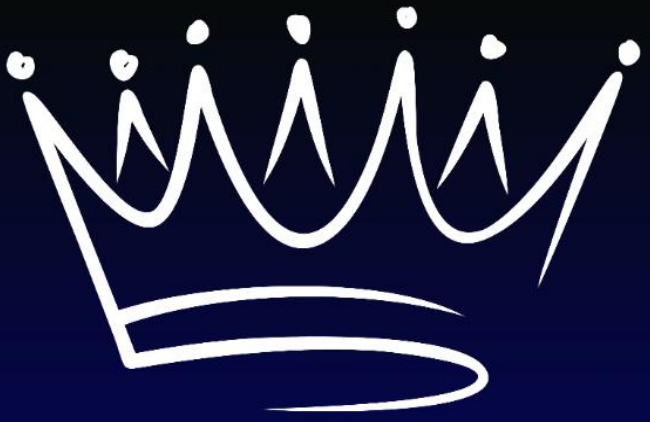
Souveraineté numérique Souveraineté d'entreprise



Yann-Eric DEVARS

Solve DSI

À la revue SERVIR et aux alumni École nationale d'administration et Institut national du service public, avec mes remerciements pour votre engagement au service de l’État et de l’intérêt général.

Puisse cet ouvrage contribuer, modestement, à nourrir la réflexion sur la souveraineté numérique, ses conditions concrètes, et les décisions qu’elle appelle.

Bien respectueusement,

Yann-Eric Devars

Yann-Eric DEVARS – Fondateur Solve DSI
Créateur du Framework DYNAMAP SI
www.dynamap.fr
06 22 13 45 71

Avant-propos

Les entreprises de la fin de l'ère industrielle, encore engourdies par un confort relatif hérité de décennies de croissance linéaire et de chaînes de valeur globalisées, se découvrent depuis peu tributaires d'une ressource immatérielle : la capacité à conserver la main sur leurs propres informations.

Cette "souveraineté" des systèmes d'information, longtemps perçue comme une posture de spécialistes soucieux de protéger leurs environnements techniques, s'est métamorphosée en prérequis stratégique, dont la perte se mesure soudainement en parts de marché évaporées, en appels d'offres perdus ou en amendes réglementaires qui annulent en un trimestre les bénéfices d'une année complète.

À mesure que le monde bascule dans l'économie des services connectés où chaque geste produit une trace, chaque trace un actif, et chaque actif un risque, la question n'est plus de savoir si l'on veut la souveraineté, mais combien il en coûte de ne pas la posséder.

Au début des années 2010, les directions générales se laissaient encore séduire par la promesse d'un cloud "universel", supposément neutre, naturellement élastique et géopolitiquement indolore.

Dix ans plus tard, la façade s'est lézardée : le Cloud Act rappelait aux acteurs européens que les données placées sous contrôle de prestataires soumis au droit américain pouvaient, à tout moment, devenir accessibles à une puissance étrangère, la crise sanitaire de 2020 révélait la fragilité d'approvisionnements matériels concentrés en quelques mégapoles asiatiques.

Les attaques comme SolarWinds, Kaseya ou Log4Shell montraient que l'interdépendance technologique, si brillante du point de vue de l'agilité, exacerbe aussi l'effet domino lorsqu'un composant critique se rompt.

Chaque incident résonnait alors comme un rappel : déléguer sans garde-fou, c'est abdiquer sans bruit la maîtrise de son avenir.

Dans ce contexte, l'Europe a choisi de transformer ses inquiétudes en normes et ses normes en avantage compétitif.

Le Règlement général sur la protection des données (RGPD) fut la première salve, le Data Act, entré en vigueur le 11 janvier 2024 et pleinement applicable à partir de septembre 2025, avance désormais l'obligation de garantir la portabilité des données industrielles et la réversibilité des services cloud, redistribuant les cartes du pouvoir entre prestataires et clients.

En exigeant que les fabricants, éditeurs et intégrateurs rendent leurs interfaces documentées et qu'ils facilitent le switch de fournisseur, l'Union européenne ne se contente pas d'ériger une protection, elle façonne un marché dans lequel la compétition se joue sur l'excellence de service plutôt que sur le verrouillage contractuel.

