POSITION PAPER

INITIATIVE SOUVERAINETÉ

INSTITUT CHOISEUL

Les infrastructures numériques, un socle d'autonomie stratégique à consolider pour la France et l'Europe

Avril 2023

L'*Initiative Souveraineté*, lancée en janvier 2022, est la plateforme de l'Institut Choiseul dédiée aux enjeux de souveraineté et de résilience. Cette Initiative a pour but d'identifier et de promouvoir des mesures pragmatiques et concrètes destinées à renforcer l'autonomie stratégique de la France et de l'Europe. Au travers de rencontres régulières réunissant acteurs économiques de premier plan et experts reconnus, et par la production de documents de synthèse et d'orientation émanant des écosystèmes réunis, l'Institut Choiseul entend ainsi prendre part au débat sur la nécessaire souveraineté nationale et européenne dans des domaines aussi variés que la défense, l'industrie, l'agroalimentaire ou encore les transports.

La 7ème *Rencontre Souveraineté & Résilience* s'est tenue le 27 janvier 2023 autour d'acteurs de premier plan qui ont partagé leur témoignage, vision prospective et bonnes pratiques : Jean-Noël BARROT, Ministre délégué en charge de la Transition numérique et des Télécommunications, Sébastien LESCOP, Co-directeur général de Cloud Temple, et Gilles BABINET, Co-président du Conseil national du numérique et *Digital champion* de la France auprès de la Commission européenne.

Introduction

La crise de la Covid a mis en lumière les vulnérabilités de la France et l'Europe en matière d'équipement et de matériel numérique. Nos dépendances à l'égard des « superpuissances » du numérique – Chine et États-Unis en tête – sont réelles, tandis que les BATX et GAFAM n'ont aucun équivalent sur le Vieux Continent. À la fin des années 1990, la France représentait 6 % des dépenses en R&D mondiales dévolues au numérique. Elle n'en pèse plus que 2 %.

Cette réalité suscite un regain d'intérêt à l'égard de notre souveraineté numérique : être maitre de ses choix et consentir à ses codépendances. Cela recouvre une dimension interne, au travers de la possibilité d'imposer sa régulation et ses normes auprès de son marché domestique et des acteurs tiers qui s'y intéressent. Et une dimension externe, en étant en mesure de réduire la dépendance aux technologies venues de l'étranger et de se protéger contre une possible fuite des données. Le terme de souveraineté doit cependant être manié avec précaution. Il s'agit davantage de renouer avec son autonomie stratégique, que de faire sécession du jeu « mondialisé » auquel se rapporte le numérique.

Les infrastructures sont la colonne vertébrale du numérique, désormais au cœur de la transformation de nos entreprises et du fonctionnement de notre société. Les couches matérielles (réseaux, centres de données, fibres optiques transocéaniques, constellations de satellites, etc.) sont indispensables aux couches hautes et applicatives. Ce sont les équipements (« hardware ») qui rendent ainsi possible le cloud, l'intelligence artificielle, la 5G.

FOCUS SUR Les trois couches du numérique

1 Couche matérielle

- Câbles sous-marins
- Centres de données
- Câbles de communication
- Fibre optique
- ...

2 Couche logicielle

- Codes et langages de code
- Protocoles réseaux
- Logiciels
- ...

3 Couche sémantique

- Toutes les données circulant sur le réseau
- Le *Big Data*
- ...

Une domination américaine et chinoise

D'après un rapport parlementaire publié en juin 2021, l'Europe reste un « nain numérique » sur le plan économique. L'examen de plusieurs marchés critiques permet d'attester la domination américaine et chinoise sur le champ des équipements.

› Les solutions françaises et européennes se marginalisent sur le marché du cloud. Celui-ci est dominé en Europe par cinq *hyperscalers* américains : Amazon, Microsoft, Oracle, IBM et Google. En 2022, ils ont capté 78 % du marché et 84 % de la croissance. Cette domination s'accélère. Même si les acteurs français sont en croissance, portés par la dynamique globale, leurs parts de marché se réduisent, faisant craindre une « mort lente ».

› Le constat est le même sur les marchés des PC et des smartphones, dominés par des acteurs soit asiatiques (Lenovo, Xiaomi, Oppo, Huawei, Samsung), soit américains (HP, Dell Technologies, Apple, Acer Group).

