FILIÈRE INFRASTRUCTURES NUMÉRIQUES

Livre blanc sur le futur des infrastructures numériques

Executive summary

Les raisons et les objectifs généraux de cette publication

Les infrastructures numériques connaissent une transformation profonde sous l'effet de plusieurs évolutions technologiques majeures et ce qui affecte de façon de plus en plus importante les acteurs traditionnels de leurs chaînes de valeur (fournisseurs de composants matériels et logiciels, équipementiers, opérateurs réseaux et *cloud*, producteurs et distributeurs de services, contenus, applications et agents…).

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 extérieurs à la filière télécoms traditionnelle, au premier rang desquels figurent les hyperscalers américains. Dans le même temps, l'intelligence artificielle devient un composant structurant de l'ensemble des infrastructures numériques, les réseaux non terrestres deviennent une composante clé de la souveraineté, dans un cadre dual civil-militaire et de convergence terrestre et non terrestre. Ces derniers mettent à terme en danger le positionnement des opérateurs de télécommunications qui pourraient perdre le contact direct client, *l'edge computing* ouvre de nombreuses opportunités de nouveaux services mais peine à trouver les bons modèles économiques sans passer par une plus forte interaction entre filières.

De manière générale, les diverses évolutions en cours constituent une formidable opportunité d'innovation et de création de valeur. Elles ouvrent la voie à de nouveaux services, à une amélioration significative des performances des infrastructures et à une accélération de la transformation numérique de l'ensemble des secteurs économiques. Elles représentent également un défi majeur, et menacent même de manière existentielle certains acteurs, les opérateurs de télécommunications, mais aussi les filières critiques utilisatrices des réseaux (dont les opérateurs d'importance vitale (OIV)), et donc globalement certaines sociétés et économies, dont, pour ce qui nous concerne le plus directement, les économies européennes. De nouveaux entrants occupent des positions stratégiques tandis que certains acteurs historiques voient leur rôle remis en question.

Au-delà des risques pesant sur la compétitivité de certains secteurs industriels, ces évolutions soulèvent des questions fondamentales concernant la souveraineté numérique, la maîtrise des infrastructures critiques, la cybersécurité, la gouvernance des données et de l'IA, la résilience des services essentiels et, plus largement, l'autonomie stratégique de la France et de l'Europe.

Si ces enjeux font aujourd'hui l'objet de nombreux travaux, le cadre général du sujet et les principaux risques systémiques sont insuffisamment identifiés. Souvent, le sujet est traité sur des angles de vue 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.

Ce livre blanc adopte donc une vision systémique. Il considère les infrastructures numériques comme un continuum technologique, économique et stratégique dont les différentes composantes deviennent progressivement indissociables.

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
- 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.

Les enjeux de souveraineté

L'ensemble des évolutions présentées dans ce document soulèvent de nombreuses questions critiques de souveraineté que nous traitons dans le cadre d'une vision globale. La notion même de souveraineté numérique est traitée ainsi que le potentiel de celle-ci dans la mise en place d'une souveraineté tout court, à la fois civile et militaire. La question des nouveaux modèles économiques devant être imaginés est traitée conjointement.

Dans son acception la plus ambitieuse, la souveraineté numérique pourrait consister à maîtriser l'ensemble de la chaîne technologique, des composants jusqu'aux services numériques, ainsi que l'opération des infrastructures et l'offre de services (dont IA) et des applications. Une telle approche apparaît aujourd'hui irréaliste à court et moyen termes compte tenu des investissements requis et des délais incompressibles, même si la France et l'Europe disposent des compétences pour le faire. Il faut donc définir le périmètre de la souveraineté et le niveau de contrôle visé (souhaité et faisable à divers horizons de temps).

L'enjeu n'est donc pas de rechercher une autonomie absolue, mais de définir les niveaux de maîtrise indispensables pour garantir la sécurité nationale, la résilience des infrastructures critiques, la compétitivité économique et la capacité d'innovation. Cette réflexion conduit à distinguer différents degrés de souveraineté, correspondant à des horizons temporels et à des domaines technologiques différents.