À peine huit mois plus tard, le 1er août 2024, l'Artificial Intelligence Act consacrait la même approche de "régulation-innovation" à l'intelligence artificielle : classer les usages par risques, fixer des garde-fous éthiques, imposer la transparence des modèles et la traçabilité des données d'entraînement.

Là encore, le message sous-jacent est limpide : nul ne conteste la mondialisation des solutions numériques, mais chacun doit garder la capacité d'en limiter l'usage, d'en auditer le fonctionnement et de s'en séparer sans mettre en péril la continuité de l'activité.

Pour les conseils d'administration, l'IA n'est plus un gadget expérimental, c'est un multiplicateur de productivité… ou un amplificateur d'exposition réglementaire si les mécanismes de souveraineté ne sont pas embarqués dès la phase de conception.

Le sujet ne se résume pourtant pas à un débat juridique, il épouse l'ensemble des dimensions économiques et sociétales de l'entreprise contemporaine.

Sur le plan financier, la valeur boursière repose désormais, pour plus de 85 % dans les grands indices occidentaux, sur des actifs incorporels : marques, algorithmes, jeux de données exclusifs.

La corrélation entre maîtrise informationnelle et capitalisation est si forte que la cybersécurité n'est plus reléguée au rang d'assurance, elle devient composante du P-&-L, visible dans la pondération ESG des investisseurs et dans le coût de la dette.

Sur le plan opérationnel, la tension sur les talents ravive l'enjeu de compétences internes : renoncer à comprendre l'architecture de ses systèmes, c'est confier son destin à des tiers dont l'objet social est, par nature, d'optimiser leur marge plutôt que la résilience de leurs clients.

Plus subtil encore, l'équation environnementale.

La souveraineté numérique interagit avec la sobriété énergétique : décider de rapatrier certaines charges de traitement ne vaut que si l'on dispose de centres de données alimentés par des sources bas carbone.

Exiger la localisation stricte des données sans mutualiser les infrastructures induit un surdimensionnement énergivore.

L'entreprise responsable doit donc conjuguer trois impératifs : contrôle, performance, décarbonation, qui souvent tirent dans des directions contradictoires.

Les arbitrages deviennent stratégie à part entière, ils réclament une gouvernance dédiée, dotée d'indicateurs qui ne soient ni purement techniques ni purement financiers, mais qui quantifient la dépendance, la latence réglementaire et l'empreinte environnementale sous un même tableau de bord.

Ajoutons à cela la dimension géopolitique : la reconfiguration des blocs technologiques, accélérée par les tensions sino-américaines et les réorganisations de chaînes de production, dessine un Internet fragmenté, où chaque sphère d'influence projette ses standards, ses formats d'API et ses exigences de contrôle des contenus.

Pour un groupe multinational, le simple fait d'exploiter une base de données clients peut exiger l'orchestration simultanée de cinq régimes juridiques parfois antagonistes.

La souveraineté n'est donc pas une quête d'autarcie, c'est la capacité à négocier et à arbitrer entre des cadres normatifs en mouvement, tout en préservant la cohérence interne des processus métiers.

Lorsque l'on parle de maîtrise, il ne s'agit pas uniquement de dispositifs cryptographiques ou de chantiers d'hébergement.

La souveraineté se joue tout autant dans la clause de sortie d'un contrat SaaS, dans le droit d'audit d'une plateforme d'IA générative, dans la compétence d'un administrateur à démêler un graphe de dépendances

open source ou dans la formation continue d'une équipe Ops capable de rebâtir un environnement sans accès internet.

Ce maillage de dispositions juridiques, techniques et humaines constitue le véritable mur porteur de la résilience : sa robustesse ne se mesure qu'au moment précis où le fournisseur défaillant, la frontière fermée ou la législation contradictoire mettent la continuité d'activité à l'épreuve.

Le présent ouvrage est né de cette conviction : il n'y a plus de barrière étanche entre la stratégie d'entreprise et l'architecture des systèmes d'information.

L'auteur, architecte d'entreprise depuis plus de dix ans, a vu les arbitrages techniques, que l'on croyait jadis cantonnés aux comités de pilotage IT, investir les conseils d'administration, influencer la gouvernance des risques, modeler la relation client et façonner l'image employeur.

