécurité, l'efficacité environnementale …)
- Diagnostic à distance impliquant la collecte temps réel de données et les analyses appropriées (par exemple dans la santé)
- *« Sensing as a service »* : Exposition des capacités du réseau à capter l'environnement.
- - Programmation de l'adaptation de la couverture réseau pour des événements spécifiques (concerts, situations d'urgence, etc.).

Les architectures totalement distribuées, basées sur la blockchain, pourraient répondre au besoin de monétisation dans la 6G. Ces systèmes permettent une rémunération transparente et sécurisée des différents acteurs impliqués, qu'il s'agisse de fournisseurs de données, de développeurs d'applications ou d'utilisateurs finaux. La blockchain assure la traçabilité des transactions et la distribution équitable des revenus, favorisant ainsi l'innovation et la participation à l'écosystème 6G. Grâce à des contrats intelligents (smart contracts), la rémunération des services peut être automatisée et conditionnée à la réalisation de performances spécifiques, créant un modèle économique plus juste et efficient. Enfin, cette approche décentralisée renforce la sécurité et la confidentialité des données, un aspect crucial pour la confiance des utilisateurs et le succès de la monétisation.

Cette monétisation absolument nécessaire de la 6G, tout en s'appuyant sur les mécanismes décrits ci-dessus nécessitera également un cadre réglementaire favorable à l'innovation (donc avec parfois une approche plus ex post plutôt qu'ex ante) et intégrant plus largement des mécanismes de différenciation de qualité de service (tout en préservant les principes d'un internet ouvert).

6. Catégorisation des opportunités et des risques pour les acteurs actuels et les nouveaux entrants

Analyse des impacts potentiels des évolutions de la section précédente et du cadre géopolitique global sur le positionnement des acteurs existants et émergents (notamment en Europe, États-Unis et Chine) et sur la constitution des filières, l'identification des opportunités et des risques, notamment en ce qui concerne la souveraineté de la France et de l'Europe.

Quelques exemples de sujets à développer ici (voir également la publication citée) :

- Fédération au niveau européen d'acteurs, à la fois des réseaux et du *cloud*, et en collaboration avec les verticaux, permettant ainsi une différenciation par rapport aux GAFAM *via* des services ciblés et des cas d'usage spécifiques.
- Préciser ce que recouvre la virtualisation des réseaux, comment cela impacte les modèles d'affaires et le positionnement des acteurs à divers horizons de temps, couvrir le cycle de vie (conception, déploiement, opération et maintenance, transformations, interaction avec d'autres acteurs, interopérabilités, etc.), impact sur la sécurité, la robustesse, la fiabilité, la résilience, rôle de l'IA et des *digital twins* dans ces cycles de vie, etc.
- Issue du secteur des télécommunications, la *cloudification* des fonctions réseaux amène de nombreux bénéfices permettant aux opérateurs de télécommunications d'embrasser l'ère de la data et de l'IA. Néanmoins, cette transformation s'est également accompagnée d'un frein de taille : la fragmentation des *Telco Clouds*. Cette non-agnosticité » des fonctions réseaux envers les *Telco Clouds* originaux a logiquement amené les opérateurs de télécommunications à pousser pour la mise en œuvre d'un *telco cloud* horizontal, repoussant les principes des solutions propriétaires et embrassant la logique du « faire ensemble ». Concrètement, les principaux opérateurs de télécommunications européens ont joint leurs forces pour créer le projet *open source* Sylva, hébergé au sein de la Linux Foundation Europe. Le projet Sylva a pour mission de livrer une implémentation de référence d'une pile protocolaire « *Telco Cloud* » 100 % *open source*, conforme aux exigences de sécurité européennes et répondant aux enjeux de souveraineté. Le projet dispose également d'un programme de validation qui permet de certifier la compatibilité des applications, qu'elles soient telco ou non.
  Au-delà de l'écosystème des télécommunications, la stack Sylva est utilisée dans le cadre de l'*edge* computing. C'est ainsi qu'on la retrouve au cœur des nœuds *edge* mis en œuvre au sein du pilote Lab8ra, financé par le PIIEC Cloud Infrastructures & Services.
  La stack Sylva est également utilisée pour héberger des applicatifs IT classiques et se positionne donc naturellement comme un enabler de la convergence télécoms, IT et *edge* pour des acteurs soucieux de la conformité aux exigences de sécurité et de souveraineté.
  Pour finir, le modèle ouvert du projet Sylva permet à tout acteur de devenir contributeur et d'ainsi s'assurer de la prise en compte de ses besoins au sein de la roadmap technique. C'est un excellent moyen d'éviter de reproduire une situation

de monopole comme celle vécue récemment dans l'IT à la suite du rachat de VMware par Broadcom !

- L'ouverture des réseaux *via* des API, l'ouverture plus générale des IN fortement convergentes (l'infrastructure numérique devenant alors un environnement de type *Platform as a Service*, voir l'Annexe I) au-delà de l'exposition (NEP, *Network Exposure Platform*), pour mettre en place des places de marchés de composants dans les infrastructures de demain, une orchestration dynamique et hiérarchique, et des modèles d'affaires associés, en faisant des choix technologiques (e.g. API CAMARA).
- **Disponibilité de la *supply chain*, présenter un graphe de dépendances.**

Juste pour citer un exemple qui montre les évolutions des positionnements, rappelons que China Telecom a déployé une IA de leur propriété, sur des infrastructures puissantes, qui lui ont permis de caser des systèmes de cybersécurité. Ils pourraient dans une deuxième phase déployer en dehors de la Chine. La Chine se positionne notamment en Afrique et en Amérique Latine.

6.1. Consolidation et renforcement du positionnement des opérateurs de télécommunications

Dans le contexte de la *« cloudification »* et de *« softwarisation »*, et de la multiplication des usages des infrastructures numériques, les acteurs télécoms ont des opportunités indéniables. À l'avenir, presque tous les appareils seront connectés partout et à tout moment. Cette opportunité confère au secteur des télécommunications un avantage unique pour conquérir les divers segments de marché que ces appareils et leurs applications représentent. Un prérequis est cependant que les acteurs télécoms se concentrent sur les facilitateurs et la capacité à différencier leurs services grâce au réseau et aux fonctionnalités les mieux adaptées aux besoins des applications. En particulier ils sont soumis à des défis sur la valorisation de leur infrastructure, qui exigent des adaptations importantes :

- Défi des délais de mise sur le marché. L'émergence de nouveaux cas d'usage à forte valeur ajoutée peut être difficilement compatible avec le rythme de standardisation et des évolutions traditionnelles des télécommunications par rapport aux échelles de temps plus rapides des acteurs du *cloud* et des applications logicielles.
- Défi pour marketer les évolutions des fonctions ou performances réseaux en arguments pertinents pour les utilisateurs sur de multiples marchés grand public ou entreprises.

Il s'agit de migrer le modèle économique des infrastructures vers un modèle de plateforme dont le marché multiface peut impliquer des acteurs tiers dans la chaîne de monétisation, en incorporant et valorisant des interfaces exposant les capacités et configurations du réseau[25,]

[25] Bien au-delà de la fourniture de l'infrastructure *cloud*, une grande force des hyperscalers est constituée par les services multiples qu'ils fournissent pour développer des applications sur leur environnement

[26]. Cette ouverture doit être conciliée avec le maintien du contrôle des fonctions stratégiques du réseau, et des garanties en matière de cybersécurité. Il s'agit aussi de valoriser la grande quantité de données à disposition des acteurs télécoms, les approches IA étant un élément clé pour ce faire. À cet égard, les réseaux de télécommunications peuvent tirer un avantage sur les hyperscalers, car les données sont par défaut explicitement associées aux propriétaires des terminaux et aux clients du réseau privé à leur disposition. Grâce à de nouvelles fonctionnalités, telles que les réseaux basés sur l'intention, la facilité de configuration et d'automatisation des réseaux, et à l'aide de solutions telles que le *slicing*, il sera plus facile de personnaliser le réseau en fonction des préférences de chaque client. L'analyse des données collectées dans le réseau peut aider à cette différenciation des besoins des multiples clients. Tout cela doit être encadré par des solutions automatisées assurant sécurité et préservation des données privées, pour le management des données clients ou l'accès des tiers aux API par exemple.

La coordination d'un tel écosystème *edge* peut être très complexe, et les approches commerciales traditionnelles peuvent rencontrer de nombreux problèmes de coordination en raison du grand nombre de fournisseurs impliqués. Une place de marché décentralisée rassemblant différents acteurs clés (fournisseurs de services applicatifs/de contenu, fournisseurs de services de communication, fournisseurs de services *cloud hyperscale*, fournisseurs de *cloud edge*) peut être la bonne réponse.

En résumé, les acteurs télécoms doivent viser à développer un écosystème sécurisé qui améliore le délai de mise sur le marché de nouvelles fonctionnalités (incluant des acteurs tiers) et qui permet de commercialiser ces fonctionnalités de manière différenciée aux différents segments de clients de l'écosystème, en se basant sur la compréhension des besoins de chaque segment de client grâce aux données collectées auprès des utilisateurs, du réseau et d'autres sources.

La constitution de cet écosystème passera par des actions (R&D, pilotes, déploiements) fédérées entre acteurs, équipementiers, opérateurs, développeurs d'applications, utilisateurs verticaux pour constituer des offres différenciatrices avec des modèles économiques pérennes et équilibrés. Le CSF des infrastructures numériques peut être un levier pour y parvenir en lien avec des CSF verticaux.

Il s'agit de migrer le modèle économique des infrastructures vers un modèle de plateforme dont le marché multiface peut impliquer des acteurs tiers dans la chaîne de monétisation, en incorporant et valorisant des interfaces exposant les capacités et configurations du réseau. Cette ouverture doit être conciliée avec le maintien du contrôle des fonctions stratégiques du réseau, et des garanties en matière de cybersécurité. Il s'agit aussi de valoriser la grande quantité de données à disposition des acteurs télécoms, les approches IA étant un élément clé pour ce faire. À cet égard, les réseaux de télécommunications ont un avantage sur les hyperscalers, car les données sont par défaut explicitement associées aux propriétaires des terminaux et aux clients du réseau privé à leur disposition. Grâce à de nouvelles

[26] Voir par exemple : Nokia acquires Rapid technology and R&D unit to strengthen development of network API solutions and ecosystem

fonctionnalités, telles que les réseaux basés sur l'intention, la facilité de configuration et d'automatisation des réseaux, et à l'aide de solutions telles que le *slicing*, il sera plus facile de personnaliser le réseau en fonction des préférences de chaque client. L'analyse des données collectées dans le réseau peut aider à cette différenciation des besoins des multiples clients. Tout cela doit être encadré par des solutions automatisées assurant sécurité et préservation des données privées, pour le management des données clients ou l'accès des tiers aux API par exemple. Une place de marché décentralisée rassemblant différents acteurs clés (utilisateurs, fournisseurs de services applicatifs/de contenu, fournisseurs de services de communication, fournisseurs de services *cloud hyperscale*, fournisseurs de *cloud edge*) peut être la bonne réponse.

En résumé, les acteurs télécoms doivent viser à développer un écosystème sécurisé qui améliore le délai de mise sur le marché de nouvelles fonctionnalités (incluant des acteurs tiers) et qui permet de commercialiser ces fonctionnalités de manière différenciée aux différents segments de clients de l'écosystème, en se basant sur la compréhension des besoins de chaque segment de client grâce aux données collectées auprès des utilisateurs, du réseau et d'autres sources. La coordination d'un tel écosystème peut être très complexe, et les approches commerciales traditionnelles peuvent rencontrer de nombreux problèmes de coordination en raison du grand nombre d'acteurs impliqués.

L'IA agentique aura certainement un rôle clé à jouer dans l'orchestration flexible et dynamique des fonctionnalités et services offerts par ces multiples acteurs. On parle ici d'un aspect important de l'IA pour les réseaux.

Par ailleurs, les réseaux sont incontournables dans la mise en œuvre des nouvelles architectures de l'IA, notamment de l'IA fédérative et agentique, avec le développement des plus petits modèles, notamment pour l'agentique avec une « fédération *à l'edge* » qui va changer les paradigmes actuels de l'IA. Nous voyons ici un des points forts de l'*edge* et tout particulièrement du *mobile edge computing* où les ressources sont déployées dans le réseau des opérateurs. Cette approche MEC est souvent citée pour ses avantages en termes de latence, mais son rôle pour le déploiement de nouvelles architectures d'IA aura certainement un impact fort à plus court terme.

De plus, les opérateurs de télécommunications peuvent prendre position dans la mise en place du plan de gouvernance de l'IA agentique que nous avons déjà évoqué.

Face à l'émergence de l'IA agentique, les opérateurs de télécommunications ont donc un rôle important à jouer dans l'orchestration et la maîtrise de cette révolution technologique en distribuant l'intelligence au plus près de l'action concernée. En fédérant les capacités de calcul distribuées entre l'*edge*, le *mobile edge* et le *cloud* centralisé (porté par les grands *data centers*), les opérateurs peuvent déployer une nouvelle couche d'orchestration avancée permettant de coordonner efficacement ces ressources même lorsqu'elles sont réparties entre acteurs de différentes tailles et utilisant des infrastructures hétérogènes. En intégrant des mécanismes d'authentification, de contrôle, de traçabilité et de sécurité dans cette couche d'orchestration, les opérateurs peuvent également protéger les utilisateurs contre les

risques liés à l'IA agentique, tels que la manipulation, la désinformation ou la violation de la vie privée.

Par ailleurs, cette capacité à orchestrer de manière dynamique et sécurisée la distribution des ressources permettrait à la France de maîtriser le développement de l'IA agentique, en évitant une dépendance excessive aux acteurs étrangers, tout en favorisant l'innovation responsable. En somme, les opérateurs de télécommunications, en tant que gestionnaires de l'infrastructure numérique, sont en position de devenir des acteurs clés dans la régulation, la sécurisation et la souveraineté de l'écosystème IA agentique, contribuant ainsi à préserver la confiance des citoyens et à soutenir la compétitivité de la France dans ce domaine stratégique.

Dans une vision plus lointaine des réseaux mobiles, nous anticipons déjà que la 6G intègrera une composante l'IA dans chaque fonction de l'accès jusqu'au cœur de réseau avec probablement de l'IA agentique qui permettra de rendre la gestion, l'orchestration, l'optimisation et la configuration des réseaux et services plus autonomes et adaptatives. En contrôlant le champ d'action des agents IA sur les infrastructures numériques, nous pourrons les protéger et limiter les risques inhérents à une trop forte délégation de décisions, même locales.

7. Recommandations

Ce document a montré que la dimension de souveraineté des infrastructures numériques face aux évolutions technologiques et de marché (réseaux, *cloud*, *edge*, NTN, IA…) est un enjeu critique pour notre futur. Il convient de définir une stratégie et un plan d'action concernant le périmètre de souveraineté que l'on souhaite atteindre, au niveau national et au niveau européen, sachant qu'aucun des deux n'est réellement possible sans l'autre. L'enjeu central est d'obtenir la souveraineté numérique et de réaliser tout son potentiel dans la mise en place d'une souveraineté tout court à la fois civile et militaire. Se pose alors la question de la définition même de la souveraineté numérique visée. Au sens le plus strict, cela pourrait signifier de contrôler toute la chaîne technologique, toutes les infrastructures et tous les services et applications. Ceci est aujourd'hui et à court/moyen terme illusoire, au regard des investissements et du temps nécessaire, même si la France dispose des compétences pour le faire. Il convient donc de préciser le périmètre de la souveraineté recherchée ainsi que le niveau de contrôle visé (souhaité et faisable à divers horizons de temps).

