



OBSERVATOIRE
géopolitique du
numérique et
des technologies
émergentes

SOUVERAINETÉ NUMÉRIQUE : DU MOT D'ORDRE À LA MÉTHODE

Thaima Samman / Avocate à la Cour, fondatrice du cabinet
d'avocats Samman, membre du Conseil d'administration de l'IRIS
Anca Caruntu / Directrice senior des affaires publiques, Cabinet Samman

Octobre 2026



PRÉSENTATION DE L'AUTEUR



Thaima Samman / Avocate à la Cour, fondatrice du cabinet d'avocats Samman, membre du Conseil d'administration de l'IRIS



Anca Caruntu / Directrice senior des affaires publiques, Cabinet Samman

Cette note a préalablement été publiée au sein de *La Revue politique et parlementaire*.

PRÉSENTATION DE L'OBSERVATOIRE

Sous la direction de **Camille Boulenguer**, chercheuse à l'IRIS, l'Observatoire géopolitique du numérique et des technologies émergentes propose un espace d'analyse et de réflexion dédié à l'étude de ces technologies et de leurs impacts multidimensionnels.

Il se donne pour objectif de centraliser et de produire une expertise indépendante sur les technologies émergentes, comme l'intelligence artificielle, les blockchains ou l'ordinateur quantique. Pour cela, l'Observatoire s'attache à analyser les implications géopolitiques, mais également économiques, sociales et éthiques des révolutions technologiques et se fixe pour objectif de favoriser le dialogue entre praticiens et chercheurs afin de se préparer aux évolutions à venir et accompagner les décideurs publics et privés.

iris-france.org



@InstitutIRIS



@InstitutIRIS



institut_iris



IRIS



IRIS - Institut de relations internationales et stratégiques

« Mal nommer un objet, c'est ajouter aux malheurs du monde », écrivait Albert Camus. Cette phrase résonne singulièrement aujourd'hui, tant le mot souveraineté sature nos débats. Il nourrit les discours, structure les polémiques, comme si sa seule invocation suffisait à conjurer l'inquiétude que suscite un monde redevenu incertain. La souveraineté est brandie comme une formule magique alors que la puissance réelle d'une nation se mesure à sa capacité concrète à agir, à innover et à résister plus qu'à ses déclarations d'indépendance.

QUAND UN MOT RASSURE DAVANTAGE QU'IL NE DÉCRIT LA RÉALITÉ

Depuis quelques années, chacun projette dans la souveraineté ce qu'il souhaite défendre ou craindre : désindustrialisation, crises géopolitiques, perte d'autonomie stratégique, dépendances technologiques, tensions énergétiques. Cette plasticité explique son succès, mais elle constitue aussi son talon d'Achille : un concept trop romantique pour s'attacher suffisamment aux solutions opérationnelles.

C'est particulièrement vrai dans le numérique. Beaucoup continuent de penser qu'une entreprise est souveraine parce que ses capitaux sont domestiques, qu'un secteur deviendrait autonome parce qu'il est isolé de la concurrence étrangère. Cette lecture oublie pourtant la réalité des chaînes de valeur contemporaines, dans un monde profondément interconnecté où aucun État ni aucune région ne maîtrise l'ensemble du cycle technologique. La profondeur financière américaine, l'intensité des investissements chinois, la vitesse d'innovation de certains acteurs privés montrent bien qu'une souveraineté fondée sur la seule propriété ou sur un monopole relève de l'illusion.

À rebours de ces réflexes défensifs, une conception plus réaliste définit la souveraineté comme une capacité d'action : produire, sécuriser, innover malgré les turbulences extérieures. Une souveraineté maîtrisée, celle qui garantit un véritable pouvoir de décision. L'enjeu n'est pas de se couper du monde, mais de réduire les vulnérabilités les plus sensibles et de construire des capacités internes permettant de décider, d'arbitrer et, surtout, de peser, grâce à un diagnostic lucide.

LE DIAGNOSTIC : UNE DÉPENDANCE ENRACINÉE DANS DES DÉCENNIES DE SOUS-INVESTISSEMENT

La souveraineté numérique n'est ni un concept français, ni même exclusivement européen : elle constitue aujourd'hui un axe central des stratégies de puissances. Partout, les États

cherchent à reprendre la main sur les infrastructures jugées critiques, à protéger leurs données sensibles et à réduire leurs dépendances technologiques ou développer leurs propres capacités. Les Émirats arabes unis ou encore Singapour¹ ont structuré une stratégie *cloud* visant à garantir un contrôle strict sur certains usages souverains. Les États-Unis ne sont pas en reste, ils ont progressivement renforcé leur politique d'exportation et d'accès aux technologies les plus stratégiques (dont, mais pas seulement, les semi-conducteurs).