En discutant avec des dirigeants de secteurs aussi variés que la santé, l'aéronautique, la finance ou l'agro-industrie, un constat s'impose : tous s'interrogent sur la mesure concrète de leur dépendance et sur la trajectoire d'autonomisation réaliste.

D'où la volonté de proposer un guide qui conjugue hauteur de vue et profondeur opérationnelle.

La première partie entreprend donc de cartographier les vulnérabilités : dépendances matérielles, captations logicielles, pressions réglementaires et érosion des compétences internes.

Chaque chapitre éclaire un angle mort, chaque étude de cas illustre la façon dont un incident ou une évolution normative peut bouleverser un modèle économique établi.

L'objectif n'est pas de céder au catastrophisme, mais d'offrir aux lecteurs un miroir sans complaisance, capable de révéler les fragilités dissimulées derrière des indicateurs de disponibilité flatteurs ou des certifications décrochées une fois l'an.

La seconde partie, plus prescriptive, déroule les leviers d'action.

Gouvernance, architecture de confiance, cloud souverain, open source industrielle, Zéro Trust, automatisation de la réponse aux incidents : autant de chapitres qui, sans masquer la complexité, proposent une méthodologie progressive et des retours d'expérience vérifiables.

Les cadres de décision y trouveront une trame pour orchestrer leurs investissements, fixer des jalons mesurables et aligner les parties prenantes : CEO, CIO, RSSI, DAF, DRH, directions métiers, autour d'une feuille de route commune.

Quant aux architectes et aux équipes opérationnelles, ils disposeront de modèles techniques, de listes de contrôle et de témoignages concrets pour transformer la théorie en chantier pragmatique.

Si l'ouvrage devait se résumer en une ligne, ce serait celle-ci : **la souveraineté n'est pas un état, mais un mouvement.**

Comme la qualité ou la sécurité, elle se cultive au quotidien, par petites itérations et par décisions structurantes, engrenée dans les pratiques de développement, dans les relations fournisseurs et dans la culture managériale.

Aucun dirigeant ne dispose du luxe d'attendre un cadre réglementaire parfait ou un produit-miracle qui garantirait, clé en main, l'autonomie digitale.

Ceux qui réussiront seront ceux qui auront compris que la souveraineté est un actif vivant : il requiert vigilance, curiosité et humilité, mais il offre en retour ce qui, dans un monde imprévisible, vaut plus cher que le capital : la liberté de choisir sa trajectoire.

En refermant cet avant-propos, j'invite donc le lecteur – qu'il soit PDG visionnaire, DSI confronté aux arbitrages budgétaires ou architecte en quête de sens à considérer son propre environnement.

Quelles briques techniques pourraient demain se dégrader faute de support ?

Quelles obligations réglementaires, encore lointaines, deviendront réelles dans le futur ?

Quelle connaissance critique repose sur un unique prestataire ?

Le voyage vers la souveraineté commence par ces questions, non par des réponses toutes faites.

Puissent les pages qui suivent fournir la trajectoire, le vocabulaire et l'élan nécessaires pour transformer l'inquiétude en stratégie et la stratégie en avantage durable.

Partie I – Les problématiques : décryptage des vulnérabilités et des dépendances

Chapitre 1 – La souveraineté, une exigence stratégique

1.1 Évolution historique : de la simple disponibilité à la souveraineté complète

Au commencement de l'informatique d'entreprise, la question qui obsédait les DSI se résumait à tenir la machine debout.

Dans les années 1960-1980, l'ère des mainframes IBM et Bull s'articulait autour du « temps machine » : il fallait fractionner les créneaux de calcul pour garantir que la paie sorte à date.

La « disponibilité » était alors synonyme de continuité transactionnelle, on réparait l'ordinateur avant qu'il ne tombe.

Les années 1990 introduisent la micro-informatique et la connectivité IP.

La haute disponibilité (clusters actifs-passifs, PRA, PCA) devient la norme.

L'objectif : éviter la panne franche d'un serveur unique.

Les métiers parlent soudain de « time-to-recover » et les métiers liés aux chaines d'approvisionnement ont depuis longtemps des tableaux de bord OTIF (« On-Time, In-Full »), la fiabilité s'industrialise : pourquoi l'IT ferait-elle différemment ?