› Le secteur des câbles sous-marins fait aussi l'objet d'investissements massifs de la part des GAFAM. D'après le groupe français Alcatel Submarine Networks, 70 % des projets mondiaux actuels sont supportés par Alphabet, Meta et consorts.

Une telle concentration d'infrastructures clés du numérique entre les mains d'entreprises non européennes pose question sur deux plans : celui de la dépendance excessive de l'économie européenne et celui de la protection des données.

Au-delà de l'équipement matériel, la fragilité de l'Europe s'exprime dans ses circuits d'approvisionnement. Elle se trouve dans une situation de dépendance quasi-totale en ce qui concerne les métaux rares nécessaires à la fabrication des infrastructures numériques (98 % des terres rares lourdes proviennent de Chine).

Un potentiel de croissance important

Les marchés des infrastructures numériques sont dynamiques, à l'instar du cloud qui connaît une progression annuelle de 6 %. Il devrait évoluer de 53 milliards de dollars en 2020 à 560 milliards d'ici 2030, ce qui correspond au poids actuel du marché des télécoms.

Le retard actuel des industriels français et européens n'est pas rédhibitoire. Ceux-ci disposent d'un catalogue de services moins profond que les acteurs dominants, mais peuvent couvrir la plupart des besoins de l'ordre des commodités. La taille – plus modeste – et la proximité territoriale et culturelle des acteurs français et européens peut par ailleurs représenter un avantage comparatif face à leurs concurrents américaines et asiatiques, qui proposent souvent des offres surdimensionnées et éloignées des enjeux business pour les ETI et les PME.

Dans une Note stratégique de l'Institut Choiseul, Hubert Védrine soulignait cependant l'équilibre à trouver entre le soutien apporté à l'effort de rattrapage industriel européen, et la nécessité de ne pas priver les entreprises françaises du meilleur des technologies existantes. À ce titre, la mobilisation des acteurs du « Numérique de confiance » au sein d'un Comité stratégique de filière voulu par Bruno Le Maire est de nature à renforcer la capacité du secteur à répondre aux besoins de l'économie française.

Les fibres optiques transocéaniques sont également loin d'avoir atteint leur plein développement. L'évolution de la nature des contenus, du texte à l'image et à la vidéo, nécessite le déploiement de nouveaux câbles sous-marins. L'irruption de nouvelles technologies fortement consommatrices en puissance de calcul et en volume de stockage, à l'instar des métavers, de l'IA et de l'informatique quantique, va démultiplier les flux de données.

En réponse, des plans d'investissement ambitieux et ciblés sont adoptés. Ce travail est engagé depuis l'été 2021 en France, avec la mise sur pied du plan « France 2030 ». Ce plan massif d'investissement, doté de 54 milliards d'euros, consacre des budgets importants à cinq dimensions des infrastructures numériques : le cloud, l'intelligence artificielle, la cybersécurité, la 5G et le quantique.

La menace de l'extraterritorialité

Issue du droit international public, la notion d'extraterritorialité renvoie à l'édiction de normes dont le champ d'application excède les frontières de l'État qui en est l'auteur. Les technologies du numérique, par nature sans frontières, constituent un terrain propice au développement de l'extraterritorialité en l'absence d'harmonisation internationale des normes.

Les États-Unis ont recours à différents leviers pour utiliser cette extraterritorialité à des fins de renseignement, notamment économique. Le *Patriot Act* de 2001 a pu être utilisé en ce sens, au moins jusqu'aux révélations d'Edward Snowden. Le *Cloud Act*, promulgué par Donald Trump en 2018, interroge. Celui-ci permet aux autorités des États-Unis de collecter, dans le cadre de leurs procédures pénales, des données stockées par des entreprises américaines en dehors de leur sol. Et plus encore, les programmes de surveillance de la *National Security Agency*, qui s'appuient sur le cadre juridique de l'État fédéral, constituent des risques avérés

Les GAFAM sont directement concernés par ces textes et le champ des données visées est large (mails, métadonnées, documents électroniques, contenus de tous types). Sur un plan juridique, des outils existent à l'échelle française et communautaire pour se protéger des effets de cette extraterritorialité des lois américaines. Mais ceux-ci n'ont pas les résultats escomptés.