Les recommandations que nous présentons dans ce document visent cet objectif. Elles ne cherchent pas à refermer la France, avec le risque évident de déclassement de ses citoyens et de son économie, mais au contraire à définir un cadre qui lui garantisse l'autonomie technologique nécessaire à atteindre, conjointement avec des partenaires de confiance, le niveau d'indépendance visé. Cela passe par l'acception d'un certain niveau de dépendance que le pays doit être prêt à assumer, vis-à-vis de fournisseurs de matériels et de logiciels clés, voire d'infrastructures et plateformes non européennes, ainsi que par le rôle que l'on souhaite donner aux solutions *open source* (à condition de les maîtriser).

La réglementation européenne très active ces dernières années peut et doit être un levier. *Via* le *Trade and Technology Council*, forum politique de coopération transatlantique créé pour coordonner les politiques entre l'Union européenne et les États-Unis sur les sujets économiques, numériques et technologiques, des solutions pourraient être imaginées. Enfin, avec les dernières réflexions européennes, une nouvelle version du *Digital Network Act* (DNA) a été annoncée, intégrant le NIS2 mais également un nouveau DNA pour lequel la résilience est identifiée comme item prioritaire, avec des visions duales civil-militaire (en lien notamment avec le rapprochement UE-OTAN sur ces sujets).

Ce DNA rappelle que des clients peuvent préférer des solutions venant d'ailleurs pour se protéger en cas de problème parce que considérées comme plus sûres au sens large, ce qui leur donne une couverture en cas de problème, par rapport au cas où ils auraient choisi un acteur plus petit, plus local.

Dans ce cadre général, et en complément des recommandations portant sur des enjeux spécifiques développées dans le reste du document — que nous avons regroupées à la fin de cette section afin d'en offrir une vision d'ensemble —, nous formulons ci-après un ensemble de recommandations à caractère plus organisationnel et transversal.

7.1. Recommandations transverses liées aux technologies et à leur valorisation

Les briques technologiques impliquées par les architectures évoquées dans ce livre blanc recouvrent à la fois le matériel, les logiciels et les applications elles-mêmes. Elles seront d'autant plus faciles à appréhender par les acteurs (académiques et industriels) qu'elles seront maîtrisées dans une vision systémique de bout en bout à la fois de façon horizontale (des grands *data centers* aux objets connectés, en passant par l'*edge* réseau, tous portant des capacités de communication, de calcul et de stockage, y compris au niveau non terrestre) et verticale (du composant aux services, en passant par les architectures de plus en plus convergentes réseaux, *cloud* IA et services). Il s'agit donc d'aider à cette maîtrise sur plusieurs axes.

7.1.1. Élaborer une ou des visions pour motiver les interactions fortes inter filières.

Une impulsion publique peut être déterminante pour catalyser ces visions intégratives, fortement créatrices de valeur, mettant en action les acteurs de diverses filières, incitant leur fédération au travers de nouveaux modèles économiques pertinents pour chacun. Il s'agit de filières n'ayant pas forcément un historique d'interactions fortes, d'où le besoin d'une impulsion publique. Plusieurs actions peuvent être envisagées :

- Faire de la stratégie d'accélération sur les réseaux du futur le catalyseur des réflexions sur la stratégie R&D liée aux briques technologiques et aux systèmes identifiés comme critiques pour la souveraineté (élaboration d'une feuille de route coconstruite avec les CSF contributeurs (infrastructures numériques, électronique, logiciels et solutions numériques de confiance, sécurité).
    - S'appuyer sur les PEPR correspondants (PEPR Réseaux du Futur[27], *cloud*, électronique, IA, quantique, cyber, etc.) pour définir une feuille de route conjointe de recherche, sur France6G pour la coordination des actions nécessaires en standardisation, conjointement avec d'autres initiatives similaires pour ce qui est des organismes de normalisation d'autres filières (notamment sur la gouvernance de l'IA).
    - Un focus tout particulier doit être mis sur les actions nécessaires à garantir le *continuum* de la recherche au marché, en soutenant des initiatives telles que FRAMExG, dans le cadre plus large décrit ici.
    - S'appuyer sur les pôles de compétitivité capables d'impliquer les écosystèmes ancrés dans les territoires.
- Impulser des feuilles de route coordonnées transverses aux CSF sur les cas d'usage et besoins associés prioritaires, quand cela est pertinent hybrides civil-militaire, en intégrant les enjeux de modèles économiques. On peut citer à titre d'exemples les CSF Automobiles, ferroviaire, Industries électroniques, industries des nouveaux systèmes

[27] Le PEPR Réseaux du Futur a déjà obtenu des résultats qui représentent une première mondiale. Il a par ailleurs contribué à des organismes de normalisation, mis à disposition des logiciels, porté des résultats dans le cadre de montages de projets européens, etc.

énergétiques, industries et technologies de la santé, industries de sécurité, logiciels et solutions numériques de confiance, solutions industrie du futur.

7.1.2. Maîtriser et contribuer aux standards

Il s'agira d'accompagner les acteurs industriels développeurs de briques technologiques s'inscrivant dans ces architectures pour connaître les standards et éventuellement proposer leurs innovations aux organismes ad hoc après les avoir protégées du point de vue de la propriété intellectuelle. Dans la continuité des missions de France6G, il est nécessaire de passer à une vision qui dépasse la filière réseau et donc la 6G, pour couvrir l'ensemble des organismes de normalisation pertinents. La continuation de l'action de FRAMExG étendue à l'ensemble des chaînes de valeur impliquées est une solution pertinente, notamment pour transformer les résultats obtenus par les PEPR Réseaux du Futur dans des brevets essentiels aux normes. Le PEPR a déjà contribué à divers organismes de normalisation et cela s'accélère avec l'arrivée à maturité des travaux de divers projets. Le PEPR a notamment pris part à l'élaboration de la récente proposition soumise à l'ETSI en vue de la création d'un groupe de travail sur les communications sémantiques. Le noyau des travaux se basant sur des résultats obtenus par le PEPR. Les pôles de compétitivité et les acteurs locaux (technopoles-French Tech)) doivent acculturer les PME / startups comme les laboratoires académiques sur ces enjeux en lien avec les SATT et l'INPI.

- Il conviendra aussi de faire en sorte que les académiques puissent trouver auprès d'industriels familiers des process de standardisation l'appui nécessaire à la reconnaissance des résultats de leurs recherches.
- Dans la mesure où de nombreuses briques logicielles sont issues de l'*open source* une action spécifique sur l'acculturation aux règles d'usage, de contribution et d'évolution sera utile auprès de l'écosystème national. Ceci pourrait être porté par les initiatives de la stratégie d'accélération, puisque que cela couvre des aspects allant de la recherche au transfert et en particulier la normalisation. De même, une vision synthétique des initiatives européennes nombreuses sur ces sujets devra être réalisée avec un suivi périodique des évolutions et des tendances. Les pôles de compétitivité numérique pourront utilement en relayer les résultats de ces actions auprès de leurs membres PME et laboratoires académiques.

7.1.3. Faciliter le développement et la mise au point de briques technologiques

- Organiser des appels à projets en cohérence avec les feuilles de route pour des actions de R&D et pilotes fédérant les acteurs de toute la chaîne des infrastructures numériques, y compris les développeurs d'applications et les utilisateurs verticaux, pour constituer des offres différenciatrices avec des modèles économiques pérennes et équilibrés entre acteurs, tout en mutualisant des infrastructures, facilitant les investissements conjoints, favorisant l'interopérabilité et vérifiant la conformité avec les régulations. Là encore, la constitution de consortia à l'échelle du territoire national pourra s'appuyer sur le relais de pôles de compétitivité qui devront contribuer aux mises en relation pertinentes (*via* un annuaire des compétences des laboratoires académiques et PME notamment).

- À l'image des plateformes 5G accompagnées par le CSF au début des déploiements de la technologie, la disponibilité d'environnements de type « bac à sable » souverain sera nécessaire pour que les contributeurs aux briques technologiques (notamment les PME) puissent les valider fonctionnellement mais aussi non fonctionnellement (sécurité, passage à l'échelle, conformité à des règlementations, réponses aux besoins de certification évoqués plus bas…). La gestion de ces bacs à sable nécessitant une offre de service qui devra être confiée à des tiers de confiance selon un business model à bâtir (y compris avec des financements publics pour soutenir le fonctionnement, comme ce fut le cas pour les PPFMI au début des PIA). Ces bacs à sable devront intégrer la mise à disposition de données nécessaires au déploiement d'algorithmes d'IA.
- Le cas spécifique des solutions NTN nécessite sûrement un grand programme structurant (PPP européen) couvrant les solutions satellites et sol pour assurer la mise au point des solutions et des services associés, en lien étroit avec le programme IRIS^2.
- La nécessité de bacs à sable spécifiques, ou de pilotes, dédiés aux usages en lien avec les CSF verticaux pourra être analysée. Des actions de type adaptation réglementaire à des fins de test pourront s'avérer nécessaires.

7.1.4. La certification de conformité

- Compte tenu de leur utilisation au sein des réseaux d'infrastructure, une approche de certification de conformité des briques technologiques (label) et aussi de vérification de la cybersécurité et aux réglementations européennes paraît indispensable pour assurer aux développeurs l'accès aux marchés. Les « bacs à sable » mentionnés au paragraphe précédent peuvent être mis à profit pour cet objectif également. Les bacs à sable réglementaires permettraient aux solutions de l'UE de passer plus rapidement de la R&D à des déploiements évolutifs, avec des outils de transparence tout au long de la chaîne d'approvisionnement pour assurer une conformité conjointe.
- La mise en place d'un centre de certification mutualisé opéré par un tiers de confiance serait un outil utile. Il devrait être certifié à l'image du label OTIC (Open Testing and Integration Center) de l'Alliance O-RAN sur les architectures Open RAN. Ces tiers lieux de certification auront aussi un rôle à jouer dans l'aide à la construction de modèles d'affaires soutenables et acceptables par tous. Dans le même temps, des capacités d'assouplissement à la conformité à certaines réglementations devra être possible (droit à l'expérimentation, à la dérogation).

7.2. Recommandations organisationnelles

Au-delà des facilités de développement et de validation, des actions non fonctionnelles seront à mettre en place sur plusieurs axes :

7.2.1. La coordination entre acteurs européens

- Porter ces questions au niveau Européen pour intégrer aux programmes européens le même type d'initiative et constituer pour les acteurs français des opportunités d'expansion de leur marché et fédérer des consortiums à l'échelle européenne. Outre les programmes de la commission et au-delà de l'Europe, les clusters Eureka (CELTIC

Next sur l'infrastructure numérique et ses services et ITEA sur le logiciel, qui regroupe une puissante communauté sur de multiples secteurs industriels) peuvent être mis à profit, sous réserve de revitaliser drastiquement les possibilités de financement des acteurs français sur des projets Eureka.

- Les structures actuelles de type 6GSNS auront sûrement à intégrer les concepts manipulés dans ce livre blanc. La France devra, proactivement, les faire évoluer mais aussi faire converger les nombreuses initiatives contributrices aux réflexions (Sylva, CAMARA…). France6G devra prendre le rôle d'information des acteurs sur tous ces groupes de réflexion et assurer une forte coordination avec les initiatives européennes pour œuvrer en synergie. Comme cela se dessine sur les infras de type 5G des recommandations européennes seront nécessaires pour contribuer sinon à une totale souveraineté aujourd'hui illusoire au moins à une indépendance maximale et maîtrisée de nos infrastructures de communication.

7.2.2. La cohérence globale des approches portées par les CSF et les filières

Divers concepts évoqués dans ce livre blanc sont communs à d'autres CSF technologiques (cyber, micro-électronique, numérique de confiance…) et contribuent à d'autres CSF orientés usage vertical des réseaux de communication et de l'IA. Il est essentiel de mettre en place les synergies et mutualisations nécessaires à une stratégie nationale et européenne coordonnée. Des groupes de travail communs, des événements communs de partage de connaissance et de réflexion sur les modèles d'affaires à construire seront à mettre en place.

Plusieurs types de partenariats sont envisageables :

- Partenariat inter-CSF (par exemple sous l'égide du CNI), avec les filières « amont » (p.ex. industries électroniques), connexes (p.ex. Logiciels et solutions pour un numérique de confiance) et « aval » (cf. infrastructures numériques et services, notamment services multi-sectoriels). Les thèmes de coopération couplés seront à organiser selon des axes compatibles avec des orientations stratégiques « supra » (Transition écologique, *continuum* innovation et numérisation des écosystèmes, Souveraineté et compétitivité (définitions calibrées pour nos thématiques), Développement des compétences, Attractivité des industries numériques et aval.
- Partenariat bilatéral de CSF (technologies/usages)**.** Il s'agit ici de tester l'appétence puis déboucher sur une convention inter-CSF sur des sujets d'intérêt partagé. En termes opérationnels, les filières stratégiques « aval » à sonder en priorité pourraient être : CSF Solutions industrie du futur, CSF Eau (Services essentiels à l'international), CSF « Nucléaire » CSF Nouveaux Systèmes Energétiques (smart grid de bout en bout), CSF Transformation et valorisation des déchets ; intégrer un volet « connectivité et intelligence » dans leur nouveau contrat : visibilité sur les nouvelles technologies de connectivité (en lien avec les travaux « innovation » du CSF IN), utilisation de la 5G industrielle, connectivité des sous-traitants. On peut imaginer un partenariat entre le CSF IN et une fédération professionnelle en direct.
- Il apparaît intéressant de nouer une alliance partenariale entre le CSF et des pôles (de compétitivité, clusters de R&D) pour mieux couvrir les territoires et les aspects de R&D et utiliser cette alliance sur le plan des coopérations inter filières envisageables. Ainsi il faudrait mandater les pôles pour qu'ils encouragent leurs membres à participer à des

travaux de la filière, avec des bénéfices croisés avec les autres filières (AAP de type croisement filières à promouvoir à l'échelle du SGPI/BPI). En termes opérationnels, les Pôles susceptibles d'être approchés seraient :

  - En Île-de-France : Systematic Paris Région, Cap Digital,
  - En Auvergne-Rhône-Alpes : Minalogic,
  - En Nouvelle-Aquitaine : Alpha-RLH (inclut le pôle radiofréquences photonique basé à Limoges)
  - En Bretagne et Pays de la Loire : Images et réseaux
  - En Provence-Alpes-Côte d'Azur : Aktantis (ex SCS).

- La mise en place d'appel à projets dédiés est structurante pour la mobilisation des pôles qui sont à même de relayer ces opportunités dans leurs écosystèmes.