Une idée forte présentée dans le document concerne la mise en œuvre de solutions permettant d'adapter dynamiquement les contraintes en lien avec la souveraineté lors de la création de chaque service et lors de chaque usage. Comme cela est décrit dans ce document, les services seront composés de manière de plus en plus dynamique, y compris en temps réel, pour répondre à des requêtes spécifiques d'utilisateurs. Leur construction se basera de plus en plus sur une intégration de composants pouvant être fournis par des acteurs différents. Cette composition sera réalisée par des groupements fonctionnels appelés orchestrateurs. 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.

Les orchestrateurs de nouvelle génération, IA natifs, devront donc 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. Ils devront également œuvrer en respectant les diverses régulations en lien avec le numérique. L'orchestrateur devient ainsi un levier de pilotage dynamique de la souveraineté des infrastructures numériques et du respect des régulations.

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.

Il ne s'agit pas ici 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.

Le périmètre du livre blanc

Le document couvre l'ensemble de la chaîne technologique, avec une vision de convergence progressive entre réseaux, *cloud* et intelligence artificielle, qui conduit à l'émergence d'un véritable continuum numérique. Ce continuum est traité dans ses caractères horizontal et vertical.

Horizontal dans le sens où le *cloud* sort des grands centres de données et se dissémine jusqu'aux divers objets connectés en passant par ce que l'on appelle le *mobile edge computing*, où les points de présence des opérateurs de télécommunications intègrent des ressources de calcul et de stockage. Tout cela contribue à la mise en œuvre de services en mode *cloud* plus performants, par exemple en termes de latence, et plus sûrs.

Vertical dans le sens où le continuum couvre les aspects allant des composants matériels et logiciels jusqu'aux applications et services offerts par les divers secteurs d'activité, y compris la tendance émergente vers des services multisectoriels, décrits dans le document.

Ces deux continuums intègrent les réseaux non terrestres, en particulier les constellations de satellites, dont l'importance stratégique n'est plus à démontrer. Ces constellations commencent déjà à embarquer des capacités de calcul et de stockage afin de disposer d'une intelligence dont l'impact potentiel dans un contexte hybride civil et militaire est majeur.

Dans ce qui suit, nous nous limitons à présenter un nombre réduit de transformations structurantes, parmi toutes celles présentées dans le document. Elles ont été choisies du fait de leur très fort potentiel de création de valeur et, bien au-delà, du fait qu'elles pourraient donner un très fort positionnement global au numérique européen et également à de très nombreux autres secteurs d'activité.

La place centrale de l'intelligence artificielle

L'intelligence artificielle, et plus particulièrement l'IA agentique, constitue aujourd'hui un facteur de transformation transverse aux évolutions des infrastructures numériques que nous avons présentées dans le document.

Elle intervient d'abord comme un outil de plus en plus incontournable pour la conception, le développement, la planification, le déploiement, l'opération et l'optimisation des infrastructures

numériques convergentes, devenues de plus en plus complexes, intégrant des technologies avancées et de plus en plus diversifiées, notamment en ce qui concerne les nouvelles technologies radio.

Par ailleurs, et maintenant avec une vision *top-down*, l'IA devient de plus en plus distribuée, notamment dans le cadre de l'IA agentique, et impose de nouvelles exigences aux infrastructures numériques. D'une part, contrairement au streaming vidéo (trafic majoritaire depuis plusieurs années), l'IA génère un trafic bidirectionnel symétrique, ce qui implique, par exemple, une pression bien plus forte sur le lien montant des réseaux mobiles. D'autre part, en termes de volume, le trafic *machine-to-machine* est récemment devenu majoritaire dans les réseaux, du fait de l'IA. Un exemple bien connu est celui des applications fondées sur des grands modèles de langage (LLM) qui scrutent tout le Web, et bien d'autres sources de contenu numérique, afin de fournir les services attendus.