En France, la loi de blocage de 1968 existe mais est rarement convoquée en raison de son caractère peu dissuasif et du faible nombre de sanctions prononcées. Au niveau de l'Union européenne, une loi de blocage a elle aussi été introduite en 1996. Ce texte n'a, dans les faits, quasiment jamais été mis en œuvre par un État membre.

L'article 48 du RGPD tente également de limiter le transfert de données vers des pays tiers. Le « Privacy Shield UE-US » avait pour vocation de réglementer le transfert de données personnelles de l'Union européenne vers les États-Unis, mais les juges communautaires l'ont invalidé dans un arrêt de 2020 (incompatibilité avec les principes du RGPD).

Face à l'absence d'un mécanisme robuste pour contrer l'extraterritorialité des lois américaines, un projet de décision d'adéquation sur la circulation sécurisée de données entre l'Union européenne et les États-Unis a été présenté en décembre dernier. Ce nouvel accord ou l'amélioration des dispositifs existants, tels que les lois de blocage, est indispensable pour rééquilibrer le rapport de force vis-à-vis des lois américaines.

Pour le secteur public, une note de la Direction interministérielle du numérique (Dinum) de 2021 rappelle que le « recours à l'offre Office 365 de Microsoft n'est pas conforme à la doctrine Cloud au Centre », qui précise que le « recours à une offre de cloud commercial est possible uniquement si cette offre est certifiée *SecNumCloud* et qu'elle est immunisée contre les réglementations extracommunautaires », afin de prémunir les administrations contre les aspirations de données vers l'étranger. La Dinum précise, dans sa feuille de route publiée en 2023, que l'État souhaite investir dans « des outils numériques mutualisés », pour la plupart développés à partir de « logiciels libres » afin d'assurer « la maîtrise, la pérennité et l'indépendance du système d'information de l'État ». Le développement du recours au logiciel libre y est clairement envisagé comme un outil pour se prémunir des ingérences étrangères.

Des attaques « cyber » qui se multiplient

La cybersécurité est la clé de voute de la résilience des entreprises européennes et d'une souveraineté numérique et économique réelle, comme le rappelait un *Position paper* de l'Institut Choiseul.

Les cyberattaques peuvent prendre la forme de rançongiciels, de programmes malveillants, d'attaques par déni de service ou d'hameçonnages, en ciblant aussi bien des particuliers que des services de l'État.

Il en résulte des piratages de données et des interruptions d'activités du fait de la captation d'informations critiques (brevets, contrats). Une infrastructure numérique peut être définitivement sabotée, entraînant alors des effets systémiques importants.

Dans le monde, un milliard de personnes subissent chaque année une cyberattaque. En France, 9 individus sur 10 ont déjà été concernés par un tel acte de malveillance. L'usage renforcé du numérique, induit par la crise de la Covid, joue un rôle d'accélérateur.

Aucune organisation n'est à l'abri de cette menace. Elle cible les entreprises, mais aussi des services publics et tout particulièrement les hôpitaux. Des établissements hospitaliers ont été paralysés pendant plusieurs semaines du fait de rançongiciels. La présidente de la Commission européenne, Ursula von der Leyen, a laissé entendre que la Chine avait pu être à l'origine d'une série de cyberattaques contre des hôpitaux en Europe pendant l'épidémie de coronavirus. Elle a souligné que l'Union européenne « ne tolérera pas » de telles activités malveillantes.

Pour répondre à cette menace, le gouvernement français retient une approche offensive. Elle se manifeste au travers d'une stratégie d'accélération dotée d'un milliard d'euros dans le cadre du plan « France 2030 ».