7.2.3. Les dispositifs de financement publics

Nombre d'enjeux technologiques évoqués dans ce livre blanc doivent bénéficier d'investissements et d'aides publiques pour satisfaire une équation économique soutenable (adaptée) pour les acteurs privés. France 2030 a alloué près de 10Mds de son enveloppe pluriannuelle au numérique. Dans un contexte où l'IA modifie en profondeur les usages et les infrastructures, il est important que ces enjeux bénéficient d'un programme de financement aligné sur les priorités européennes dans une logique de masse critique financière (rapport Draghi et Letta) qui soutienne la vision partagée d'une souveraineté européenne en définition, d'un soutien sur les briques les plus critiques, d'une réévaluation régulière de la santé financière des acteurs souverains, d'assurer que les fournisseurs d'infrastructures européens disposent d'un marché de taille critique et de garder des marges financières sur les plans successeurs de France 2030 et au sein du cadre financier pluriannuel 2028-2034 en négociation pour adresser les ruptures futures dans un numérique en ébullition.

Il est à noter que plusieurs leviers de politique publique mériteraient d'être pris en compte lors des prises de décisions concernant les financements publics.

Il est important d'analyser quel acteur est à l'origine des innovations et à la gouvernance : il est fortement souhaitable que l'organe principal de gouvernance (comité de pilotage, comité technique, majorité des mainteneurs) soit domicilié en Europe, et que les décisions stratégiques ne soient pas prises unilatéralement par des entités non européennes.

Les propositions européennes perdant trop souvent pour des questions d'écosystème et non pas pour des raisons techniques, certains financements devraient soutenir des intégrations, les processus de déploiement et des dynamiques de communauté.

Des efforts considérables sont nécessaires pour favoriser l'entreprenariat technologique, notamment en *deeptech*, et de le soutenir dans la durée, afin d'éviter que les pépites, potentielles licornes, se délocalisent à la recherche de financements ou soient absorbées par des acteurs non européens. Des actions pour faciliter l'accès des jeunes entreprises technologiques aux financements nationaux et européens sont nécessaires, des organisations existent, mais un accompagnement plus adapté, en réseau européen étroit, est nécessaire.

La commande publique devrait être davantage mobilisée comme levier d'adoption, y compris pour les jeunes entreprises, en intégrant des critères techniques exigeants sur la souveraineté de la chaîne de gouvernance, des exigences de localisation des données et du support, des critères environnementaux et de sécurité (NIS2, DORA, RGPD), où les acteurs européens ont un avantage structurel, allotissement favorisant les PME, et publication d'un catalogue de référence des solutions *open source* à gouvernance européenne (étendant la logique du SILL avec des critères d'origine et de gouvernance qu'il n'intègre pas aujourd'hui).

En général, il est largement préférable de financer l'interopérabilité depuis les projets américains vers les projets européens, et non l'inverse, afin notamment d'éviter de renforcer la position du projet américain comme standard de référence.

Les métriques d'évaluation des subventions devraient par ailleurs récompenser les déploiements européens dans le secteur public, la croissance de la communauté de développeurs européens, la réduction de dépendance aux infrastructures américaines.

Il serait utile d'analyser en détail la pertinence de co-financer une véritable Fondation *open source* européenne dotée d'une autonomie juridique, financière et communautaire complète — capable d'offrir aux projets une protection de marque, une gouvernance neutre, une défense juridique et un appui marketing, sans déléguer le contrôle stratégique à des entités américaines. Le Sovereign Tech Fund allemand est un modèle partiel, qui mériterait une montée en échelle européenne et un mandat explicite sur la gouvernance, pas seulement sur la maintenance technique.

7.2.4. La formation

Les initiatives « Compétences et Métiers d'Avenir » (CMA) sur le sujet des réseaux (IMTfor5G+ porté par l'IMT et RIS3 porté par l'Université de Rennes) devront intégrer dans les formations dispensées les concepts évoqués dans ce document qui dépassent très largement ceux des réseaux 5G et 6G et devront faciliter le continuum formation, recherche, transfert, innovation. Les établissements devront aussi disposer d'accès à des plateformes matérielles nécessaires à ces formations (à mutualiser avec les capacités de tests « bac à sable » et certifications évoqués ci-dessus). Il est fondamental de promouvoir les capacités hybrides pour l'intégration trans-domaine et la « pensée Systémique » **:** Des ingénieurs et des scientifiques des données et de l'IA doivent acquérir une compréhension holistique et systémique des infrastructures numériques, capables d'intégrer des agents IA à travers divers systèmes et de comprendre les effets en cascade.

Au-delà des formations aux technologies, les formations aux réglementations européennes applicables (*Digital Service Act*, *Digital Networks Act*, *AI Act*…) seront essentielles. Des formations duales technos/droit européen et national seront à envisager.

Également, des formations aux diverses approches de transfert et à l'entreprenariat s'imposent, en lien direct avec les diverses approches d'accompagnement.

7.3. Compilation des recommandations

Section «

La chaîne technologique et ses enjeux de souveraineté ».

Recommandation n° 1

La conception des briques technologiques stratégiques est un sujet clé pour la souveraineté, il donne par ailleurs lieu à de la propriété intellectuelle. Le soutien au maintien d'une forte capacité de conception des briques technologiques est indispensable.

La sélection des priorités devrait se faire dans le cadre présenté dans la section Recommandations.

L'innovation dans le domaine de la conception des briques technologiques doit être soutenue à la normalisation, notamment dans le cadre des brevets essentiels aux normes.

Les pouvoirs publics devraient mobiliser les financements, notamment dans le cadre d'une initiative globale académique-industrielle, telle que celles financées par la stratégie d'accélération des réseaux du futur dont l'intérêt est indéniable, mais i) dans le cadre plus global des infrastructures numériques et des convergences progressives technologiques et entre filières présentées dans ce document et ii) davantage axée sur la continuité de la chaîne de l'innovation, de la recherche au marché. Cette initiative devrait être focalisée sur des innovations fortes amenant à des différenciateurs de marché significatifs, tout en facilitant le maintien de l'écosystème global nécessaire à l'émergence de ces avancées. La mobilisation cohérente des outils déjà en place (IRT, ANR, dispositif de la stratégie d'accélération, PUI, BPI et régions) est nécessaire *via* une feuille de route innovation partagée.

La commande publique devrait soutenir les industriels français et européens engagés dans ces évolutions et également favoriser l'émergence d'acteurs compétitifs, en visant le long terme pour éviter des délocalisations notamment vers les États-Unis. Des clauses spécifiques de souveraineté des solutions dans les marchés publics et notamment ceux portés par les opérateurs d'importance vitale (OIV) sont de nature à faciliter l'atteinte cet objectif.

La conception des briques technologiques se base fortement sur des avancées scientifiques. Sous l'impulsion des pouvoirs publics, les industriels et les acteurs académiques devraient renforcer leurs collaborations, développer une stratégie coordonnée d'innovation et de participation aux travaux de normalisation et accroître la production de brevets essentiels aux normes afin de renforcer la souveraineté technologique et l'influence européenne. Les PEPR ont permis d'avancer dans ce sens, mais sans financement dédié, des financements devraient viser spécifiquement ces objectifs, avec une initiative co-pilotée par des acteurs académiques et industriels.

La constitution d'un écosystème de recherche et innovation national, s'appuyant notamment sur les pôles de compétitivité à Paris et en région, et partageant une même feuille de route (*via* les stratégies d'accélération concernées), permettrait d'accélérer le processus. Un plan national « infrastructures numériques souveraines et soutenables », partagé entre les structures d'accompagnement de financement qui guiderait les axes de

recherche collaborative des TRL les plus bas aux TRL les plus élevés représenterait un cadre global utile.

Recommandation n° 2

Les convergences technologiques ne produiront pleinement leurs effets que si elles s'accompagnent de l'émergence de nouveaux modèles économiques adaptés. Les pouvoirs publics devraient donc promouvoir et soutenir, au même titre que les innovations technologiques, la conception, l'expérimentation et la diffusion de modèles économiques innovants permettant de structurer de nouvelles chaînes de valeur, de favoriser le partage des investissements et des risques et un partage équitable des bénéfices globaux, ainsi que d'accroître la compétitivité des acteurs européens des infrastructures numériques.

Cela permettrait une plus grande capacité de création de valeur pour les entreprises de divers secteurs d'activité et un meilleur positionnement des citoyens.

Quelques pistes d'action :

- Lancer des appels à projets centrés autant sur l'innovation économique et organisationnelle que sur l'innovation technologique.

- Adapter, lorsque nécessaire, les cadres réglementaires afin de faciliter les coopérations entre filières.

- Soutenir des démonstrateurs intégrant simultanément innovation technologique et innovation économique.

- Organiser des groupes de travail dédiés aux nouveaux modèles économiques, en s'appuyant sur les pôles, les IRT, etc.

- Orienter les appels d'offres publics pour y inclure des clauses de souveraineté et de résilience.

Tout cela devrait mener à ce que les industriels visualisent de manière concrète le potentiel de mise en œuvre de modèles de co-investissement et de partage des risques et des revenus entre acteurs des différentes filières.

Recommandation n° 3

Dans les objectifs réalisables de souveraineté, il est nécessaire d'évaluer les dépendances existantes et de définir des objectifs exigeants mais réalistes, d'évaluer les risques en lien avec les partenaires de confiance et prévoir les moyens pour les réduire, à court, moyen et long terme.

Il est ainsi nécessaire de mettre en œuvre une stratégie de souveraineté fondée sur une gestion dynamique des dépendances critiques. Les pouvoirs publics et les industriels devraient identifier les dépendances technologiques, industrielles et géopolitiques les plus sensibles, définir des objectifs de réduction réalistes et priorisés, et élaborer des feuilles de route à court, moyen et long terme. Cette stratégie devrait s'appuyer sur le développement

d'alternatives françaises et européennes dans les domaines les plus critiques (grâce à des avancées technologiques et un travail en écosystème), sur le renforcement des compétences et de la recherche, ainsi que sur un dialogue permanent entre les pouvoirs publics et les acteurs industriels afin d'anticiper les évolutions géopolitiques susceptibles d'affecter les chaînes d'approvisionnement et d'éviter notamment que des partenaires de confiance d'aujourd'hui soient disqualifiés demain pour des critères géopolitiques qui dépassent le cadre décisionnel des entreprises.

Il faudra en particulier :

- Mettre en place une cartographie régulièrement actualisée des dépendances technologiques et industrielles, avec une approche transversale à toute la chaîne technologique et de valeur.
- Définir, dans un cadre multi-filière, des niveaux cibles de réduction des dépendances en fonction des risques. Le cadre holistique multi-filière est le seul qui permettrait des positionnements efficaces dans ce contexte.
- - S'appuyer sur l'Indice de Résilience Numérique (IRN) pour aider les organisations à réfléchir à leurs dépendances en termes de solutions de communication internes et externes.

Recommandation n° 4

Définir un cadre méthodologique pour aider les entreprises à répondre à des critères de souveraineté dans leurs décisions de conception, d'investissement ou de choix de partenaires de confiance.

Référencer et mettre à disposition les outils méthodologiques existants ou à développer

Développer des méthodes d'évaluation multicritères intégrant les dimensions technologiques, économiques, juridiques et géopolitiques.

Recommandation n° 5

Dans ce document, il a été mis en évidence que les orchestrateurs deviennent des éléments centraux des architectures, en permettant l'adaptation dynamique des infrastructures pour répondre aux besoins des usagers. Faire de l'orchestrateur un levier de pilotage dynamique de la souveraineté des infrastructures numériques. Les orchestrateurs de nouvelle génération devraient intégrer nativement des politiques de souveraineté leur permettant de sélectionner, d'allouer et d'adapter les composants et les ressources (calcul, réseau, stockage, services, données, agents) en fonction du niveau de souveraineté requis par chaque usage. Cette approche permettrait d'assurer le niveau de souveraineté attendu tout en optimisant les performances et les coûts, en évitant le recours systématique à des solutions imposant un niveau maximal de souveraineté lorsque celui-ci n'est pas nécessaire.

Compte tenu du caractère structurant et transversal des orchestrateurs, notamment multisectoriels, il est recommandé de lancer un programme national ou européen de

recherche et d'innovation associant technologies, économie et sciences sociales afin de concevoir les architectures d'orchestration, les mécanismes de décision et les modèles économiques permettant la mise en œuvre opérationnelle de cette souveraineté adaptative. Il est également suggéré de soutenir une conception ouverte des orchestrateurs et le développement de composants logiciels pouvant être intégrés dans différents orchestrateurs.

Il ne s'agit pas de se focaliser sur un composant, mais de concevoir les solutions qui permettront de mettre en œuvre et d'articuler les divers composants et les nouveaux modèles économiques, notamment dans un cadre multisectoriel.

Dans le cadre de l'utilisation de composants *open source* dans ces solutions, il faudra s'assurer que les acteurs européens et français sont en position d'être au cœur du processus de décision sur les contenus de ces composants.

Recommandation n° 6

Les deux composantes du *continuum* numérique, horizontale et verticale, sont complémentaires et doivent être traitées ensemble dans le cadre de la Recommandation #2. Cela requiert la mise en place du cadre général, multi-sectoriel, figurant dans la section Recommandations.

Mettre en place une gouvernance du *continuum* numérique fondée sur les convergences technologiques, économiques et sectorielles. Cette gouvernance devrait dépasser les approches en silos afin d'assurer la cohérence des politiques de recherche, d'innovation, de normalisation, de régulation et d'industrialisation sur l'ensemble de la chaîne de valeur des infrastructures numériques. Elle devrait s'appuyer sur une coordination renforcée des acteurs y compris des secteurs utilisateurs du numérique.

Des synergies fortes entre les deux agences de programme concernées sont donc absolument nécessaires, avec éventuellement la mise en place d'une cellule de coordination spécifique, garantissant la prise en compte des enjeux technologiques, économiques et sociétaux en lien avec la mise en place de ce *continuum*[28].

Recommandation n° 7

Dans le contexte des infrastructures numériques européennes, l'ouverture des réseaux *via* des solutions *open source* constitue un levier stratégique pour garantir l'interopérabilité, accélérer les déploiements et stimuler l'innovation collaborative. En adoptant des standards ouverts, cette approche facilite l'intégration de solutions variées, évite la

[28] Les recommandations 2 et 6 pourraient être fusionnées, mais leur interprétation nous semble plus simple en les gardant séparées et positionnées dans le cadre de leurs sections respectives, l'une sur les briques technologiques et l'autre sur le *continuum* du numérique.

dépendance à des fournisseurs uniques et permet aux acteurs publics, privés et académiques de développer des architectures compatibles et résilientes.

Toutefois, cette ouverture doit être encadrée par une gouvernance forte pour éviter la fragmentation, gérer la compatibilité entre différentes solutions et assurer la sécurité et la pérennité des systèmes.

Si l'*open source* offre de nombreux avantages en termes de contrôle, de flexibilité et de développement d'un écosystème européen, il comporte également des risques importants, notamment en matière de propriété intellectuelle, où la diffusion libre peut compliquer la protection des innovations et des brevets.

De plus, la gestion des vulnérabilités, la normalisation et la coordination restent des défis majeurs, nécessitant une vigilance constante pour éviter que l'ouverture ne fragilise la sécurité ou n'entraîne une fragmentation incompatible avec la souveraineté européenne.

Ainsi, une stratégie claire d'ouverture, associée à une gouvernance européenne rigoureuse, est essentielle pour bâtir des infrastructures numériques souveraines, résilientes et innovantes, tout en maîtrisant les enjeux de sécurité, de propriété intellectuelle et de standardisation.