Au tournant du millénaire, la virtualisation puis le cloud public promettent l'élasticité infinie.

VMware, AWS ou Azure transforment l'infrastructure en variable d'ajustement budgétaire, l'entreprise loue sa robustesse comme elle loue de l'énergie.

Mais cette agilité masque une dépendance croissante : en décembre 2021, une simple défaillance réseau dans us-east-1 paralyse Netflix, Robinhood et les commandes vocales Alexa pendant plusieurs heures (que serait-il passé sur des voitures autonomes ?).

C'est la décennie 2015-2025 qui fait muter la disponibilité en souveraineté :

L'extraterritorialité entre en scène avec le CLOUD Act (2018), donnant à la justice américaine un droit d'accès aux données stockées hors du territoire US lorsque l'opérateur relève du droit fédéral.

Les cyber-attaques de chaîne d'approvisionnement frappent à grande échelle :
- SolarWinds (2020) infiltre 18 000 organisations, compromettant agences fédérales et entreprises du Fortune 500 à cause d'une mauvaise gestion des niveaux de prestation.

- Log4Shell (Log4J) (2021) révèle qu'une librairie Java anodine (gratuite) peut ouvrir une brèche mondiale.

Le régulateur européen riposte : le Data Act impose au 12 septembre 2025 la portabilité nativement réversible des services cloud, tandis que l'AI Act, entré en vigueur le 1er août 2024, encadre les modèles d'IA et exigera en 2026 une traçabilité complète des données d'entraînement.

En moins d'une génération, la notion de « garder le service ouvert » s'est muée en « garder la maîtrise, où que réside le service ».

La souveraineté n'est plus un attribut technique, c'est un paramètre stratégique du bilan.

1.2 Risques macro-économiques : cyber-instabilité, ruptures d'approvisionnement, extraterritorialité des lois

Cyber-instabilité et coût du risque

En 2025, Allianz classe pour la troisième année consécutive les incidents cyber au rang de premier risque global pour les entreprises (38 % des répondants).

Les chiffres confirment l'intuition : le coût moyen d'une violation de données atteint 4,88 millions USD selon IBM, bondissant de 10 % en un an.

Cette inflation s'explique moins par le vol d'information que par la désorganisation opérationnelle : arrêt de production, perte de confiance

client, hausse des primes d'assurance, voire dégradation de notation ESG lorsque la gouvernance des données est jugée insuffisante.

Ruptures d'approvisionnement et volatilité industrielle

La pénurie mondiale de semi-conducteurs (2021-2023) a démontré qu'un composant à quelques centimes peut bloquer une ligne de production à plusieurs milliards.

Les constructeurs automobiles ont vu leur capacité chuter de 7 millions de véhicules, tandis que le prix des puces automobiles progressait de plus de 30 %.

Or, les SI ne sont pas immunisés : une fab asiatique qui ferme pour cause de tensions géopolitiques suffit à priver un cloud privé de serveurs de remplacement, mettant en cause la continuité d'activité.

Effet de levier juridique

L'extraterritorialité transforme une obligation lointaine en risque financier immédiat : Cloud Act, FISA, Patriot Act…

Autant de régimes capables de forcer un fournisseur à livrer des données sans que le client puisse s'y opposer.

À l'inverse, le Data Act façonne un déplacement de valeur en faveur de l'utilisateur, en rendant sanctionnable la pratique du **vendor lock-in** plus que la fuite de données.

Il ne s'agit plus seulement de se prémunir, il faut organiser contractuellement la réversibilité, sous peine de se voir interdire certains marchés publics ou partenariats sensibles.

L'entreprise moderne navigue donc dans un triptyque instable : agitation cyber croissante, chaîne logistique sous tension, collision de réglementations concurrentes.

La souveraineté devient le seul mécanisme de couverture intégrale : elle réduit l'exposition technologique, rééquilibre la négociation contractuelle et protège l'actif informationnel contre la volatilité réglementaire.

1.3 Quand la dépendance technologique devient un risque systémique

La dépendance n'est pas nouvelle, elle est systémique depuis que les plateformes numériques concentrent plusieurs ordres de grandeur de valeur.

Trois dynamiques se cumulent : centralisation, opacité, accélération.