En ce qui concerne les particuliers, la sensibilisation au risque est un levier essentiel. La plateforme cybermalveillance.gouv.fr cumule 8 millions de visiteurs sur cinq ans, dont la moitié pour la seule année 2022. Deux dispositifs importants ont été mis en place :

- Le premier est un filtre anti-arnaques. Celui-ci se glissera sur le navigateur, pour filtrer préventivement les sites identifiés comme étant malveillants. L'idée est de contrer les attaques dont le point d'entrée repose souvent sur une stratégie d'hameçonnage, afin de collecter des données personnelles ou des informations de paiement. Une version bêta sera disponible à l'été 2023, en vue d'une généralisation pour les Jeux olympiques de 2024.
- Le second est un Cyberscore, inscrit dans la loi, qui doit entrer en vigueur en octobre 2023. Celui-ci va s'appliquer dans un premier temps aux plateformes numériques les plus utilisées par les Français. Attribué à l'issue d'un audit portant sur la sécurisation et la localisation des données hébergées, le Cyberscore indiquera à l'internaute s'il peut communiquer, en toute tranquillité, ses données personnelles au site sur lequel il se connecte. Cette transparence valorisera les sites vertueux et, à l'inverse, encouragera ceux qui ne le sont pas à consentir aux efforts nécessaires. ■

Failles et perspectives internes

La persévérance d'une culture de la rente en Europe

À nombre égal d'habitants, les États-Unis investissent six fois plus que la France dans l'innovation numérique. En valeur absolue, les investissements américains sont donc trente fois supérieurs aux nôtres. Pour avoir une part de capital dévolu aux technologies de l'innovation par tête comparable à celle des États-Unis, la France devrait investir 30 milliards d'euros par an, contre 5 actuellement.

Un travail de facilitation du capital-risque a été mené de façon significative aux États-Unis depuis les années 1960. Le chemin est inaccompli en Europe où perdure une culture de la préservation de la rente. La part du PIB français consacrée à la R&D et à l'enseignement supérieur s'élève à 3,5 %, lorsqu'elle atteint 9 à 10 % dans les pays locomotives. En Israël, ce pourcentage se situe à 9,5 %.

La régulation contribue à ce phénomène. Certaines start-ups se sentent limitées dans leur capacité à produire de l'intelligence artificielle ou d'autres innovations en raison d'une interprétation coercitive du RGPD. L'appétence au futur doit être plus prononcée en France et en Europe.

Nous sommes entrés dans une ère où l'innovation de rupture est dominante, tandis que les acteurs français et européens sont davantage enclins à recourir à l'innovation incrémentale. Le coût du licenciement, cinq à six fois supérieur en France qu'aux États-Unis, encourage cette approche prudente en matière de R&D.

La neutralisation du risque est un problème de fond. ChatGPT doit servir d'inspiration. Avec l'audace et les financements adéquats, il aurait pu être européen. L'investissement de départ a certes été significatif (100 millions de dollars), mais ouvre désormais la voie vers un gain exponentiel.

Un déficit de compétences numériques

L'Europe fait face à un déficit majeur de compétences en matière numérique. Il y a dix ans, des travaux de la Commission européenne soulignaient que ce déficit de compétences concernerait 1 million d'emplois à horizon 2020. Cette prédiction s'est confirmée, puisque ce déficit serait actuellement de 1,2 million.

Ceci témoigne d'une forme de cécité des politiques publiques nationales et communautaires, en partie compensée par France Compétences qui permet de favoriser la formation de techniciens et la diffusion d'expertises en code ou en ingénierie.

Quand la France forme 40 000 ingénieurs par an, ce chiffre est de 450 000 en Chine. Les autorités chinoises n'ont pas eu d'importants efforts auxquels consentir pour parvenir à cette situation, du fait d'une pyramide démographique favorable et des lois de la statistique.

Les États-Unis ont pour leur part développé une approche migratoire. Si le pays est cinq fois plus peuplé que la France, il ne forme en propre « que » 70 000 ingénieurs. Mais de nombreux fondateurs des licornes américaines sont des primo-accédants à la nationalité. C'est la même chose pour ce qui est de la recherche et du profil de leurs PhD. La force des États-Unis réside dans leur capacité à capter des talents venus de l'étranger.

La France n'a ni l'un ni l'autre. La pyramide démographique nationale est défavorable et la stratégie vis-à-vis de l'étranger a longtemps été conservatrice. Une approche nouvelle a été mise en place et doit être saluée, mais ne prendra effet qu'au terme d'une génération. Enfin, les femmes restent éloignées des métiers du numérique, réduisant fortement la capacité du secteur à attirer des talents.