Il est fortement souhaitable d'analyser plus en détail le besoin d'orienter des financements vers des innovations européennes en avance, ce qui est détaillé dans ce document, d'identifier les briques technologiques pour lesquelles l'*open source* constitue un avantage stratégique et d'élaborer une feuille de route coordonnée entre les initiatives nationales et européennes.

Recommandation n° 8

Pour garantir la souveraineté spatiale de la France et de l'Europe sur le volet critique des infrastructures numériques, plusieurs axes doivent être adressés au travers de la formulation d'un programme tendant à :

- Assurer une autonomie dans l'ensemble de la chaîne de valeur, telle que décrite dans ce document
- Valoriser la complémentarité TN-NTN et l'opportunité de la 5G et de la 6G
- Prendre en compte le secteur aval dans la conception des politiques spatiales, en différenciant les divers besoins : large bande, connectivité d'objets, services critiques, etc.
- Appréhender la dualité civil-militaire de l'espace extra-atmosphérique
- Faire du cadre réglementaire de la LOS (Loi sur les Opértions Spatiales) française un avantage compétitif pour l'industrie européenne.

Une analyse des nouveaux modèles économiques est indispensable ; en effet, le risque est que les acteurs ayant pris des positions fortes dans le cadre des NTN absorbent l'intégralité du marché des télécommunications, en s'appuyant sur les réseaux nationaux pour offrir à leurs clients des services globaux.

Section « Positionnement des acteurs actuels »

Recommandation n° 9

Créer une cellule multidisciplinaire en charge d'analyser les stratégies pour renforcer les opérateurs de télécommunications européens dans leur cœur de métier et dans les ouvertures vers les nouveaux marchés mentionnés dans ce document.

Cela devra passer par une combinaison d'approches : un certain niveau de consolidation, des interactions technologiques plus fortes permettant des fédérations se comportant comme un seul acteur qui passe à l'échelle, notamment dans le cadre de partenariats au niveau européen avec des acteurs d'autres filières : *cloud*, cyber, IA pour des offres consolidées grâce au bon niveau d'interopérabilité technologique et une orchestration dynamique des ressources et des fonctionnalités multi-acteurs, multi-secteurs.

La même cellule devrait analyser le potentiel économique d'une transformation progressive de ces infrastructures convergentes multi-acteurs vers une logique ouverte, de type *Platform as a Service* (PaaS), tel que présenté dans ce document, permettant une bien plus forte création de valeur, à travers l'intégration dynamique de nouveaux composants, proposés par des acteurs tiers, tels que des industriels de divers secteurs d'activité, pour la composition dynamique de nouveaux services. Ces composants pouvant par ailleurs être disponibles sur une place de marché portée par ces infrastructures convergentes.

Cela pourrait enclencher une évolution des infrastructures numériques européennes d'une logique d'infrastructures cloisonnées vers des plateformes ouvertes, interopérables et orchestrées, capables de fédérer des écosystèmes industriels, de soutenir de nouveaux modèles économiques et de piloter dynamiquement des exigences de performance, de résilience et de souveraineté.

Recommandation n° 10

Tel qu'évoqué dans ce document, l'utilisation de l'IA pour la conception, le développement, la planification, l'opération sécurisée et résiliente des infrastructures numériques doit continuer d'être soutenue afin de garantir que la France et l'Europe disposeront des infrastructures nécessaires à permettre le développement socio-économique, du moins à la hauteur de celui prévu dans d'autres blocs. Les outils pour ce soutien existent déjà, il faut pérenniser leur financement.

Au-delà de cela, la France dispose d'atouts permettant le déploiement d'infrastructures disposants de différenciateurs majeurs au niveau global. À titre d'exemple, tel que décrit plus haut, les infrastructures numériques européennes pourraient intégrer un plan de gouvernance données et IA, ce qui représenterait un différenciateur majeur du fait que cela permettrait un déploiement beaucoup plus pertinent et rapide de l'IA agentique distribuée,

y compris multi-acteurs, y compris pour la mise en place de services multisectoriels, tout cela représentant un accélérateur majeur du développement économique.

La gouvernance des données et de l'IA, dont le besoin est aujourd'hui de plus en plus admis comme élément clé pour réaliser tout le potentiel de l'IA agentique, deviendra ainsi une fonction d'infrastructure numérique, transversale donc, au même titre que le calcul, le stockage ou la connectivité. Le lien avec notre recommandation #5 sur les orchestrateurs pour la souveraineté est direct.

Cette piste doit être explorée rapidement, par exemple en créant une cellule multi-filière (réseaux, *cloud*, IA, verticaux) et multidisciplinaire (technologie, économie) et en cas de conclusions positives (ce qui semble évident), la formulation d'une feuille de route pour permettre d'avancer dans un domaine où un leadership global est encore possible.

Recommandation n° 11

Construire une autonomie stratégique européenne sur l'ensemble de la chaîne de valeur des réseaux non terrestres (NTN), ce qui inclut l'embarquement de l'IA.

Pour ce faire, la France et l'Europe doivent soutenir l'émergence des technologies critiques nécessaires aux NTN, et renforcer leur capacité à produire des briques technologiques matérielles clés à ces systèmes : processeurs embarqués, antennes, lanceurs, terminaux et chipsets, technologies optiques inter-satellites (OISL), modems 5G/6G NTN, plateformes matérielles pour l'embarquement simplifié du calcul et de l'IA, etc. Toutes ces technologies ne sont pour le moment pas suffisamment matures en Europe et la dépendance envers les États-Unis, la Corée du Sud ou Taïwan est extrêmement importante. La conception et le savoir-faire technologique doivent donc être préservés et renforcés, et les chaînes de valeur doivent être sécurisées et diversifiées, d'autant plus que, outre les acteurs historiques, des jeunes entreprises se positionnent avec un fort potentiel dans ce secteur, y compris pour l'IA embarquée.

Pour ce faire, la mise en place de programmes spécifiques, notamment en matière de R&D, avec un soutien financier important permettrait de rattraper le retard en la matière et bâtir une réelle autonomie stratégique européenne. Ainsi, il semble essentiel d'assurer une connexion forte avec les initiatives européennes existantes que sont le *Semiconductor Act* et le *Chip Act* afin de capitaliser sur les avancées.

L'Union européenne et la France doivent renforcer leur soutien politique, financier et industriel au programme IRIS². Ce dernier constitue un levier stratégique majeur pour garantir une infrastructure souveraine de télécommunications par satellites. Soulignons l'importance d'infrastructure souveraine pour le besoin *broadband* comme *narrowband* (IoMT, D2D, D2H - *Gov/Defense*). Afin d'éviter la fragmentation des financements, l'Union européenne doit éviter la multiplication de constellations nationales concurrentes au profit d'un programme commun porté par l'écosystème industriel européen dans une optique de souveraineté stratégique, technologique et industrielle et de compétitivité européenne.

Par ailleurs, des outils pour la conception, la planification et le contrôle optimal de ces systèmes doivent être conçus, la France disposant d'une avance certaine dans ce domaine. Ces outils doivent permettre non seulement d'optimiser certaines fonctions clés, comme l'embarquement de l'intelligence ou le routage inter-satellite, mais doivent également permettre d'évaluer les risques de saturation et de collisions, impactant la résilience et la production de déchets dans l'espace, ainsi que d'autres risques écologiques liés notamment à la faible espérance de vie des satellites en orbite basse ou à la pollution visuelle affectant les travaux des astronomes.

Recommandation n° 12

Les réseaux satellitaires et non satellitaires doivent être interopérables pour renforcer résilience, couverture et services critiques. Le passage aux standards 5G NTN (requis pour la constellation IRIS²) et plus tard 6G est un levier majeur pour garantir l'interopérabilité TN/NTN, réduire les dépendances aux solutions propriétaires, et ouvrir le satellite à un marché de masse grâce aux effets d'échelle de la 5G.

La France et l'Europe doivent donc s'impliquer davantage dans la normalisation (notamment 3GPP) et l'ensemble de la chaîne technologique doit être soutenue.

Les initiatives de la stratégie d'accélération, telles que le PEPR réseaux du futur pour la recherche, France6G sur l'implication dans les standards ou FRAMExG pour développer des portefeuilles de brevets essentiels aux normes peuvent être des solutions, si comme souhaité, elles perdurent dans le temps.

La rencontre en mai 2026 entre le Président Macron et le groupe Science 7 (S7) du G7 a souligné l'importance de renforcer la recherche dans le domaine des réseaux non terrestres (NTN) et de consolider davantage les synergies entre les mondes académique et industriel. S'il y a consensus sur le fait qu'une maîtrise scientifique et technologique de ces réseaux est absolument nécessaire aux pays du G7, et en particulier en Europe, au vu des enjeux géostratégiques, il y a aussi consensus sur le fait que la régulation du domaine, et en particulier l'attribution des orbites, est un sujet critique qui requiert de nouvelles bases scientifiques pour la prise de décision[29]. Ces concepts sont détaillés dans le document « Large Satellite Constellations: Perspectives and Challenges ».

La France dispose, dans ce domaine, d'atouts majeurs ainsi que de résultats scientifiques et technologiques différenciants qu'il convient de valoriser pleinement. Les actions menées dans le cadre du PEPR Réseaux du Futur s'inscrivent pleinement dans cette dynamique et méritent d'être pérennisées au-delà de l'échéance du programme afin de consolider les acquis et d'amplifier leur impact.

[29] Notamment en fonction de l'évaluation de la capacité de support de ces ressources orbitales (problème des collisions), de l'évaluation des interférences optiques et radio (astronomie, communications terrestres), et de l'évaluation des transformations de la chimie de la haute atmosphère qui découle des lancements et des rentrées de satellites.

Recommandation n° 13

Au niveau politique, les opérateurs et autres acteurs aval (services, IoT, applications) doivent être intégrés à la conception des politiques spatiales, afin d'éviter un déséquilibre entre investissements industriels amont et besoins réels du marché. Au niveau économique, il est essentiel de rééquilibrer la répartition des revenus entre les acteurs qui financent et déploient les infrastructures et ceux qui en génèrent de la valeur, de manière à garantir un modèle durable et équitable pour l'ensemble de la chaîne.

Recommandation n° 14

Les frontières entre usages civils, commerciaux et militaires des applications spatiales s'estompent : les constellations commerciales sont utilisées à des fins militaires, et sont régulièrement ciblées ou brouillées. Pour rester compétitive, l'Europe doit adopter une approche duale et intégrée, afin d'optimiser l'utilisation des ressources civiles et militaires, en favorisant les constellations à double usage et en s'appuyant sur des partenariats public/privé puissants, comme le font les États-Unis.

Il faudrait mettre en place un pilotage stratégique européen, éventuellement de type PPP (comme 6GSNS) dual civil/défense qui soit en charge de la gestion du projet, de l'émergence des standards nécessaires, de l'organisation des programmes de R&D nécessaires et de la stratégie de partage public/privé des usages, de la vision de bout en bout (segments sols inclus).

Recommandation n° 15

Le futur cadre européen (*EU Space Act*) doit harmoniser au sein de l'Union le niveau d'exigence de la LOS française en matière de prévention et de gestion des débris spatiaux, de gestion du trafic spatial, et de durabilité des activités spatiales, afin d'interdire les pratiques de « *dumping* » réglementaire, de garantir des conditions de concurrence équitables entre acteurs, et donc de renforcer la compétitivité des opérateurs français. L'accès au marché européen par des opérateurs extra-européens doit par ailleurs être conditionné au respect des mêmes normes.

Recommandation n° 16

La France dispose de compétences au meilleur niveau international dans le domaine de la cybersécurité et d'acteurs bien positionnés sur certains secteurs. Ceux-ci doivent être soutenus dans leurs efforts d'innovation pour répondre aux changements de paradigme évoqués dans ce document et maintenir un positionnement fort.

Il est donc nécessaire d'intégrer les acteurs du secteur dans les diverses initiatives proposées dans les recommandations précédentes.

Les transformations mentionnées dans ce document représentent une opportunité pour l'émergence de nouveaux acteurs, ce qui requiert également une stratégie nationale et un soutien fort, notamment en lien avec la croissance des budgets militaires.

Des acteurs de la sécurité intérieure et de la sécurité extérieure doivent donc également intégrer les initiatives proposées.

La France est également forte dans le domaine du quantique, que ce soit dans l'utilisation de quantique pour la distribution des clés (QKD) ou sur la sécurité post quantique (PQC, comment sécuriser les systèmes à l'ère où le quantique peut affaiblir considérablement les méthodes de cybersécurité actuelles).

Deux sujets d'innovation sont ici à soutenir particulièrement dans les programmes à venir : la conception jointe QKD-PQC et les réseaux quantiques (sujet qui par ailleurs dépasse largement la cybersécurité et qui couvre en particulier le calcul quantique distribué).

Recommandation n° 17

Promouvoir une action européenne pour éviter le risque de l'émergence d'une couche de cybersécurité propriétaire, pilotée par les grands acteurs du *cloud* et de l'IA générative et traduire dans les divers *« Act »* cette vision non-propriétaire de la cybersécurité des infrastructures numériques.

8. Contributeurs

Ce document a été rédigé par un sous-groupe de travail du groupe de travail innovation du comité stratégique de filière animé par Arnaud Vilain (Orange) et Gaël Roger (FFT). Sa rédaction a été coordonnée par Daniel Kofmant (IMT et PEPR Réseaux du Futur) et Gérard Le Bihan (I&R).

Les contributeurs et relecteurs ont été :

ACOME

- Philippe Rossier

Airbus

- Oriol Vidal
- Marie Dunyach

Arcep

- Amanda Alvès
- Patrick Lagrange

Abilian

- Stéfane Fermigier

CEA

- Dimitri Ktenas, en représentation du PEPR Réseaux du Futur

CNRS

- Serge Verdeyme, en représentation du PEPR Réseaux du Futur

DGE

- Thomas Orazio
- Oumaima El Bouhmadi
- Éric Berner
- Domitille Legrand
- Julien Talagrand

Ericsson

- Victor Ardvisson

Eutelsat

- Noan Renault
- Étienne Lesoeur
- Daniele-Vito Finocchiario

- Fabien Buleux

Hub One

- Ollivier Mellina

Images & Réseaux

- Gérard Le Bihan

Institut Mines Télécom

- Daniel Kofman
- François Bacelli

Laforge

- Arnaud Muller, en représentation du CSF « Logiciels et Solutions Numériques de Confiance »

NOKIA

- Bogdan Uscumlic
- Makram Bouzid
- Nicolas Le Sauze
- Samuel Dubus
- Jérémie Leguay
- Olivier Audouin

Open source expert

- Cédric Ravalec

Orange

- Marianne Mohali
- Nicolas Homo
- Arnaud Vilain

Probal

- Yann Lechelle, en représentation du CSF « Logiciels et Solutions Numériques de Confiance »

Thalès

- Emmanuel Dotaro

Annexe I : une vision d'ensemble des transformations en cours

Nous reprenons ici l'article « Des services réseaux aux plateformes du numérique et aux services multisectoriels », signé par Francis Jutand (Conseil Général de l'Économie) et Daniel Kofman (Télécom Paris), publié en septembre 2024 dans la série **Quelles infrastructures numériques du futur ?** Ce numéro a été coordonné par Francis Jutand et Daniel Kofman.