En prenant une vision plus structurelle et multisectorielle, il est admis aujourd'hui que l'IA agentique a un pouvoir de transformation majeur de tous les secteurs d'activité, avec une promesse de très forte création de valeur. Exploiter pleinement ce potentiel suppose toutefois de mettre en œuvre des mécanismes innovants de gouvernance de l'IA et des données, notamment dans un cadre multi-acteurs, potentiellement multi-sectoriel.

Nous donnons ici un exemple pour clarifier l'idée. Toute entreprise a une gouvernance humaine[1]. Lors du déploiement de solutions d'IA agentique, les agents doivent respecter les décisions de cette gouvernance humaine et doivent œuvrer dans le cadre de la stratégie de l'entreprise (en proposant éventuellement une évolution de celle-ci, mais *a priori* sans s'en écarter avant validation). Ces agents vont interagir avec des agents d'autres entreprises, partenaires ou pas, et avec d'autres organisations.

Afin de garantir que les agents agissent dans ce cadre-là, tout en respectant les règlementations, et de pouvoir analyser et si nécessaire contrôler leur comportement, il faut mettre en place un plan numérique de gouvernance de l'IA et des données.

Il s'agit d'une solution logicielle qui va, de manière automatique, transformer la gouvernance humaine de l'entreprise en une gouvernance numérique et produire à partir de là des mandats pour les agents. Ces mandats seront dynamiques et s'adapteront aux évolutions des réglementations, aux évolutions du marché, etc. En interne, ils prendront en compte dans leurs prises de décisions la gouvernance humaine de l'entreprise. En externe, ils commanderont un plan de contrôle qui va mettre en œuvre diverses politiques, dont des politiques de contrôle d'accès, d'usage et de traçabilité d'usage des données de l'entreprise, mais également des agents de l'entreprise.

Si nous avons dédié de longues lignes à ce sujet, c'est parce que nous le considérons comme un élément ayant le potentiel de repositionner très fortement l'écosystème numérique français et européen et pouvant ouvrir un énorme potentiel de création de valeur pour l'ensemble des secteurs d'activité.

Les opérateurs d'infrastructures numériques, du fait de leur caractère transverse, sont susceptibles d'occuper une position stratégique dans la mise en œuvre de cette gouvernance, notamment en proposant à leurs clients, en mode service (*Platform as a Service*, PaaS), un plan de gouvernance et de contrôle ouvrant ainsi pour eux-mêmes de nouvelles perspectives de forte croissance et de création

[1] Du moins pour l'instant ; en effet, le Président argentin Javier Milei propose de créer une réglementation permettant la création d'entreprises avec une gouvernance 100% numérique. Pour simplifier, il s'agirait d'entreprises contrôlées par des robots.

de valeur. Par ailleurs, ils joueraient ainsi un rôle important dans la mise en place d'un niveau élevé de souveraineté, en garantissant une approche nationale et européenne de cette gouvernance.

L'ouverture des Infrastructures numériques et un changement radical de paradigme

Les réseaux de télécommunications, et plus globalement le continuum numérique évoqué plus haut, offriront tout leur potentiel au travers d'une majeure ouverture des infrastructures numériques.

Les réseaux deviennent déjà plus ouverts, en offrant des interfaces de programmation d'applications (API, *Application Programming Interface*), qui permettent à leurs clients de contrôler eux-mêmes les ressources qui leur sont allouées (cela couvre notamment le concept de *Network as a Service*, où l'instanciation des services réseaux est faite à la demande, au travers de ces API, et en temps réel).

Mais l'ouverture peut aller bien plus loin. En effet, les architectures convergentes réseaux, *cloud* et IA pourraient incorporer des composants logiciels fournis par des tiers, typiquement des entreprises clientes, qui les utiliseraient pour orchestrer leur service avec des éléments répondant à des besoins spécifiques. Cela donnerait une grande dynamique à la création de nouveaux services et permettrait de mettre en œuvre des entreprises bien plus agiles.