Une acculturation désormais très forte aux outils étrangers

Le marché français est aujourd'hui couvert, pour son écrasante majorité, par des outils étrangers, et notamment américains. Il en découle une formation, une acculturation et des habitudes de travail liés aux interfaces américaines. Nos usages du numérique, que l'on le veuille ou non, sont aujourd'hui largement déterminés par les ergonomies de ces applications.

La conversion à des outils souverains ne peut être pensée sans réflexion sur la capacité du public à s'en saisir pleinement et facilement, afin de démultiplier les chances d'appropriation. Pour cette raison, une recommandation pourrait être de s'appuyer de manière invisible et indolore sur les interfaces déjà largement répandue via des logiciels libres afin de favoriser cette transition.

Une sécurité insuffisamment mature

Le marché des infrastructures numériques françaises et européennes manque de maturité sur le plan de la régulation de la sécurité.

Si l'on prend l'exemple du cloud, il n'existe aucune norme de sécurité à respecter pour en vendre en France à des professionnels (hormis le RGPD). Unique référentiel en vigueur, *SecNumCloud* est le fruit d'un travail porté par l'Anssi. Extrêmement exigeant, il reste difficile à obtenir et concerne bien moins de 1 % de la consommation du cloud en France.

Sous l'impulsion de l'État, des projets de « cloud de confiance » qui seraient en mesure de respecter ce référentiel, s'appuyant sur des technologies américaines mais portées par des acteurs européens ont été lancés (*Bleu* et *S3NS*). Du fait notamment de la complexité technique sous-jacente, la mise en place de ces plateformes souveraines n'est pas immédiate. De nombreuses critiques n'ont pas manqué d'émerger, d'ailleurs, contre le recours à ces cloud de confiance pour le stockage de données publiques.

La sécurisation des technologies numériques passe aussi par celle des sites physiques auxquels elles se rattachent. Cet enjeu a été consacré par un arrêté de juin 2006, qui classe les télécommunications parmi les secteurs d'activité d'importance vitale. En 2020, 70 antennes relais ont été prises pour cibles en France.

En janvier 2021, des militants anti-5G ont ainsi privé 1,5 million de personnes de radio et de la TNT, en incendiant un émetteur près de Limoges. De même, l'incendie du site OVH de Strasbourg a eu des conséquences sur des services essentiels en plein Covid. Des écoles et des universités ont rencontré des difficultés à mener leurs cours à distance. L'importance stratégique des datacenters requiert un renforcement des sites sur lesquels ils sont implantés.

Renforcer l'égalité d'accès aux infrastructures numériques

L'égal accès à des infrastructures numériques de qualité est une condition indispensable à la confiance que nous accordons collectivement aux nouvelles technologies. Dans cette perspective, deux plans ont été menés avec succès par le gouvernement pour répondre à la demande de connectivité des citoyens.

- Le premier est le plan France Très Haut Débit (THD), initié en 2013, fixant comme objectif l'accès pour tous au très haut débit (> 30 Mbit/s) en 2022. La France a ainsi été le marché le plus dynamique d'Europe de septembre 2019 à septembre 2020, avec un accroissement de 2,8 millions d'abonnés au THD.

- Le second est le *New Deal Mobile*, un accord passé entre l'État et les opérateurs pour accélérer le déploiement de la couverture 4G en France. Il vise la couverture d'un ensemble de zones blanches et prévoit d'autres obligations liées aux axes routiers et ferroviaires.

Ces progrès sont à saluer. Selon un classement IDATE DigiWorld, la France est le pays d'Europe où la fibre se déploie le plus en valeur absolue.

Les investissements du secteur des télécoms ont progressé de 7 milliards d'euros en 2014 à plus de 10 milliards en 2019. De son côté, la couverture mobile du territoire est passée de 46 % en 2018 à 76 % au milieu de l'année 2020.

Le rythme de ces déploiements doit être maintenu et renforcé. D'après la Commission européenne, de vastes zones ne sont pas encore couvertes en France, en particulier celles moins densément peuplées ou rurales.