Nous rentrons dans une nouvelle phase de la transformation numérique. Dans la continuité d'une transformation en silos, par secteur d'activité, nous passons à une phase qui ouvre la voie aux services multisectoriels, transversaux aux divers verticaux. L'énorme potentiel de création de valeur est identifié et ne cessera de se développer vu le potentiel d'innovation qui est ainsi ouvert ; les risques pour les acteurs et pour la souveraineté des pays sont multiples. Cette évolution est rendue possible par une série de nouveaux paradigmes, dont la *softwarisation* et virtualisation des infrastructures, la convergence progressive entre les réseaux et le *cloud*, l'évolution des interfaces, les jumeaux numériques et l'IA, ainsi que l'ouverture des réseaux et systèmes aux acteurs externes. Ce dernier point transforme les infrastructures du numérique dans des plateformes de services, permettant à ces derniers d'être conçus et établis en temps réel, en orchestrant des composants d'acteurs multiples, pour répondre dynamiquement à des besoins spécifiques et évolutifs.

Nous présentons dans cet article une vision intégrée de ces diverses évolutions.

Mots clés/Keywords : services multisectoriels, ouverture des réseaux, nouvelles architectures, nouvelles géographies des acteurs du numérique.

Réseaux et verticaux, un changement de paradigme

Les générations successives des réseaux mobiles ont historiquement poursuivi comme objectifs majeurs l'augmentation de la capacité, des débits et de la couverture, à des coûts rendant économiquement rentable leur déploiement. Avec l'avènement de la 5G, un changement de paradigme est introduit : la conception partiellement synergétique avec divers secteurs d'activité, tels que les transports et l'industrie du futur (mentionnons par exemple les initiatives *5G Automotive Association, 5G Alliance for Connected Industries and Automation* et *Software Republic*).

De manière simplifiée, nous sommes passés d'une logique où les réseaux étaient conçus et déployés, puis le marché décidait « quoi en faire », à une logique dans laquelle un travail sur les possibles cas d'usage est réalisé très en amont et avec une participation directe de divers secteurs d'activité. Il en ressort des spécifications fonctionnelles et non fonctionnelles mieux adaptées aux besoins réels de ces secteurs.

Ainsi, les divers secteurs d'activité ne se limitent plus à être des utilisateurs des réseaux, mais deviennent des partenaires technologiques de ceux en charge des infrastructures numériques.

Les réseaux véhiculaires en tant qu'extension d'un réseau d'infrastructure représentent un exemple bien connu. Par ailleurs, les réseaux dits *à l'edge* (au bord) deviennent progressivement une partie intégrante des infrastructures du numérique.

Nous verrons par la suite que les interactions technologiques entre les réseaux et divers verticaux se diversifient fortement avec les nouvelles générations de réseaux, donnant lieu à des évolutions majeures d'architectures, de services et de modèles économiques. Cela est encore plus significatif dans le cadre des réseaux privés ; ces derniers étant un des atouts clés pour la diffusion de la 5G et des réseaux du futur en général.

Cette interpénétration accrue se traduit par une dépendance fortement croissante des divers secteurs d'activité vis-à-vis des infrastructures du numérique, imposant sur celles-ci de nouvelles contraintes, notamment en termes de sûreté et de sécurité, mais également en termes de flexibilité (création automatique et dynamique de réseaux dans le cadre de systèmes virtualisés) et de latence (notamment dans le cadre du contrôle de sites industriels).

Convergence réseaux-*cloud*, MEC

En 2012, un groupe de 13 opérateurs de télécommunications, dont Orange, ont publié un livre blanc[30] qui introduit le concept de virtualisation des fonctions réseau (NFV pour *Network Functions Virtualization*). Ce document a représenté en quelque sorte la validation de concepts qui étaient déjà étudiés, mais dont on doutait fortement de leur acceptabilité massive par ces acteurs.

Historiquement, les équipements de réseau de télécommunications ont été construits comme des solutions *hardware*, spécifiques à chaque constructeur et comme des boîtes noires. Cela présente de nombreux inconvénients : les difficultés et délais pour introduire de nouvelles fonctionnalités, le coût élevé et la dépendance technologique. Certes les réseaux sont standardisés, mais en fait seules les interfaces entre grands blocs fonctionnels le sont.

Le document mentionné, partiellement motivé par le grand succès des centres de calcul appelés *data centers*, capables d'implémenter avec flexibilité une multitude de fonctionnalités, services et applications, préconise le remplacement des équipements dédiés par un *hardware* générique (serveurs informatiques) et l'implémentation software des fonctionnalités réseaux.

La *softwarisation* des réseaux, est ainsi formalisée et fortement accélérée.

En conséquence, d'une part, de très nombreuses fonctions réseau sont aujourd'hui offertes en mode *cloud*, y compris pour la radio (*cloud-RAN*) et ce phénomène s'accélère. D'autre part, le *cloud* sort des grands *data centers* pour se disséminer jusqu'aux extrémités (le terme *edge* est utilisé dans la littérature) et notamment au niveau du MEC (*Mobile Edge Computing* ou *Multi-access Edge Computing*), permettant de nombreuses nouvelles applications, notamment celles sensibles à la latence ou nécessitant une protection particulière des données. Cela joue un rôle central dans les interactions avec les verticaux mentionnées plus haut. Le terme *edge* tel qu'utilisé dans ce contexte fait référence, soit à des points de présence des réseaux proches des clients finaux (bien plus proches que les grands *data centers*), ce qui est le cas du MEC, soit à des équipements côté usager, comme des terminaux, des voitures ou autres objets connectés.

[30] Network Functions Virtualization - An Introduction, Benefits, Enablers, Challenges & Call for Action.

L'ensemble de ces évolutions prises conjointement nous font parler de convergence ou interpénétration réseau-*cloud*. L'utilisation du paradigme *cloud* dans les architectures de réseau permet à ces derniers d'introduire une très grande agilité et flexibilité, et le déploiement de ressources *cloud* dans les points de présence des réseaux permet aux clouds une grande diversité de nouvelles applications et usages.

Cette convergence facilite la mise en œuvre de diverses solutions réseaux, telles que le *slicing*, c'est-à-dire, la capacité de partitionner les réseaux en attribuant des parties (*slices*) à différents clients. Ce concept général ne diffère en principe pas trop du concept historique de réseau privé virtuel, mais ici la flexibilité est totale, chaque *slice* pouvant avoir des propriétés fonctionnelles et non fonctionnelles qui lui sont propres et avec la possibilité de faire évoluer dynamiquement et en temps réel les fonctions qu'il comporte et les ressources qu'il utilise.

Tout cela est possible grâce à la virtualisation des fonctions, qui de ce fait peuvent être ajoutées, éliminées ou déplacées dynamiquement. En effet, les fonctions, devenues purement logicielles et tournant sur du *hardware* générique, ne sont plus enfermées dans des boîtes noires.

Par ailleurs, les évolutions mentionnées plus haut sont un facilitateur majeur pour l'ouverture des réseaux. Cette ouverture se met en place de deux manières principales. Dans la première approche, les architectures des réseaux deviennent potentiellement plus ouvertes permettant à une diversité d'acteurs de proposer des composants de réseau et aux opérateurs de construire leur réseau en déployant et interconnectant des composants de fournisseurs différents. C'est le cas notamment des solutions Open RAN. Dans la deuxième approche, les réseaux proposent des interfaces, notamment des API, qui permettent à d'autres acteurs de contrôler une « partie » du réseau, typiquement celle qui leur est attribuée, notamment dans le cadre du *slicing*. Ce concept se généralise et introduit de nouveaux changements de paradigme, comme nous le verrons dans la section suivante.

Un élément clé des architectures ainsi définies est l'orchestrateur, l'intelligence qui permet à chaque instant d'identifier les fonctionnalités nécessaires, de les agencer et de leur attribuer les ressources dont elles ont besoin.

Toutes ces évolutions sont en cours, mais sont loin d'avoir abouti malgré leur intérêt certain. Une des raisons est que même si la technologie répond plutôt bien aujourd'hui aux besoins de convergence mentionnés (dans des cadres restreints qui ne couvrent pas les évolutions à venir présentées plus bas), les filières industrielles concernées se trouvent dans une situation de concurrence de plus en plus forte et de ce fait ont du mal à trouver les moyens et le temps pour opérer une plus forte convergence, qui prenne en compte notamment de nouveaux modèles d'affaires ; nous y reviendrons plus loin dans ce chapitre.

Des services réseaux aux plateformes du numérique

L'étape suivante dans l'ouverture mentionnée plus haut consiste dans la possibilité pour des acteurs tiers de déployer leurs propres composants dans les infrastructures convergentes

réseau-*cloud*. Ces fonctionnalités, développées par des tiers et déployées à travers des APIs[31], portées ainsi par les infrastructures convergentes réseau-*cloud*, sont notamment en lien avec des services (de tout type, pas uniquement services réseau) et des applications fournies également par des acteurs tiers, pas nécessairement les mêmes que ceux qui déploient les fonctionnalités.

L'ouverture du cœur de réseau pour accueillir de telles fonctionnalités rend même possible l'émergence d'une *marketplace* de ces fonctionnalités déployées sur les infrastructures que nous traitons et ouvre ainsi de nombreuses opportunités et des risques importants.

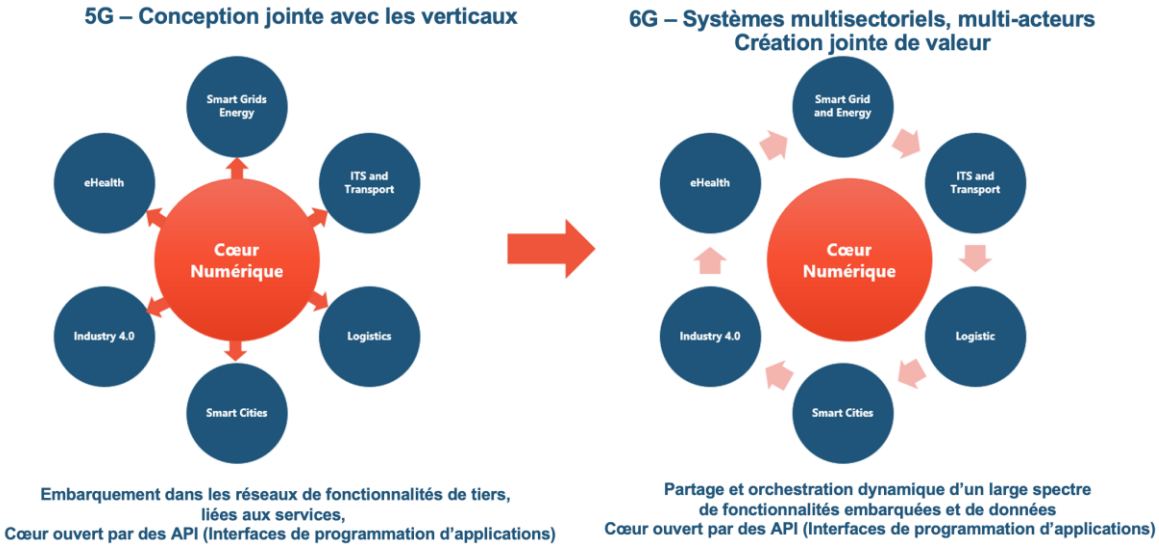
L'idée générale, posée de manière « caricaturale », serait de voir les infrastructures convergentes réseau-*cloud* comme un PaaS (*Platform as a Service*) qui accueille de nouvelles fonctionnalités, de divers acteurs tiers, permettant de construire dynamiquement, à la demande, de nouveaux services et applications. Toute la chaîne, en partant du réseau lui-même, pouvant être construite à la demande et en temps réel.

Ce type de solutions est aujourd'hui plus prospectif, mais envisageable dans un horizon de 5 à 8 ans. Néanmoins, des verrous sont à lever, notamment dans la conception de nouveaux types d'orchestrateurs, dans la conception de mécanismes de validation des propriétés des composants acceptés dans la *marketplace*, dans la spécification des niveaux de qualité sur divers critères à exiger de ces composants, etc.

Vers les services multisectoriels

Indépendamment des évolutions que nous venons de mentionner, une autre transformation se met en place. La numérisation, qui jusqu'à présent s'est faite en silos, par secteur d'activité, passe à une nouvelle phase, avec l'avènement de services multisectoriels. Dans ce cadre, des acteurs de secteurs d'activité différents collaborent pour développer conjointement des services fortement innovants s'appuyant sur les services et les données de chacun, tout en gardant la maîtrise de leurs données et infrastructures. Selon les modèles économiques choisis, ils peuvent aussi être en « coopétition ». L'image suivante contient une représentation graphique de ces concepts.

[31] API : *Application Programming Interface.* L'idée principale d'une API est qu'elle permet à des acteurs externes d'interagir avec le système qui la propose sans savoir comment ce système est conçu et implémenté. Ces interactions peuvent être de multiples niveaux, tels que la demande d'une construction à la demande d'un réseau virtuel ou plus simplement l'activation d'un service simple, par exemple de messagerie.



La convergence réseau-*cloud* et l'ouverture des réseaux au travers des API mentionnées plus haut représentent clairement des facteurs d'accélération de cette tendance émergente.

Ici encore, les verrous sont multiples. Du point de vue technologique, l'orchestration dans un cadre multi-sectoriel pose de nouveaux problèmes. Pour les lecteurs familiers de l'architecture de l'Internet, on peut faire l'analogie avec l'introduction du routage externe, multi-systèmes autonomes. Notamment, les choix technologiques deviennent extrêmement dépendants des modèles d'affaires potentiels entre acteurs. À la différence du routage Internet, nous sommes ici face à une très grande diversité d'acteurs, de fonctionnalités à orchestrer, de contraintes à prendre en compte (notamment en lien avec l'accès aux données) et surtout à un ensemble d'acteurs et de fonctionnalités qui varie en permanence. La garantie de la qualité de service de bout en bout, le respect de bout-en-bout des politiques de sécurité et de protection des données de chaque acteur impliqué, le respect de leurs politiques en termes d'impact environnemental et de sobriété énergétique, ne représentent que quelques-uns des défis à affronter.

Face à cette explosion de la complexité, des approches de conception, planification, opération, contrôle, maintenance, etc. basées sur de l'intelligence artificielle et l'utilisation de jumeaux numériques sont en cours d'étude, mais encore dans des stades très embryonnaires. Le lecteur intéressé est invité à lire le chapitre 25 du document des annales. De plus, une prise de conscience commence à apparaître concernant la surestimation du potentiel de l'IA et même de l'IA générative, et plus précisément de la capacité à trouver des modèles d'affaires permettant de faire face aux coûts engendrés par cette IA. Un article du 20 juin 2024 évalue que l'industrie de l'IA devrait générer un chiffre d'affaires annuel de 600 milliards de dollars pour être rentable[32] et fait référence à une potentielle bulle autour de l'IA. Même si ceci concerne surtout la course au gigantisme des modèles généralistes, les IA génératives

[32] AI's $600B Question, Sequoi, juin 2024.

spécialisées pourraient être également impactées par un nouveau retournement de situation dans le financement de l'IA.

Nous sommes donc dans un cadre général qui permet de clairement identifier la voie, vu les avantages indiscutables des solutions décrites, mais dont il est très difficile d'évaluer les horizons de temps auxquels des solutions stables seront disponibles.