1. Centralisation : Les dix premiers fournisseurs cloud contrôlent plus de 70 % de l'infrastructure mondiale.

Une panne ou un changement brutal de grille tarifaire se répercute instantanément sur des milliers d'acteurs.

L'incident AWS de décembre 2021 a démontré qu'un bug réseau unique suffit à figer des plateformes critiques de e-commerce et de médias, l'impact se compte en dizaines de millions de dollars perdus à l'heure.

2. Opacité des chaînes logicielles : L'affaire SolarWinds illustre le « cheval de Troie » moderne : 18 000 organisations, convaincues de mettre à jour un outil de supervision légitime, introduisent sans le savoir une porte dérobée pilotée par un attaquant étatique.

Dans une galaxie d'assemblage logiciel, l'entreprise ne contrôle plus son graphe de dépendances, elle doit cartographier puis segmenter pour limiter l'effet domino.

3. Accélération réglementaire et réputationnelle : Une faille zero-day comme Log4Shell se transforme en problème de compliance avant même que les correctifs ne soient appliqués, agences, assureurs et investisseurs exigent des preuves de remédiation sous 72 heures (pour l'instant).

La contrainte n'est pas uniquement technique : elle mobilise juristes, communicants et directions métiers, au risque de saturer la capacité décisionnelle de l'organisation.

Du single point of failure au « common mode failure »

Le plus grand danger n'est plus la panne isolée, mais l'échec par mode commun : plusieurs entreprises d'un même secteur, utilisant la même pile technologique ou le même sous-traitant, subissent simultanément la défaillance.

L'assureur voit sa corrélation de risque grimper, le régulateur envisage des stress tests informatiques (cf. DORA dans la finance), les analystes extra-financiers ajustent leurs notations.

Autrement dit, la dépendance technologique sort du domaine IT pour rejoindre la colonne « risques systémiques » de l'économie mondiale.

Vers un indice de dépendance souveraine

Certaines organisations pionnières construisent déjà une pondération des fournisseurs par criticité métier, score de réversibilité contractuelle, pourcentage de code source maîtrisé, délai de renaissance sur infrastructure alternative.

À horizon 2027, on peut anticiper que les agences de notation extra-financière intégreront ce type de métrique dans leurs ratings ESG.

La souveraineté deviendra alors un actif comptable, son absence, une décote de valorisation.

La souveraineté des systèmes d'information n'est pas un luxe protectionniste : c'est une extension naturelle de la gestion des risques dans une économie hyper-numérisée.

Du mainframe cloisonné aux plateformes cloud polyglottes, l'objectif s'est déplacé de la disponibilité locale vers la maîtrise globale, la valeur boursière, la conformité et même l'empreinte environnementale y sont désormais arrimées.

Ignorer cet axe, c'est faire de la dépendance technologique le maillon faible de la stratégie d'entreprise.

Chapitre 2 – Pressions réglementaires et géopolitiques

2.1 RGPD, NIS 2, DORA : panorama des obligations européennes

Au sein du marché unique, la souveraineté numérique se matérialise d'abord par un triple axe réglementaire :

1. Le RGPD (nouvelle versions) devint applicable le 25 mai 2018 et demeure le pivot.

Il institue un régime de responsabilité extracontractuelle, aligne les sanctions sur la puissance économique de l'opérateur (jusqu'à 20 M€ ou 4 % du chiffre d'affaires mondial) et, surtout, démontre depuis cinq ans une montée en intensité répressive : le cumul des amendes franchit 6,2 milliards € en juin 2025, contre 4,6 milliards un an plus tôt, soit +34.

Cette trajectoire en cloche témoigne d'une doctrine désormais assumée des régulateurs : la dissuasion financière et la responsabilisation de la gouvernance.

2. La directive NIS 2 élargit le périmètre de cybersécurité à dix-huit secteurs critiques, impose un pilotage par le conseil d'administration et des plans de gestion de crise, et doit être transposée par les États membres.

Elle grave dans le marbre une logique « due-diligence cyber » : non-seulement prouver qu'on protège, mais démontrer qu'on anticipe les ruptures d'approvisionnement numériques (supply-chain security, vulnérabilité open source, posture post-quantique).

3. Le règlement DORA applique, une exigence de résilience opérationnelle homogène aux banques, assureurs et sociétés d'investissement.