L'Europe, et la France en particulier, n'avaient longtemps aucune raison de rougir de leurs laboratoires de recherche ni de leur capacité à concevoir et faire émerger des innovations majeures. Pourtant, l'ouverture des marchés européens et leur interconnexion, censées accélérer la diffusion de l'innovation et nourrir la croissance, se sont paradoxalement accompagnées d'un sous-investissement progressif dans les couches basses de la chaîne de valeur numérique. Comme on le verra tout au long de ce dossier, ce déficit concerne tout autant ce qui se joue sous terre (les matières premières essentielles), sous la mer (les câbles sous-marins), dans le ciel (les satellites), que dans les semi-conducteurs, les équipements matériels, les centres de données, les infrastructures informatiques dans les nuages, le *cloud*, ou encore les systèmes et modèles d'intelligence artificielle.

En parallèle, les États-Unis façonnaient un écosystème technologique porté par un capital risque sans équivalent (137 milliards d'euros investis dans la *deeptech* par exemple, contre 21,6 milliards en Europe en 2025). Taïwan et la Corée du Sud déployaient, de leur côté, des stratégies combinant subventions publiques, taux de change favorables et protections tarifaires ciblées pour faire émerger des champions, comme TSMC ou Samsung, capables d'absorber les coûts vertigineux des équipements les plus avancés.

Peu à peu, l'Europe s'est retrouvée dépendante d'infrastructures devenues essentielles à l'architecture même du numérique mondial. Et, après la bataille perdue des infrastructures matérielles et logicielles, le sous-investissement chronique de l'Europe continue de pousser ses champions technologiques à chercher des financements hors du continent. Le pionnier du logiciel français Business Objects en 1994 suivi de plusieurs champions de la tech française, comme Criteo dans l'AdTech, ont choisi une introduction au Nasdaq (couplée pour certains avec une cotation à Paris) pour accélérer leur croissance. Plus récemment, les leaders européens du quantique, le finlandais IQM et le français Pasqal, ont annoncé viser une

¹ Collectif, *Sovereign Clouds Are Reshaping National Data Security*, BCG, 27 juillet 2025. <https://www.bcg.com/publications/2025/sovereign-clouds-reshaping-national-data-security>

cotation à cheval entre l'Europe et les États-Unis, afin de conjuguer ancrage européen et accès aux capitaux mondiaux.

LES SUJETS ESSENTIELS : PROTÉGER, PRÉVENIR, CONTRÔLER

Si le diagnostic est juste, le traitement a une chance de fonctionner et le patient de retrouver sa vigueur, voire de revenir dans la course. Au regard du rapport de force technologique comme des conditions actuelles de financement, faut-il vraiment faire primer la nationalité du capital ? Ou plutôt la capacité à maîtriser certains leviers technologiques décisifs ? Et, si oui, lesquels ?

Protéger : une cyberdéfense à la hauteur des menaces

La souveraineté numérique commence par la capacité régalienne à défendre le territoire, physique comme numérique. Cela implique de détecter, attribuer, analyser et contrer des attaques qui visent désormais aussi bien les infrastructures critiques que les systèmes vitaux. Et cela exige que l'État dispose d'un accès effectif aux données nécessaires à la protection des intérêts fondamentaux du pays. Sans cette puissance de réaction, aucune politique technologique crédible n'est possible.

Prévenir : une cybersécurité robuste comme infrastructure invisible du pouvoir

« La cybersécurité, c'est une condition de la souveraineté. Si on est victime de toute cyberattaque possible, on n'est pas souverain », rappelle Vincent Strubel, directeur général de l'ANSSI, l'agence de cybersécurité française. Il ajoute : « Il y a une tendance à faire des raccourcis, à se dire qu'il faut forcément des solutions françaises pour répondre à tous les besoins. Ce n'est pas réaliste, ce n'est pas nécessaire, ce n'est pas souhaitable ».²

La prévention consiste à réduire les vulnérabilités qui fragilisent les administrations, les entreprises et les opérateurs stratégiques. S'appuyer sur les outils les plus sûrs, indépendamment de leur nationalité, est devenu un impératif pragmatique : empêcher les intrusions, éviter la paralysie, protéger l'intégrité informationnelle. La cybersécurité n'est plus un adjuvant technique, mais l'infrastructure invisible qui conditionne la continuité économique, institutionnelle et démocratique.

² Entretien accordé à l'AFP, 30 mars 2026.