Convergence réseau-*cloud*, Ouverture et Hyperscalers, un futur incertain

L'ensemble des évolutions mentionnées dans les paragraphes précédents pose de manière encore plus centrale la question des investissements et du partage de la valeur entre les filières historiques et notamment entre opérateurs de télécommunications et hyperscalers. Depuis plus de 20 ans (Google par exemple a été créée en 1998 et le premier iPhone date de 2007), cette question du partage de la valeur est soulevée par les opérateurs qui sont les principaux investisseurs dans les infrastructures de réseaux qui supportent les services des hyperscalers. Ils disposent ainsi du contrôle de ces réseaux et des ressources confortables de communication associées. Les évolutions mentionnées risquent de réduire fortement leur positionnement clé dans la chaîne de valeur. Si nous ajoutons à cela les investissements des hyperscalers dans des câbles sous-marins de très grande capacité, la croissance forte du marché des réseaux non terrestres (avec notamment les constellations de satellites en orbites basses et moyennes) avec la concurrence accrue qui se dessine dans ce domaine et la multiplicité d'opérateurs de télécommunications en Europe qui se traduit par le fait que les entreprises en question ont un poids financier limité (en comparaison aux autres acteurs mentionnés), les risques pour les opérateurs de télécommunications, mais aussi pour les équipementiers fournisseurs historiques de ces derniers, sont évidents.

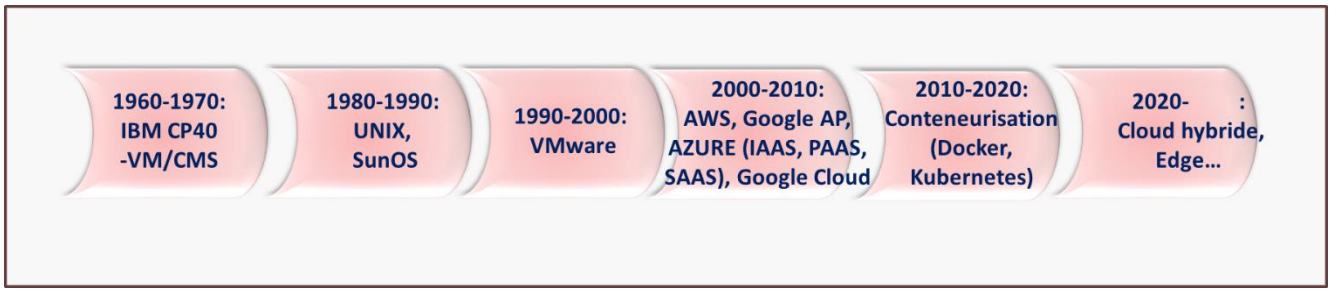
Mitiger ces risques impose une vision holistique des acteurs impliqués, des évolutions technologiques, des nouveaux modèles d'affaires, de la réglementation, etc. Les décisions sont difficiles : la *softwarisation* des réseaux a des avantages notables pour les opérateurs, mais elle les rend plus vulnérables aux positionnements d'autres acteurs. De même, l'ouverture des réseaux, à la mode Open RAN, est d'intérêt pour les opérateurs, mais met en risque le positionnement des constructeurs, qui néanmoins n'ont pas le choix et doivent suivre. L'IA semble *a priori* un moyen clé pour la maîtrise de la croissance très rapide de la complexité, mais elle a ses propres défis et un risque de ralentissement dans les investissements. Le multi-sectoriel est une voie de forte création de valeur, très probablement la prochaine phase de la transformation numérique, mais la disposition des acteurs pour y avancer n'est pas claire et les modèles économiques pour accélérer les processus sont à définir.

Dans ce cadre, de nouvelles formes d'organisation de l'écosystème pourront éventuellement émerger, ouvrant la porte à des rôles nouveaux, facilitateurs des relations technologiques ou économiques entre les parties prenantes.

Tout ceci accroît de manière notoire les enjeux autour de la souveraineté numérique, voire de la souveraineté tout court, compte tenu l'imbrication croissante du numérique avec tous les secteurs d'activité. Une réflexion de fond, globale, multipartite semble s'imposer dans l'intérêt de tous à moyen terme et cela même si la pertinence et les modalités ne semblent pas évidentes à court terme.

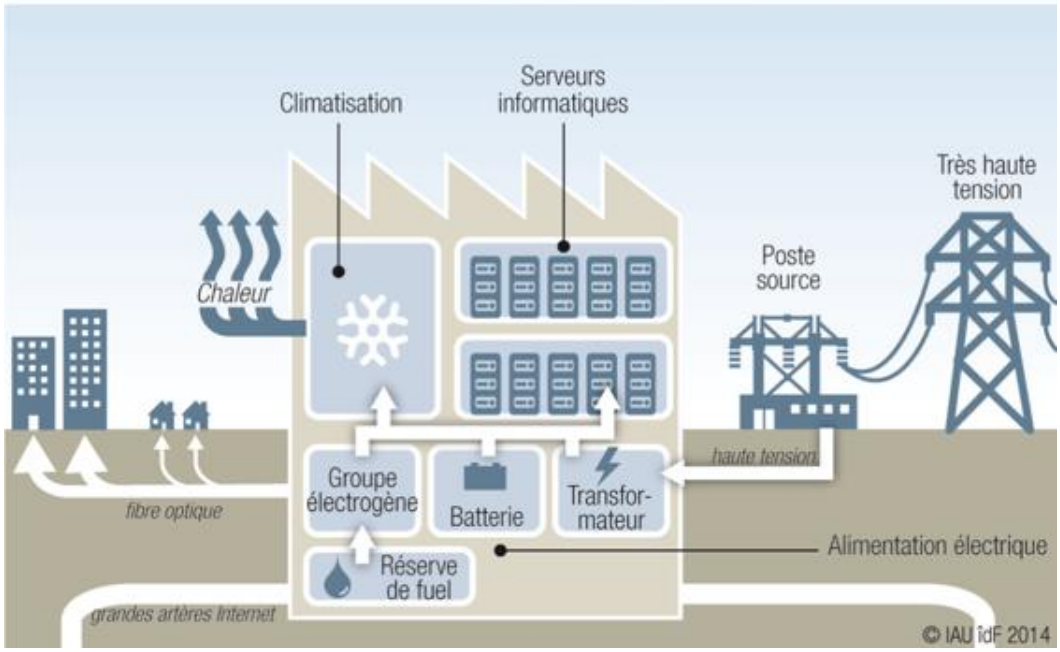
Annexe II : une vision des chaînes de valeur en jeu et de leurs acteurs ainsi que des alliances

Plusieurs chaînes de valeur sont parties prenantes des solutions envisagées sur les futures architectures des infrastructures numériques. La virtualisation est un facilitateur clé de ces architectures. Ce n'est pas une nouveauté et elle a connu des évolutions majeures au cours des dernières décennies :



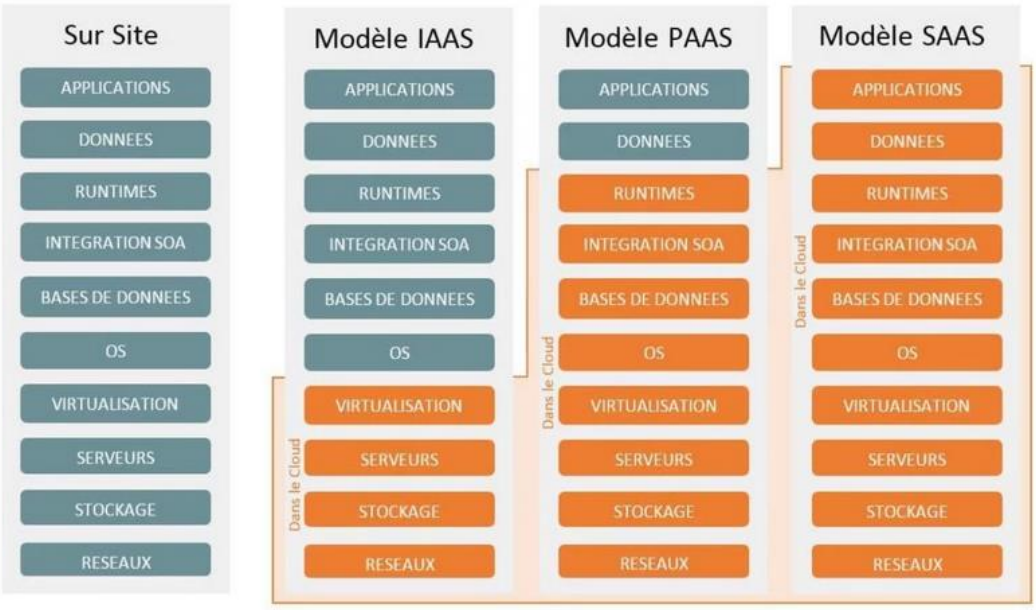
Les environnements de type *data centers* ne se limitent pas aux seuls serveurs informatiques, ils nécessitent plusieurs acteurs (intégration, gestion sécurisée de l'énergie, évacuation de la chaleur…).

Les composants fonctionnels d'un *data center*



Au cours du temps des notions de structuration du niveau des services rendus par ces infrastructures ont été imaginées :

- IaaS (*Infrastructure as a Service)* : le niveau d'exécution le plus basique incluant le matériel
- PaaS (*Platform as a Service*) : fonctions logicielles communes permettant le partage entre applications
- SaaS (*Software as a Service*) : accès partagé à des applications

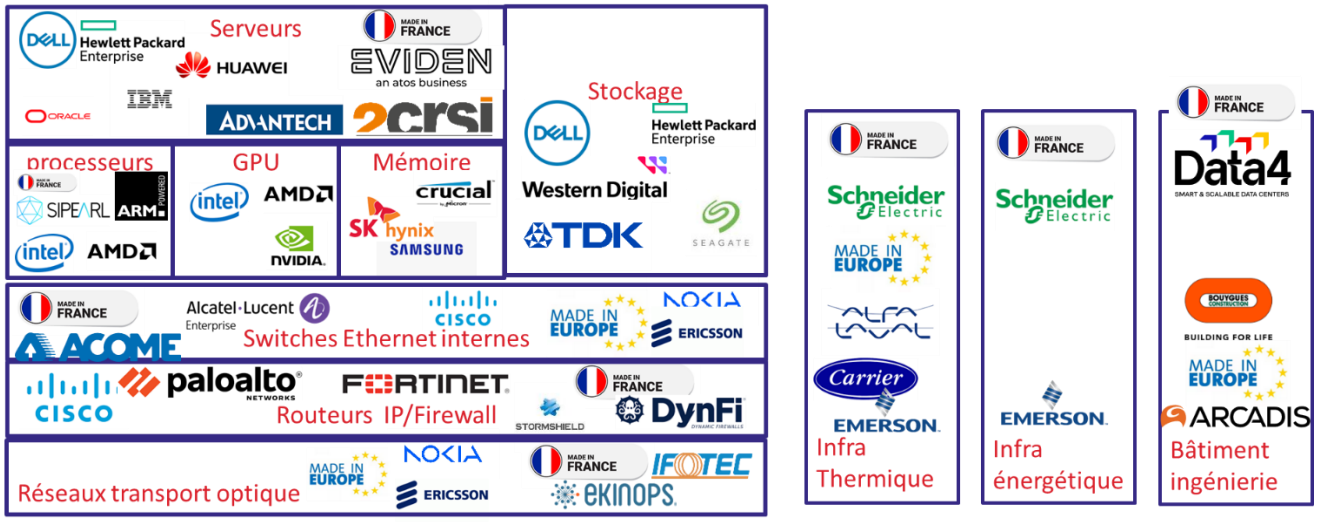


Les constituants

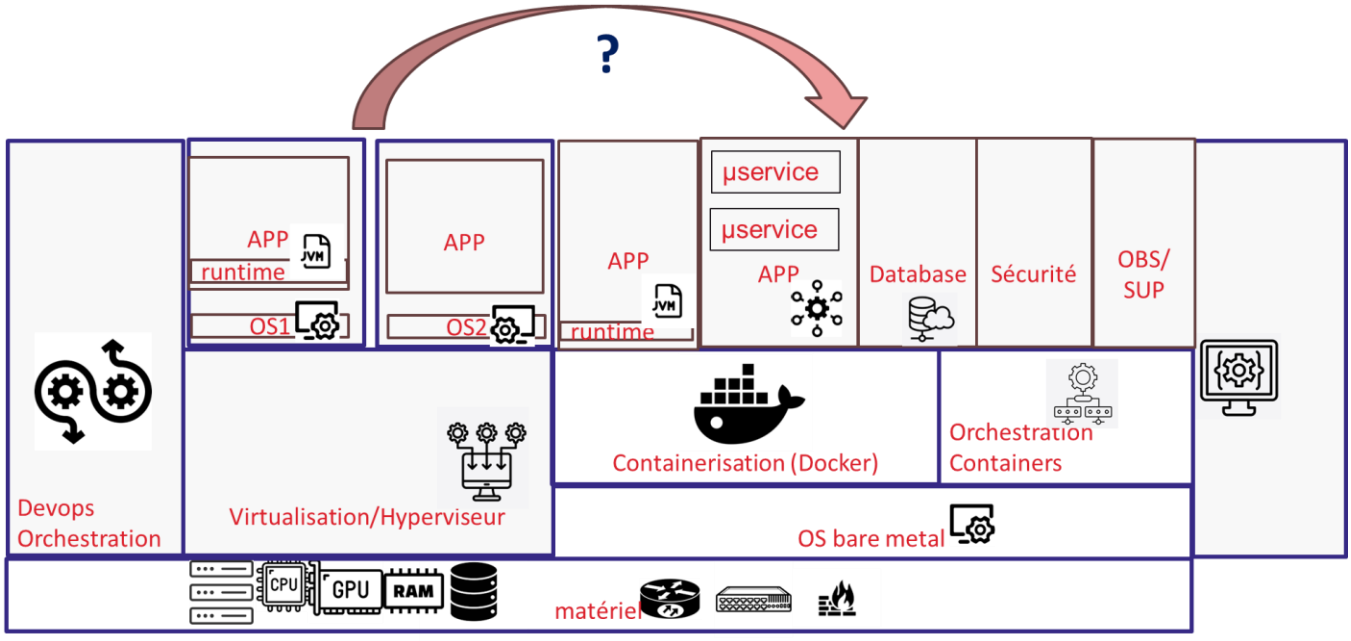
Les briques matérielles constitutives de ces infrastructures sont aujourd'hui largement dominées par des acteurs hors Europe :

- SERVEURS : Processeurs, GPU, Mémoire.
- Stockage : disques.
- CONNECTIVITE : Routeurs, Firewall, Switches Ethernet, Accès réseaux de transport optique (avec des acteurs européens et français).
- SECURITE : transverse.