Pour la première fois, l'Union encadre contractuellement la dépendance aux prestataires cloud considérés comme des tierces parties critiques : clauses obligatoires de réversibilité, reporting d'incidents sous 4 heures, tests de pénétration pilotés par le superviseur.

Effet d'empilement

Le trio RGPD-NIS 2-DORA crée une matrice de conformité croisée : la violation d'un seul pilier (ex. incident cyber non déclaré) engendre un risque de double sanction (NIS 2 + RGPD), tandis que l'indisponibilité prolongée d'un service financier peut activer la mécanique DORA et le RGPD sur la réparation du préjudice moral.

Pour le comité d'audit, le coût réel de non-conformité devient multidimensionnel : amendes, action collective, notation ESG, prime d'assurance, voire exclusion d'appel d'offres publics.

Les dirigeants découvrent alors une nouvelle métrique : le coût marginal de souveraineté.

Concrètement, investir 1 € dans une infrastructure chiffrée souveraine peut éviter 4 € d'exposition réglementaire cumulative.

L'argument n'est plus philosophique, il devient financier.

2.2 Cloud Act, FISA : l'effet extraterritorial des régulations non européennes

Si Bruxelles déploie un bouclier normatif, Washington conserve l'épée de Damoclès extraterritoriale.

Deux textes concentrent les inquiétudes :

Le CLOUD Act oblige tout fournisseur soumis au droit fédéral à remettre, sur mandat, les données qu'il détient « où qu'elles se trouvent ».

En juillet 2025, Microsoft France a reconnu qu'aucune promesse d'hébergement intra-UE ne saurait neutraliser cette contrainte.

Les projets de mise à disposition de la donnée dans le pays du client (Dissémination des Data Centers pour rassurer sur la localisation des données) ne règlent donc pas la question : la juridiction l'emporte sur la localisation.

FISA (et son futur successeur) autorise la surveillance sans mandat judiciaire de non-ressortissants hors des États-Unis.

Les requêtes sont moins volumineuses que celles du CLOUD Act mais leur opacité procédurale alimente le risque réputationnel.

Pour un groupe européen, trois scénarios se dessinent :

1. Conspiration juridique : le fournisseur reçoit un « ordre » de l'autorité et ne peut pas alerter son client.

La violation RGPD est alors subreptice.

2. Conflit frontal : l'entreprise est informée et confrontée à une injonction contradictoire (Cloud Act vs RGPD). Elle doit choisir entre désobéir à l'un ou l'autre.

3. Contournement cryptographique : adoption d'un chiffrement « end-to-end » à clés sous contrôle exclusif du client.

C'est la seule voie sûre pour neutraliser l'extraterritorialité, mais elle complexifie la conformité DORA lorsqu'il s'agit d'exporter des journaux d'audit.

Au-delà du couple États-Unis/UE, d'autres législations convergent vers le même modèle de contrôle : la Network Data Security Regulation chinoise, entrée en vigueur le 1er janvier 2025, impose un examen de sécurité préalable à tout transfert transfrontière de données « importantes ».

L'entreprise se retrouve prise dans un triangle de lois aux logiques opposées : exfiltration potentielle aux États-Unis, rétention obligatoire en Chine, portabilité imposée dans l'UE.

Conséquence stratégique : le périmètre de souveraineté se déplace du centre de données vers le contrôle des clés et du pipeline logiciel.

Les RSSI parlent désormais de design par juridiction : où la clé ne migre jamais hors du territoire juridique choisi.

Les conseils d'administration, eux, intègrent dans le registre des risques l'hypothèse d'une demande légale secrète susceptible de rendre le bilan non conforme du jour au lendemain.

2.3 Vers des blocs numériques : fragmentation ou redéfinition de l'Internet ?

Depuis 2020, la crainte du "Splinternet" est passée de la métaphore à la métrique.

L'objectif n'est plus seulement de filtrer l'intérieur, mais d'affaiblir la connectivité des rivaux : câbles sous-marins, puces, standards.

Trois dynamiques redessinent la carte :

Bloc occidental : États-Unis, Union européenne, alliés nord-atlantiques.

Convergence sur l'OTAN numérique (partage de renseignement cyber), divergence sur l'extraterritorialité.