Les investissements de l'Europe dans la constellation de satellites Iris permettront de limiter la dépendance de l'Europe en la matière et de réduire les fractures numériques. ■

Propositions - Orientations - Actions

Faire de la commande publique un tremplin pour le numérique souverain

La commande de l'État dans le numérique représente 18 % des achats globaux en France. En matière de cloud, la plupart de ces achats sont dirigés vers des entreprises non européennes. En réaction, l'État a formulé en juillet 2021 la doctrine « Cloud au centre » à destination des ministères et de ses opérateurs.

L'une des mesures phares de cette doctrine est d'héberger les données collectées dans l'une des deux plateformes interministérielles ou dans l'un des clouds qualifiés SecNumCloud. Mais, en 2022, la commande des opérateurs de l'État et des ministères n'était conforme à cette doctrine qu'à hauteur de 15 %.

La passation de marchés publics est un levier puissant de consolidation des écosystèmes technologiques, tel que l'a souligné le document publié par l'Institut Choiseul et France Digitale sur les champions européens du numérique. L'attribution par le Pentagone à Amazon, Google, Microsoft et Oracle d'un mégacontrat nommé JWCC, doté de près de 10 milliards de dollars, en est une illustration.

Plusieurs recommandations peuvent être formulées :

- soutenir les solutions françaises lorsqu'elles existent, en exigeant de l'administration qu'elle établisse un cahier des charges fondé sur la réversibilité, la portabilité et la souveraineté des données ;
- réserver une part des appels d'offre aux ETI du numérique, afin de permettre de faire émerger un « Mittelstand » numérique en plein développement en France ;
- conduire un audit de la stratégie d'équipement numérique de l'État ;
- donner la capacité à l'État d'acheter de la licence logicielle sur du pluriannuelle
- instaurer un reporting au sein des administrations sur la localisation et le traitement de leurs données ;
- accompagner la transition des administrations publiques vers des solutions souveraines grâce notamment au recours aux logiciels libres ;
- adopter, au niveau européen, un *Small Business Act* dédié aux acteurs du numérique.

Enfin, les référentiels à venir, qu'ils s'appliquent aux achats numériques des acteurs public ou privé, pourraient intégrer ces mêmes critères de souveraineté et de localisation européenne des données hébergées. La refonte en cours du référentiel régulant le statut d'Hébergeur de donnes de santé (HDS) serait ainsi l'occasion d'y intégrer ces exigences. Et pour garantir un bon niveau d'information des décisionnaires quant à la sécurité des infrastructures numériques qu'ils utilisent, le principe de transparence du Cyberscore à venir pourrait être étendu aux solutions destinées aux entreprises et aux organisations.

Le « green » est à ce jour un instrument sous-exploité de valorisation des champions français et européens vertueux en matière environnementale. Cet enjeu est d'autant plus important que, selon l'Ademe, les datacenters et autres infrastructures de réseau génèrent 53 % des émissions de gaz à effet de serre imputables au numérique.

Il peut être proposé de :

- soutenir le développement de « Product Category Rules », dans le but de comparer l'impact environnemental de différents types de produits ou services numériques et guider le choix des acheteurs publics ;
- prévoir systématiquement des critères environnementaux dans les marchés publics relevant du numérique.

Encourager le développement d'une culture du risque

La France est confrontée à un problème d'affectation du capital. Des efforts ont été entrepris ces dernières années pour libérer le capital-risque et ceux-ci doivent être poursuivis. Un travail conséquent doit encore être mené en la matière au niveau européen. L'enjeu est de diriger davantage le capital vers le risque plutôt que vers la rente.

En trois décennies, la compétitivité industrielle de la France a été réduite à sa portion congrue. L'industrie représentait 27 % du PIB il y a trente ans contre 11 % aujourd'hui. Ce qui a été détruit en trente ans mettra possiblement autant de temps à se relever.

Ce rattrapage nécessite de prendre acte d'un nouveau paradigme, qui ne doit pas systématiquement opposer le principe de précaution à celui d'innovation. Il s'agit à la fois d'un enjeu de compréhension des acteurs dirigeants et de culture collective.

Il peut être suggéré de :

- repenser le rapport au risque dans la structuration des liens sociaux et de travail, en adoptant des règles de mobilité et d'évolution de l'emploi spécifiques au secteur du numérique ;
- faciliter l'accès au capital risque à l'échelle européenne ;
- soutenir la formation de profils « ingénieurs », de la primaire au supérieur, et attirer les talents féminins dans la filière ;
- augmenter la part de dépenses du PIB français consacrée à l'efficacité du système de recherche.