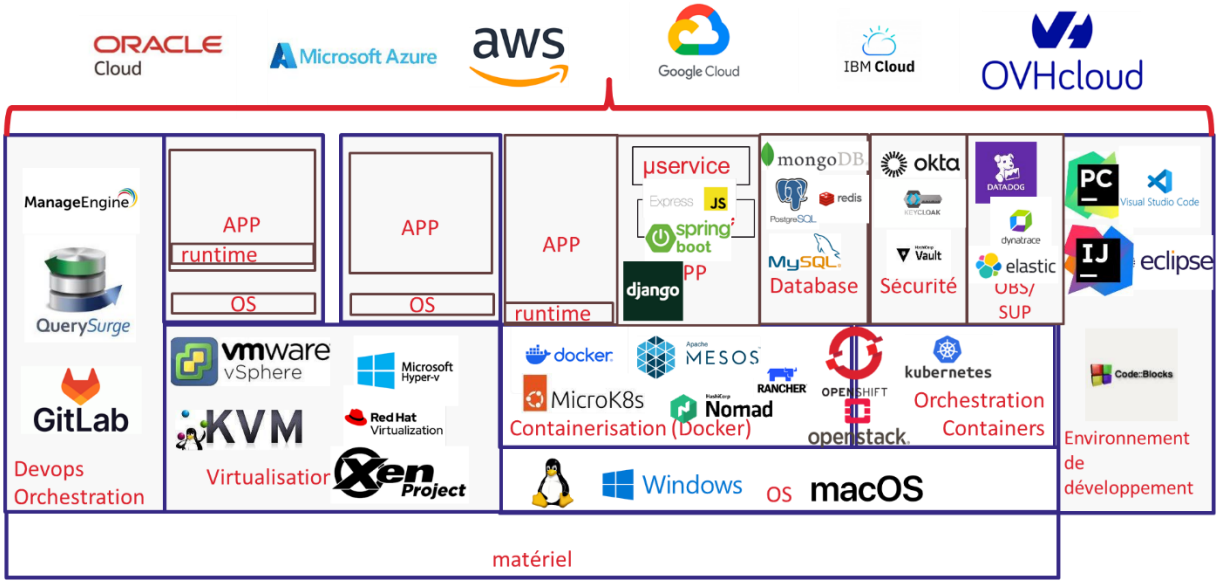
Du côté des intégrateurs et des environnements spécifiques (énergie, climatisation) quelques acteurs européens et français sont actifs.



Les briques logicielles permettant les différents types de déploiement cités plus haut sont souvent issues de composantes *open source* en général produites ou pour le moins maitrisées par des acteurs d'outre-Atlantique avec des rachats récents importants par des acteurs clés (IBM, Google…) :



Les principaux logiciels :



Beaucoup d'*open source* sont utilisés :

- Kubernetes : orchestration de conteneurs.
- OpenStack : gestion IaaS, calcul, stockage et mise en réseau.
- Docker : conteneurisation d'applications.
- Terraform : Infrastructure as Code pour la gestion de ressources (langage déclaratif compatible AWS, Google Cloud, Azure…).
- Ansible : automatisation de la gestion des configurations.
- Ceph : stockage distribué (objet, bloc et fichier).
- Prometheus : surveillance des ressources et gestion des métriques.
- Apache CloudStack : Gestion IaaS.
- Grafana : visualisation et monitoring (dashboards et alertes).
- OpenNebula : gestion de *cloud* privé.
- MinIO : stockage objet dans un monde AWS.
- Vagrant : gestion VM des environnements de développement.

Les mastodontes du domaine offrent en général plusieurs solutions par exemple Kubernetes ou Openstack pour les environnements de containerisation.

Les partenariats et les alliances

Face aux leaders du *cloud* des solutions souveraines voient progressivement le jour (parfois avec des partenaires US), ainsi en France :

- Bleu : Capgemini, Orange et Microsoft
- S3NS : Thales et Google
- Scaleway : filiale du groupe Iliad
- Outscale : filiale Dassault Systèmes
- Numspot : Banque des territoires, Docaposte, 3DS Bouygues (IaaS outscale)
- OODRIVE, Clever Cloud, OVH Cloud, OBS…

Equipementiers comme opérateurs ont aussi mis en place des partenariats avec les leaders du *cloud* pour travailler le sujet de la convergence réseau/*cloud*. Ainsi Orange travaille avec AWS, Google, Microsoft tout comme Thalès et Ericsson, Nokia y a rajouté IBM. Des expérimentations sur des preuves de concepts de réseau (5G) déployés sur ce type d'infrastructure ont concerné plusieurs opérateurs européens :

Par ailleurs plusieurs initiatives multi-acteurs se sont mises en place pour accompagner les développements des nouvelles architectures

1. Open RAN : pour transformer les réseaux mobiles en introduisant des composants ouverts et interopérables *via* :
    a. Innovation et compétition accrues en ouvrant les interfaces et en standardisant les protocoles,
    b. Flexibilité et agilité pour les opérateurs pour le choix de solutions adaptées aux besoins spécifiques et de déploiement des réseaux plus flexibles et réactifs
    c. Réduction des coûts en permettant l'utilisation de composants provenant de différents fournisseurs,
    d. Sécurité et souveraineté des réseaux conformes aux réglementations locales en matière de sécurité et de confidentialité des données
    e. Adaptabilité aux besoins variés (Internet des objets (IoT), conduite autonome, réalité virtuelle/augmentée…)
    f. Acteurs français : Orange, Airbus, Thalès, Ericsson, Nokia, IMT, Eurecom, AW2S, Obvios

2. Sylva (Linux Foundation) : pour standardiser et simplifier l'infrastructure *cloud* pour les opérateurs de télécommunications *via* :
    a. Interopérabilité des opérateurs et fournisseurs de fonctions réseau
    b. Souveraineté et sécurité (données et services conformes aux réglementations locales
    c. Efficacité énergétique des infrastructures *cloud*
    d. Flexibilité et rapidité : Faciliter le déploiement rapide et flexible des applications réseau (*Container as a Service* (CaaS))
    e. Acteurs français : Orange, Ericsson, Nokia

3. OpenAPI est une spécification standard (ex-Swagger) qui permet de décrire des API REST de manière lisible à la fois par les humains et les machines.
    a. Elle facilite la documentation, l'automatisation, le test et l'interopérabilité des API.
    b. Avantages de l'usage d'OpenAPI pour les opérateurs

        ✓ Standardisation : format commun et ouvert.

        ✓ Interopérabilité : facilite les intégrations B2B et B2D.

        ✓ Automatisation : génération automatique de SDK, mocks, tests, CI/CD.

        ✓ Adoption développeur : accès simplifié à des fonctions réseau complexes.

    c. Acteurs français : Orange, Ericsson, Nokia

4. CAMARA (Linux Foundation) est une initiative ouverte visant à simplifier l'accès aux capacités des réseaux de télécommunications *via* des API (CAMARA utilise la démarche OPENAPI) pour :
    a. Permettre une intégration transparente et sécurisée des applications avec les réseaux xG
    b. Garantir une expérience utilisateur fluide et soutenir la portabilité des applications à travers différents réseaux et pays
    c. Faciliter la programmabilité et l'automatisation du réseau
    d. Exposer des capacités réseau *via* des API ouvertes e.g.
    e. La localisation,
    f. La qualité de service (QoS)
    g. La facturation en temps réel,
    h. Le contrôle de tranche réseau (network *slicing*)
    i. Acteurs français : Orange, Ericsson, Nokia

5. NEPHIO (Linux Foundation) est un Partenariat avec Google Cloud pour
    a. Simplifier l'automatisation des réseaux de télécommunications grâce à des technologies *cloud native* basées sur Kubernetes.
    b. Automatiser l'infrastructure *cloud* et les fonctions réseau (CNF) (*edge*).
    c. Réduire la complexité des déploiements multifournisseurs et multisites
    d. Accélérer l'intégration des fonctions réseau avec une approche GitOps et des CRDs (Custom Resource Definitions) Kubernetes.
    e. Favoriser l'interopérabilité entre les opérateurs, les fournisseurs *cloud* et les éditeurs de logiciels réseau.
    f. Réduire les coûts

6. TM FORUM « OPEN DIGITAL ARCHITECTURE »
    a. Standardiser l'architecture IT des opérateurs (OSS/BSS) et favoriser l'interopérabilité
    b. Favoriser une approche en composants modulaires pour les fonctions des systèmes IT (facturation, gestion des clients, réseaux, etc.) (plug & play)

c. Soutenir la migration vers le *cloud native* (technos et déploiement public/privé/*edge*))
d. Accélérer l'intégration *via* des API ouvertes (intégration multi-fournisseurs).
e. Faciliter l'automatisation (orchestration) et l'IA/ML (gestion)
f. Créer un écosystème multi-fournisseurs de modules compatibles ODA.
g. Acteurs français : Orange, Ericsson, Nokia, Cap Gemini.

7. *Cloud native* telecom architecture (Linux Foundation)
   a. Accélérer l'adoption des technologies *cloud natives* pour les réseaux de télécommunications
   b. Éviter la fragmentation en créant un programme de conformité unifié
   c. Développer de meilleures pratiques pour les réseaux *cloud* natifs et Kubernetes
   d. Créer un catalogue de tests pour évaluer les fonctionnalités fonctionnelles et non fonctionnelles
   e. Établir un programme de certification pour les fonctions réseau *cloud natives*, basé sur le programme de certification CNCF
      i. Renforcer la confiance et l'adoption des technologies *cloud natives* dans le secteur des télécommunications
      ii. Faciliter l'intégration et la coopération entre les différents acteurs du domaine
   f. Acteurs français : Orange, Ericsson, Nokia

8. AI RAN Alliance annoncée au MWC 2025 avec trois axes principaux :
   a. IA pour le RAN (AI-for-RAN) : Utilisation de l'IA pour améliorer les performances du RAN, notamment en augmentant l'efficacité spectrale et en optimisant la gestion des ressources radio.
   b. IA et RAN (AI-and-RAN) : Intégration conjointe IA et RAN sur une infrastructure partagée, maximisant ainsi l'utilisation des ressources et ouvrant la voie à de nouveaux services.
   c. IA sur le RAN (AI-on-RAN) : Évolutions du RAN pour supporter des briques IA à la périphérie du réseau, permettant une efficacité opérationnelle accrue et l'introduction de nouveaux services pour les utilisateurs mobiles
   d. Acteurs français : Ericsson, Nokia

Les plateformes IA des hyperscalers

Les GAFAM surfent déjà sur le développement exponentiel de l'IA et mettant à disposition des offres spécifiques pour accueillir les développements IA :

- Google Cloud AI (Google)
  - NLP (BERT, PaLM, Gemini) et *frameworks* (TensorFlow, Keras).
  - Vertex AI (plateforme unifiée)
  - AI Hub (place de marché de modèles et d'outils IA)

- PaLM API / Gemini API (IA générative)
- AutoML (entraînement de modèles)

- AWS AI/ML (Amazon Web Services)
  - Amazon SageMaker (plateforme complète de *machine learning*)
  - Amazon Bedrock (IA generative serverless)
  - Amazon Comprehend (NLP), Rekognition (vision), Polly (*text-to-speech*) et Transcribe (*speech-to-text*).
  - CodeWhisperer (assistant IA pour développeurs).

- Azure AI : Partenariat stratégique avec OpenAI, solutions d'IA intégrées.
  - Azure OpenAI Service (accès aux modèles GPT-4, DALL·E, Codex)
  - Azure Machine Learning Studio (plateforme ML complète)
  - Azure Cognitive Services (API IA clé en main)
  - Copilot et Semantic Kernel (IA dans les applications Microsoft 365 et développement assisté).

- Apple : IA embarquée et IA conversationnelle.
  - Core ML (framework ML intégré dans iOS, macOS, watchOS)
  - SiriKit et NLP (traitement et compréhension du langage).
  - Create ML (entraînement simplifié de modèles sur Mac).
  - IA multimodale (reconnaissance d'images, ARKit, Vision framework).

- ORACLE
  - OCI Generative AI : modèles de langage de grande envergure (LLM).
  - OCI Generative AI Agents : combinaison LLM et génération augmentée par récupération (RAG)
  - Oracle Digital Assistant : création d'assistants virtuels (chatbots)
  - OCI Language : analyses de texte sophistiquées à grande échelle.
  - OCI Speech : transcription de la parole en texte et synthèse vocale
  - OCI Vision : analyse d'images basé sur l'apprentissage profond.
  - OCI Document Understanding : extraction de données clés à partir de fichiers documentaires *via* des API et des outils en ligne de commande.

- IBM :
  - Watson Studio : création, l'exécution et la gestion de modèles d'IA,
  - Watson Assistant : développement de chatbots et d'assistants virtuels
  - Watson Natural Language Understanding :
  - Watson Machine Learning
  - IBM Cloud Pak for Data plateforme intégrée de données et d'IA

- Meta AI (Facebook/Meta)è recherche IA et l'IA open-source.
  - PyTorch (framework open-source développé par Meta)
  - LLaMA (Large Language Model Meta AI) (modèles de langage open-source)
  - Horizon AI (optimisation de contenu et recommandation dans les produits Meta).
  - FAIR (Facebook AI Research) (initiatives en IA et publications open-source)

Annexe III : rappels sur le positionnement des satellites dans l'écosystème du numérique

Les satellites sont essentiels pour fournir facilement une **connectivité complémentaire à la couverture des réseaux terrestres** car ils offrent :

- Une couverture **globale** (mers et océans, aérien)
- Une couverture pour les **zones blanches** (montagne, zones rurales isolées ou difficiles d'accès …), non couvertes par les réseaux terrestres. Là où les travaux d'installation de la fibre coûtent trop cher, les raccordements sont trop complexes ou dans les endroits peu ou mal couverts par les réseaux mobiles, le satellite demeure une solution de transition ou une réelle alternative.
- Une connectivité **de secours** (par exemple, en cas de désastre naturel impactant les réseaux terrestres) apportant de la résilience. De manière plus prosaïque, certaines entreprises ou grands magasins peuvent avoir un lien satellitaire comme lien de secours en cas de problème ponctuel et local de leur accès fibre (chaque minute sans accès réseau pouvant signifier des ventes en moins, ne serait-ce que du fait des besoins de connectivité liés aux cartes bancaires)
- Renforcer la résilience des réseaux terrestres en offrant plusieurs types de connectivité, que ce soit une connectivité **directe** vers l'utilisateur final (ou vers des objets connectés), ou connectivité « *backbone* » pour une station de base cellulaire (ou autre relais sans fil) isolée, en mode backhaul

Orbites et fréquences des satellites de télécommunications

Il existe plusieurs types de satellites sur lesquels s'appuient les réseaux NTN, différenciés selon leurs orbites :

- Satellites GEO (à orbite géostationnaires) : altitude 35 786 km, se déplaçant de manière synchrone avec la Terre, et quasi-fixe par rapport à un point de la Terre. Ces satellites offrent, dans le cadre de certains services visés particulièrement, un moindre coût par bit, et des terminaux utilisateurs peu chers, mais une latence élevée (+480ms). Par exemple : les 31 satellites géostationnaires Eutelsat. À noter que l'impact carbone d'un réseau de satellites GEO est réduit par rapport à une couverture terrestre équivalente (les satellites étant alimentés en énergie solaire).
- Satellites MEO (Constellations en orbite moyenne), altitude entre 8000 et 20 000 km, latence de 100 – 150 ms. Par exemple : la constellation O3b de SES.
- Satellites LEO (Constellations en orbite basse) : plus coûteux, basse latence (<50ms), terminal utilisateur plus complexe/cher (plus cher en coût mais potentiellement subventionné). Exemples : Starlink, Oneweb. Les services LEO marquent un changement dans la perception d'un service qui était régional en GEO et qui est désormais global en LEO (infrastructure mondiale mais des services régionaux et des spécificités en termes de sécurité et d'indépendance).