Contrôler : maîtriser les nœuds des interdépendances technologiques

Aucun État, y compris les États-Unis, ne contrôle toute la chaîne numérique. La puissance consiste désormais à maîtriser quelques nœuds clés des interdépendances : ceux qui donnent accès à la négociation permettent de fixer des standards ou d'imposer des garanties. Autrement dit : l'autarcie est hors de portée, mais le contrôle de capacités critiques assure une marge de manœuvre stratégique.

La stratégie des briques essentielles

La souveraineté numérique ne se décrète pas : elle se construit, patiemment, stratégiquement. Et, pour la France comme pour l'Europe, elle ne se construit pas *contre* un adversaire, mais autour d'un principe simple : accepter les interdépendances, tout en se donnant les moyens de ne plus les subir. L'objectif n'est ni l'autarcie ni la naïveté, mais la capacité à disposer de leviers qui redonnent un pouvoir de négociation.

Car une entreprise, une administration ou un État ne devient vulnérable que lorsqu'il n'a plus d'alternative crédible, lorsque ses infrastructures essentielles reposent entièrement sur des technologies situées hors de son champ juridique. À l'inverse, disposer de capacités propres, même partielles, suffit à transformer une dépendance en rapport de force. C'est autour de trois chantiers clés que ce mouvement s'organise : les infrastructures, la technologie et le savoir-faire.

Ancrer des infrastructures critiques sur le territoire

L'« entreprise sans usine », vision portée par Serge Tchuruk lorsqu'il dirigeait Alcatel, incarne une époque : celle d'une mondialisation heureuse, d'une démocratie libérale que l'on pensait « victorieuse », pour reprendre l'analyse de Francis Fukuyama, et d'une économie où l'externalisation ne semblait poser aucun enjeu stratégique.

Mais l'histoire « a repris ses droits », et le monde numérique s'est, lui aussi, doté de frontières.

Faut-il pour autant imaginer qu'une infrastructure numérique se « relocalise » comme une usine ? Les guerres à l'Est et au Sud de l'Europe montrent l'inverse : la vraie sécurité repose sur des infrastructures stratégiques multi-localisées, mais avec des briques critiques sur le territoire national, seules garantes d'un contrôle, d'une supervision et d'une régulation pleinement exercés par l'État et les acteurs locaux.

Dans cette perspective, les offres *cloud* d'OVH, Scaleway ou Outscale jouent un rôle essentiel. Elles ne couvrent pas tous les besoins, elles ne sont pas exemptes de risques d'extraterritorialité, qu'il s'agisse des États-Unis (où toute entreprise opérant sur le marché

ou utilisant le dollar peut être concernée) ou du Canada (où un juge a récemment demandé l'accès aux données d'OVH). Mais les alternatives qu'elles offrent permettent déjà de reprendre la main.

À ces acteurs s'ajoutent des projets plus hybrides et plus ambitieux : avec un objectif conjoint de cybersécurité et de cybergdéfense, la joint-venture S3NS Google-Thales est déjà certifiée SecNumCloud, le plus haut niveau de sécurité réservé aux données les plus sensibles à mettre à l'abri des lois extraterritoriales et sera peut-être suivie de Bleu, dans une démarche similaire entre Orange, Capgemini et Microsoft.

Leur logique repose sur un compromis assumé : bénéficier de technologies de pointe tout en assurant un contrôle opérationnel et juridique local, grâce à une gouvernance française, des conditions d'accès spécifiques et des mécanismes de cloisonnement des données. Elles ne cherchent pas à remplacer les géants du *cloud*, mais à créer une alternative crédible. Un modèle inédit, qui pourrait inspirer l'Europe.

Avec une démarche différente liée à une cybersécurité de haute performance, l'offre AWS European Sovereign Cloud, sous juridiction allemande, vise à neutraliser les risques d'extraterritorialité, même si, à la différence toutefois des projets français, elle ne s'appuie pas sur un partenaire industriel local, limitant les perspectives de co-développement au-delà des enjeux de cybersécurité.

Diversifier les choix pour maîtriser les technologies clés

L'étude du Parlement européen de décembre 2025 sur les dépendances numériques l'a clairement montré : la souveraineté ne passe ni par le repli ni par l'autosuffisance, mais par une stratégie pragmatique. Développer des architectures hybrides, bâtir des infrastructures souveraines pour les usages les plus sensibles, et multiplier les fournisseurs dans une approche *multicloud*, par exemple, deviennent les conditions d'une autonomie réelle.