L'étape suivante serait que ces infrastructures numériques plus ouvertes mettent en place des places de marché de ces composants apportés par des tiers. Cela découple le potentiel de création de valeur pour les fournisseurs de ces composants, sous contraintes d'usage selon l'acquéreur (accès limité à certaines fonctions bien sûr reflété dans le prix) et crée de nouvelles lignes d'affaires pour les opérateurs d'infrastructures numériques. Nous pouvons faire ici l'analogie avec les *stores* des fournisseurs de mobiles.

Les composants

Rien de ce qui a été présenté n'est viable sans les composants, éléments importants de toute stratégie de souveraineté, telle qu'évoquée plus haut. La chaîne technologique part des composants : électroniques, optiques, quantiques, logiciels. Nous différentions donc ici les logiciels composants des infrastructures, au cœur des nouvelles architectures, 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 souvent dans un objectif de performances maximales. Ceci génère donc des dépendances.

Parmi les composants, nous incluons ceux permettant de mettre en œuvre des liaisons radio et optiques, dont les technologies évoluent très vite avec l'avènement de concepts de plus en plus performants (*beamforming*, Massive MIMO, *CellFree*, RIS, utilisation de plus hautes fréquences, quantique, …). Par ailleurs, dans certains cas, comme pour les fibres optiques, 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. de + 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, 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 du document offre une liste technique, considérée prioritaire, de ces composants.

Si nous nous concentrons sur les aspects de la souveraineté liés aux composants, Il convient de distinguer :

- 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

La conception des briques technologiques est un sujet clé pour la souveraineté. Il donne par ailleurs lieu à de la propriété intellectuelle.

La conception des briques technologiques se base fortement sur des avancées scientifiques, le monde académique et son interaction avec l'industrie joue ici, comme pour les transformations structurantes présentées plus haut, un rôle très important.

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.

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.

Les analyses concernant la souveraineté dans le cadre des composants doivent traiter très attentivement la question de *l'open source*.

Afin d'éviter de mauvaises compréhensions, rappelons ici que quand on parle d'ouverture des réseaux ou des infrastructures numériques en général, cela peut concerner deux sujets différents.

Le premier est celui traité plus haut, ouverture au sens « services ». Le second est l'ouverture des solutions matérielles et logicielles qui permettent de déployer ces infrastructures, qu'elles soient ouvertes ou fermées dans le sens « services ». L'ouverture dans ce deuxième sens 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.

Les recommandations

L'analyse conduite dans ce livre blanc couvre les dimensions technologiques, économiques, réglementaires et géopolitiques des transformations en cours et à venir des infrastructures numériques. Elle conduit à un ensemble cohérent de recommandations, qu'elles soient stratégiques, spécifiques à des idées innovantes proposées et à des enjeux identifiés, transversales ou organisationnelles, afin d'accompagner la construction d'une politique ambitieuse des infrastructures numériques au service de la souveraineté, de la compétitivité et de l'innovation.

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.

Nous ne présentons pas ici l'ensemble des recommandations du livre blanc, mais il nous semble pertinent de présenter l'une d'entre elles qui est transversale à toute la vision présentée.

Une impulsion publique peut être déterminante pour catalyser les visions intégratives décrites dans le document, 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[2], *cloud*, électronique, IA, quantique, cyber, etc.) pour définir une feuille de route conjointe de recherche, s'appuyer 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 dans le document.
    - S'appuyer sur les pôles de compétitivité capables d'impliquer les écosystèmes ancrés dans les territoires.
- Impulser des feuilles de route coordonnées transverses aux Comités Stratégiques de Filière sur les cas d'usage et besoins associés prioritaires, quand 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 énergétiques, industries et technologies de la santé, industries de sécurité, logiciels et solutions numériques de confiance, solutions industrie du futur.

[2] 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.