L'utilisation du spectre radiofréquence utilisé par les réseaux NTN satellitaires est soumise à la réglementation. Plusieurs bandes de fréquence sont assignées par l'Union Internationale des Télécommunications (ITU). On distingue en particulier :

- Les bandes hautes (C, Ku, Ka) : applications à **bande large** ou *broadband* (jusqu'à 500Mbit/s), avec antenne parabolique ou plate électronique (connectivité fixe ou mobile, connectivité gouvernementale, entreprises, etc.).
- Les bandes basses (L, S) : applications à **bande étroite** ou *narrowband* (internet des objets, messages ou Internet bas débit, terminaux personnels, applications civiles ou militaires), avec terminaux personnels (téléphone).

Les protocoles utilisés pour le moment par les satellites de télécommunications sont propriétaires, mais pour la plupart basés sur la forme d'onde standard DVB-S2. Les satellites futurs seront plus probablement basés sur le protocole 5G-NTN, standardisé par le 3GPP à partir de la Release 17. L'utilisation prochaine de 5G-NTN permettra une intégration plus facile et complète (par ex : un seul cœur réseau 5G, un seul terminal avec plusieurs antennes, *handover* transparent pour l'utilisateur). L'utilisation du standard 3GPP est aussi un garant d'un écosystème industriel ouvert, à l'opposé d'un système propriétaire qui ne permet pas l'entrée de nouveaux arrivants.

Par ailleurs, la constellation IRIS² (*Infrastructure for Resilience, Interconnectivity and Security by Satellite*), financée par l'Union Européenne, l'ESA (Agence Spatiale Européenne) et les opérateurs européens Eutelsat, SES et Hispasat, marque un tournant des constellations en se positionnant sur le standard 5G, en opposition aux solutions propriétaires.

De plus, les solutions standards ouvrent la voie à une **convergence des services terrestres et satellitaires**, un niveau de maintenance supérieur et potentiellement à terme des coûts d'implémentations réduits.

A l'horizon 2030, une intégration native des réseaux satellitaires dans le cadre du futur standard 6G constituera une seconde évolution complémentaire mais tout aussi radicale et aura pour objectif d'optimiser leur performance.

Les marchés visés par ces constellations sont :

- Le *broadband* connectivité fixe pour le résidentiel et/ou les réseaux d'entreprises reliant différents sites (connexion principale ou de secours), l'interconnexion de réseaux mobiles (*backhaul*) et les services de connexion à la dorsale d'internet (*trunking*).
- La connectivité mobile qui peut être soit collective soit individuelle. La connectivité collective couvre la connectivité large bande pour avions, bateaux, trains... un marché en forte croissance. À noter l'ouverture de nouvelles routes maritimes circumpolaires en raison de la fonte des glaces liée au réchauffement climatique. La connectivité individuelle, elle concerne davantage les voitures (télémétrie des voitures autonomes, divertissement).
- Les services gouvernementaux et de sécurité, avec interconnexion de sites dispersés.

Les constellations en bandes basses offrent des débits plus faibles, elles visent :

- La Messagerie ou les applications faible débit pour les smartphones (« Direct to phone » ou « Direct to Cell »), sur lequel se positionne également Starlink qui envisage une constellation spécifique
- L'Internet des Objets : traçage de colis, récolte de données par des senseurs (compteur électrique, température, humidité, alarme incendie)

Les constellations en bandes basses peuvent utiliser les bandes MSS 2 GHz (1980-2010 MHz et 2170-2200 MHz) : déjà harmonisée UE avec usages services connectivité à bord des avions (par ex la constellation Inmarsat) et IoT (constellation Echostar). On peut citer l'acquisition en cours des licences du spectre d'Echostar par Starlink. Ces bandes réduites présentent l'inconvénient d'être opérées par des acteurs non européens. Un renouvellement des autorisations en Europe est attendu en 2027, avec possibilité de nouveaux services/acteurs pour 5G NTN (par exemple dans le cadre d'une phase 2 d'IRIS²).

Une autre alternative pour les constellations bandes basses est d'utiliser un partage de spectre entre réseaux terrestres et satellitaires. Ce partage est envisagé localement (Australie, USA), mais présente de nombreux défis (régulation, frontières entre pays attribuant des licences terrestres à différents opérateurs, interférences dans les zones partagées).

Annexe IV : les critères clés pour définir un partenaire de confiance

- **Sécurité, conformité aux réglementations et résilience**

Cela concerne la conformité aux normes et aux réglementations, la transparence des processus, la gestion des vulnérabilités, des audits de sécurité réguliers par des tiers indépendants et accrédités, la résilience opérationnelle (plans éprouvés de continuité d'activité et de reprise après sinistre). En particulier, un partenaire de confiance doit assurer la résidence des données en Europe (ou en France), respecter les RGPD, NIS2 et les futurs règlements à venir (CRA, DORA…). Le partenaire de confiance doit aussi offrir des mécanismes de contrôle tels que la gestion des clés de chiffrement par le client, intégrer des mesures de cybersécurité avancées et adaptatives, notamment la protection contre les menaces émergentes comme l'informatique quantique, tout en garantissant un service toujours disponible, une interconnexion fiable, résiliente et sécurisée. La prévention de la fraude, la vérification d'identité, et la traçabilité des opérations font aussi partie des éléments de confiance qui doivent être intégrés dès la conception, avec des services d'authentification forte et de provenance vérifiable, indispensables dans un environnement où l'intelligence artificielle et le contenu synthétique prennent une place croissante.

- **Transparence et gouvernance**

Absence d'influence indue d'États ou d'entités non alignées avec les valeurs démocratiques et les principes de marché ouverts, conformité réglementaire, en particulier en matière d'accès aux données

- **Alignement stratégique et technologique :**

Cet alignement passe par le co-développement de solutions, le partage de la propriété intellectuelle de manière équitable et la contribution à l'écosystème ouvert, un engagement envers des standards ouverts et de l'interopérabilité des solutions pour éviter le verrouillage technologique. Les partenaires de confiance doivent de préférence s'inscrire dans une démarche de développement de solutions *open source*, afin de renforcer la souveraineté technologique et la résilience de nos infrastructures.

La confiance repose globalement sur la maîtrise des actifs et la capacité à innover dans un cadre éthique et européen, pour garantir la sécurité numérique des citoyens et des entreprises françaises dans un contexte international et géopolitique complexe.

- **Fiabilité et performance :**

Qualité des produits/services, support et maintenance.

Annexe V : souveraineté, partenaires de confiance et IRN

Le 26 janvier 2026 s'est tenue la première rencontre dédiée à la souveraineté numérique sous l'égide la ministre déléguée chargée de l'Intelligence Artificielle et du Numérique, Anne Le Hénanff.

Cette rencontre avait comme objectif premier de **partager une vision commune et d'engager une dynamique collective pour faire face aux dépendances numériques**, qui deviennent de plus en plus préoccupantes.

La Ministre a souligné que toutes les parties prenantes doivent reconnaître la réalité de nos dépendances, qui sont aujourd'hui trop nombreuses, et qui portent atteinte à notre liberté et à notre contrôle. Elle a insisté sur la nécessité de définir nos propres standards pour préserver notre souveraineté.

À cette occasion a été présenté à la fois une initiative privée : l'Indice de Résilience Numérique (IRN) ainsi que l'observatoire de la souveraineté numérique, porté par le Haut-commissariat à la Stratégie et au Plan.

La complémentarité de ces deux outils permet d'établir un diagnostic basé sur des faits et des données chiffrées, afin de faire preuve de lucidité face à ces enjeux.

Cette rencontre avait un triple objet :

- Partager l'IRN
- Partager une vision stratégique
- Engager une dynamique collective

Cette initiative vient compléter le sommet Franco-Allemand du 18 novembre dernier où avaient été identifiées des thématiques prioritaires : l'intelligence artificielle, le quantique, la cybersécurité et le *cloud*, avec une attention particulière aux solutions certifiées SecNumCloud et sur la nécessaire création des conditions favorables pour réduire nos dépendances qui nécessite de développer les acteurs français et européens et favoriser une préférence européenne sur les marchés. L'ambition affichée est qu'en 2026, la France et l'Union européenne devront choisir leurs solutions numériques en cohérence avec leurs valeurs, en passant à l'action.

La France, pour être exemplaire, va adopter une nouvelle doctrine en matière de commande publique « Make or Buy ». Pour autant la Ministre a rappelé que le marché public étant plus petit que le privé, il est essentiel que les acteurs privés s'engagent davantage pour défendre un modèle européen.

Les comités stratégiques de filières (CSF) ont ce rôle de mettre en avant les offreurs de solutions français. C'est le cas du CSF IN sur les infrastructures numériques qui a publié depuis plusieurs années son catalogue mis régulièrement à jour et du CSF solutions numériques de confiance qui doit lancer le sien d'ici mars 2026.

L'IRN s'appuie sur une analyse structurée inspirée de DORA, centrée sur les métiers critiques, les systèmes et processus vitaux, en évaluant huit dimensions : résilience stratégique,

résilience économique et juridique, résilience data & IA, résilience opérationnelle, résilience supply-chain, résilience technologique, résilience sécurité, résilience environnementale.

L'IRN établit une cartographie pondérée mettant en évidence les niveaux de vulnérabilité. Selon ses fondateurs, les axes d'améliorations identifiés viseront à Réduire les coûts (optimisation des licences et négociation en position de force), augmenter l'agilité (capacité à changer de solutions sans coût prohibitif), renforcer la conformité (maîtrise des données et respect du RGPD), accroître l'innovation interne (développement de compétences et différenciation compétitive). À date, la méthodologie a été testée avec RTE et Docaposte. Les sociétés CMA CGM, Ouest-France, SNCF ont également pris part aux travaux.

Olivier Sichel, Directeur Général de la Caisse des Dépôts et Président d'honneur de l'ADRI, a témoigné et souligné l'importance de l'IRN dans un contexte mondial marqué par la géopolitique et l'intelligence artificielle. Inspiré des démarches d'analyse des risques en finance, cet indice vise à fournir un langage commun pour évaluer la résilience numérique des entreprises et des collectivités.

Comment mesurer l'IRN ?

Petites structures : autoévaluation *via* des outils sur GitLab, sans obtention de label officiel.

Grandes entreprises : diagnostic approfondi avec un label payant, en partenariat avec le CSF solutions numériques de confiance.

Gouvernance et perspectives de cet indice :

L'association ADRI, chargée de faire évoluer l'indice, va prochainement devenir une AISBL (association européenne). Elle travaillera au niveau européen et asiatique pour promouvoir cette démarche d'analyse qui nécessite une adoption à large échelle tant géographique que du nombre d'entreprises.

Clément Beaune, Haut-commissaire à la Stratégie et au Plan est intervenu pour rappeler **le** contexte de la création **d'un observatoire de la souveraineté numérique** (lettre de mission fin 2025) dont l'enjeu est de :

- Produire un diagnostic rigoureux et partagé de nos dépendances numériques
- Fournir des outils concrets pour orienter les décisions d'achats des acteurs publics et privés
- Contribuer dans un second temps au pilotage des études afin de nourrir le diagnostic de nos dépendances les plus critiques

Cet observatoire permettra d'assurer un suivi des différentes initiatives, consolider les données existantes et agir en complémentarité des travaux menés, tant au niveau national qu'européen avec les entités suivantes pour l'Etat et les collectivités : DAE, DGE, SGPI, DG Trésor, Banque de France/INSEE au niveau Européen : commission européenne (DG Connect, JRC), autres Etats membres.

Ainsi la base de données sur les dépendances numériques va se constituer en collectant les données qualitatives et quantitatives pour caractériser la nature, le niveau et les déterminants des dépendances numériques ainsi que les marges de manœuvre. Toutes les structures :

entreprises privées, administrations de l'Etat, opérateurs, collectivités territoriales) ont été destinataires d'un questionnaire mi-2026.

En conclusion, cette première rencontre témoigne de la volonté forte de la France de renforcer sa souveraineté numérique face aux enjeux géopolitiques, technologiques et économiques. La mise en place d'outils comme l'IRN, la mobilisation des acteurs publics et privés, ainsi que la régulation ciblée, sont autant d'éléments clés pour réduire notre dépendance et préserver nos valeurs. Cependant, la cohérence entre les initiatives publiques et privées, ainsi que la concrétisation des engagements, seront déterminantes pour atteindre ces objectifs autant qu'une adoption coordonnée à large échelle et premièrement à l'échelle européenne.

Annexe VI : composants

Au-delà des développements portant sur les matériaux et sur les procédés technologiques de fabrication des composants (qui ne sont pas dans le périmètre de ce livre blanc), nous décrivons ci-dessous des priorités d'action à moyen terme portant sur le champ des composants, par grands domaines applicatifs :

Les réseaux de communication

- Concevoir les composants pour les systèmes électroniques massive MIMO à différentes fréquences, dans différents cadres applicatifs (6G, applications duales, …)
- Optimiser les performances des composants des systèmes de communications optiques : FSO, fibre, systèmes MIMO (solutions cohérentes et non cohérentes)
- Poursuivre l'intégration de l'IA et de l'IA générative dans les méthodes de conception des composants.
- Élaborer des jumeaux numériques des réseaux d'accès intégrant les canaux de propagation comme outil d'aide à la conception des composants
- Développer des composants pour les approches de sensing co-existant avec les systèmes de communications
- Élaborer des composants matériels flexibles compatibles avec la virtualisation du réseau
- Développer des matériaux multifonctionnels et/ou biosourcés dédiés à l'électronique RF, pour la miniaturisation, la reconfigurabilité ou encore l'intégration discrète des front-ends radio de futures générations sur tout type de plateformes (mobile ou non).
- Elaborer des méthodologies d'analyses de cycle de vie, permettant de différencier les 'coûts' environnementaux de ces composants.

Composants pour le calcul HPC & IA @ Scale

- Composants pour le futur des interconnexions haut débit faible latence (liaisons inter-cartes – inter xpu (série puis parallèle) par interposeur ou directement sur les puces (électronique et photonique intégrée sur silicium).
- Rechercher des concepts de composants en rupture pour les centres de calcul visant une gestion énergétique optimale
- Efficacité des interactions matériel-logiciel, dans le cadre des nouveaux matériels et visant des systèmes ouverts (sans couplage obligatoire entre produits matériels et logiciels, limitant la flexibilité du marché).

Sécurité des Composants embarqués et des Systèmes

- Poursuivre les travaux engagés sur les outils d'évaluation de la sécurité des composants
- Proposer de nouvelles générations de composants matériels sécurisés en s'appuyant sur les évolutions des technologies de la microélectronique, notamment d'intégration 3D/hétérogène dans un contexte de contraintes de coût et de passage à l'échelle.

Réseaux non terrestres

- Anticiper le déploiement de réseaux satellitaires en orbite basse (LEO) et moyenne (MEO) de fortes capacités : optimisation de l'efficacité des composants et circuits, impact de l'augmentation du nombre de voies RF, diminution des puissances ampli
- Adapter la charge utile pour une transmission directe vers les téléphones portables standards
- Étudier et modéliser l'effet des radiations sur les composants et systèmes
- Optimiser le matériel de la charge utile des drones