Car certains domaines sont aujourd'hui la charpente du numérique mondial : les câbles sous-marins, les satellites, les semi-conducteurs, le *cloud*, l'intelligence artificielle, et demain peut-être le calcul quantique. Diversifier les fournisseurs et les partenariats, c'est réduire les dépendances critiques, renforcer la capacité de négociation des États et des entreprises, et continuer à accéder à la performance que seuls quelques acteurs mondiaux peuvent assurer.

Si l'Europe a perdu du terrain sur plusieurs segments, elle conserve des atouts qu'il s'agit de consolider plutôt que de recréer. Dans les semi-conducteurs, ASML, STMicroelectronics ou Infineon restent des piliers stratégiques, notamment pour l'industrie automobile, même s'ils

doivent eux aussi naviguer dans une géopolitique technologique en mutation rapide et dans le *cloud* avec les offres sous différents formats tels que décrits ci-dessus.

Le calcul haute performance (HPC) devient lui aussi un levier stratégique. Le projet porté par MARA, après sa prise de participation et le refinancement d'Exaion, la pépite blockchain d'EDF, en offre une illustration : il s'agit d'implanter en France des data centers de nouvelle génération, auxquels Exaion apportera une couche logicielle de services. L'État a veillé à maintenir EDF au capital, aux côtés de MARA et de Xavier Niel. Résultat : une gouvernance française, un contrôle exercé depuis le territoire sur une partie des infrastructures et du savoir-faire, et l'amorce d'une filière électrotechnique capable de faire émerger de nouveaux acteurs de rang mondial.

La véritable clé de voûte : garder le savoir-faire sur le territoire

Aucune infrastructure ni aucune technologie ne fonctionne sans femmes et hommes capables de les concevoir, de les maintenir et de les faire évoluer. Le savoir-faire constitue l'infrastructure invisible du numérique.

Dans ce domaine, l'Europe, et notamment la France, disposent d'un avantage comparatif rare, nourri par l'excellence de leurs formations scientifiques, la force de leurs laboratoires et une tradition de recherche en mathématiques, algorithmique et technologies avancées qui continue d'alimenter un vivier exceptionnel de talents.

Mais cet atout reste fragile : la compétition mondiale pour les cerveaux s'intensifie et la capacité à retenir ou attirer des experts dépend de plus en plus de facteurs structurels, financement de l'innovation, perspectives de croissance, profondeur des écosystèmes industriels.

Dans cette perspective, la présence de laboratoires de recherche et d'entreprises développant de la tech ou des infrastructures sur le territoire issues d'entités étrangères ne sont pas que des menaces et n'offrent pas que des solutions techniques. Elles offrent la perspective de rester ou de revenir dans son pays par la création d'emplois d'expertise et le développement d'écosystèmes de compétences.

L'enjeu consiste désormais à multiplier ces opportunités par une véritable politique de formation, de mobilité et d'attractivité, afin d'offrir des raisons concrètes à des figures de pointe, Yann Le Cun, Arthur Mensch, ou la génération qui suit, de trouver en France et en Europe un terrain d'innovation crédible et propice à la prise de risque.

Sans cet investissement continu dans les compétences, la souveraineté numérique ne peut être qu'un projet défensif. Avec lui, elle devient un projet industriel capable de durer.

Les premières étapes de la souveraineté ne passent-elles pas dès lors par le maintien et la constitution de certaines infrastructures critiques localement, par l'assurance de la diversité des services indispensables pour éviter les monopoles et par la capacité à entretenir et attirer l'intelligence et le savoir-faire ?

Pour la France et l'Europe, la souveraineté numérique ne peut pas être ni un slogan ni un état à atteindre définitivement. Elle est un processus, fait d'arbitrages et de compromis. Elle suppose de penser simultanément la protection, la résilience et la maîtrise des technologies, sans céder à la tentation du repli. Les solutions les plus efficaces ne sont pas les plus visibles. Elles reposent sur des architectures hybrides et des partenariats maîtrisés pour réussir le développement progressif des capacités propres. Car, au fond, la souveraineté numérique ne consiste pas à se soustraire aux interdépendances, mais à être en mesure de les contrôler.

L'expertise stratégique en toute indépendance



2 bis, rue Mercœur - 75011 PARIS / France

+ 33 (0) 1 53 27 60 60

contact@iris-france.org

iris-france.org



L'IRIS, association reconnue d'utilité publique, est l'un des principaux think tanks français spécialisés sur les questions géopolitiques et stratégiques. Il est le seul à présenter la singularité de regrouper un centre de recherche et un lieu d'enseignement délivrant des diplômes, via son école IRIS Sup', ce modèle contribuant à son attractivité nationale et internationale.

L'IRIS est organisé autour de quatre pôles d'activité : la recherche, la publication, la formation et l'organisation d'événements.