Se positionner sur les chantiers d'avenir

L'objectif de la souveraineté numérique n'est pas de démondialiser, mais de parvenir à peser sur l'échiquier global pour conserver une capacité de choisir. Il s'agit de s'insérer dans le jeu numérique de la spécialisation des nations. Dans un contexte d'hyperspécialisation, la France et l'Europe doivent pouvoir choisir leurs combats, qu'il s'agisse par exemple des « chipsets » (liés à la conception des systèmes d'armes de demain) ou des concentrateurs de données (source d'écosystèmes de start-ups appelées à devenir le prochain CAC 40).

Les chantiers d'avenir sont nombreux (IA, Edge, quantique, métavers, architectures nouvelles de type homomorphique, etc.) et peuvent être investis « à la française » ou « à l'européenne » (origine du capital risque, technologies utilisées, partenariats industriels, prise en compte environnementale, alignement avec les valeurs européennes…). La France compte 24 licornes contre 29 pour l'Allemagne et 43 pour le Royaume-Uni. Au niveau mondial, les États-Unis et la Chine caracolent en tête, avec respectivement 615 et 174 licornes recensées.

Des réussites existent et sont à massifier. Le prix Nobel de physique reçu par Alain Aspect en atteste, récompensé pour avoir ouvert « une voie pionnière vers l'informatique quantique ». À pleine maturité, le calcul quantique pourrait être 1 milliard de fois plus rapide que les technologies actuelles, y compris les supercalculateurs. Le quantique pourrait, dans les vingt années à venir, être la source d'innovations majeures dans des secteurs d'importance critique (anticipation de catastrophes naturelles ou modélisation de remèdes médicaux).

Il peut être recommandé de :

- encourager la création d'entreprises par des docteurs en marge de leur activité de recherche, à l'instar de Pasqal, Quandela ou Alice & Bob ;
- favoriser l'incubation de start-ups en milieu universitaire, pour éviter une « fuite de cerveaux » vers des géants du numérique non-européens ;
- légiférer sur un texte permettant de faciliter l'accès aux start-up/PME aux contrats étatiques sur le modèle du *Small Business Act* américain ;
- répliquer la mise en place de plateformes nationales pour identifier et expérimenter de nouveaux cas d'usage, sur le modèle de celle créée autour du quantique et dotée d'un premier investissement de 70 millions d'euros. ■

Les infrastructures numériques en chiffres

560 Mds $
Au niveau mondial, le marché du cloud devrait représenter 560 milliards de dollars d'ici 2030

18 %
La commande de l'État dans le numérique représente 18 % des achats globaux en France

2 %
La France représente 2 % des dépenses mondiales en R&D dédiées au numérique

L'Institut Choiseul

L'Institut Choiseul est un *think and do tank* indépendant, non partisan et à but non lucratif. Il se dédie au décryptage des grands enjeux économiques et à la fédération de la jeune génération économique.

Pour alimenter le débat public et incarner les dynamiques économiques en cours, l'Institut Choiseul produit des Notes Stratégiques, des études ponctuelles et des classements de jeunes leaders. Pour fédérer et animer ses communautés, il déploie des évènements de haut-niveau mêlant networking convivial, témoignages d'experts et de praticiens et échanges sur des sujets de prospective, sur différents territoires et verticales économiques, en France, en Europe et en Afrique.

Au croisement de la communauté d'affaires et du cercle de réflexion, l'Institut Choiseul offre une plateforme aux décideurs économiques privés comme publics pour s'identifier mutuellement, se mettre en réseau, promouvoir leurs initiatives et réfléchir aux grandes tendances économiques de demain.

Les partenaires de l'Initiative Souveraineté

L'Institut est accompagné par un noyau dur de partenaires fondateurs, tous acteurs français ou européens, qui prennent une part active à la discussion et à la formalisation de recommandations :

INSTITUT CHOISEUL

Institut Choiseul

12, rue Auber 75009 Paris
+33 (0)1 53 34 09 93

www.choiseul.info