L'UE forge son autonomie normative (RGPD, NIS 2, Data Act) et investit dans des câbles et des moyens de connexion pour sécuriser son trafic transatlantique.

Bloc sino-russe : doctrine de cybersouveraineté affichée.

Grande Muraille numérique, obligation de stockage local, quantique.

Les sanctions occidentales accélèrent le découplage : Pékin finance des routes optiques alternatives via l'Asie centrale, Moscou prépare un DNS souverain.

Bloc des non-alignés numériques : Inde, Indonésie, Brésil, Nigeria.

Ils exploitent la rivalité pour négocier des transferts technologiques et imposer leur propre localisation (Digital Personal Data Protection Act indien, 2023).

La fragmentation n'est cependant pas synonyme d'isolement total : l'interopérabilité technique subsiste, mais les conditions d'accès (chiffrement, conformité, taxes sur la donnée) deviennent l'équivalent numérique des droits de douane.

Scénarios futurs : si la tendance se confirme, les experts prévoient un basculement du coût d'interopérabilité (multi-cloud, multi-standards) de 3 % à plus de 8 % des OPEX IT dans les grands groupes.

D'où l'émergence de nouveaux métier chargés de cartographier en temps réel les flux, d'orchestrer le chiffrement multi-juridictionnel et de négocier les exceptions légales.

De Bruxelles à Washington, de Pékin à Delhi, la loi réinvente l'architecture du réseau.

Pour l'entreprise européenne, la souveraineté ne peut plus être considérée isolément, elle est l'intersection d'un triptyque : conformité locale, résilience technique, diplomatie contractuelle.

Chapitre 3 – Chaînes d'approvisionnement et « vendor lock-in »

3.1 Cartographie des dépendances matérielles et logicielles

Les algorithmes et les données qu'ils traitent façonnent la valeur boursière plus sûrement que les usines, la souveraineté commence par une radiographie exhaustive de la chaîne d'approvisionnement : de la gaufre de silicium jusqu'à la dernière dépendance logicielle.

Or, ce circuit ressemble moins à une route linéaire qu'à un graphe tentaculaire dont chaque nœud : fabricant de puces, éditeur de micro-service, mainteneur open-source, peut devenir un point de rupture.

Dans l'entreprise, cartographier ces arborescences n'est plus un exercice documentaire, c'est un acte de gouvernance, au même titre qu'un audit financier.

La dépendance matérielle, une monoculture de fait.

En 2025, près de 68 % de la production mondiale de circuits avancés sort toujours des laboratoires du premier fabricant.

Son carnet de commande est plein pour plusieurs années et aucune émergence sur le marché de la tech ne peut négliger cet aspect avant de se lancer sous peine de manquer de matière première dès le départ.

La concentration n'est pas qu'un risque géopolitique : elle rigidifie la courbe d'adoption technologique et place la négociation des volumes au même niveau que l'ingénierie.

Le goulot GPU, symptôme d'un oligopole programmé.

Au-delà du CPU, la carte graphique est devenue la « pelle du Far West de l'IA ».
(Et l'on sait combien dans l'ouest Américain il valait mieux vaut vendre des pelles que de chercher de l'or pour faire fortune).

Les serveurs GPU se négocient à neuf mois de délai moyen et leur prix de gros a bondi de 21 % en un an, le marché, évalué à 38 milliards $ en 2025, devrait tripler d'ici 2032, rendant la moindre coupure logistique immédiatement visible dans le P-&-L.

L'architecte d'entreprise n'a plus seulement à optimiser le SI et ses coûts, il doit scénariser l'indisponibilité prolongée d'un composant qui, faute de substitut crédible, peut suspendre toute feuille de route d'IA générative par exemple.

Les métaux rares, la dépendance de plus en plus visible.

À cela s'ajoute la dépendance aux terres rares, néodyme pour les aimants de moteurs pas-à-pas, palladium pour les condensateurs multicouches, gallium pour les amplificateurs 5G.

Faute de sources de diversification matures avant 2027, l'entreprise doit bâtir une politique de stocks stratégiques ou négocier des clauses de priorité d'allocation dans ses contrats d'intégration matérielle.

Le firmware comme nouvelle frontière du risque.

Plus sournois encore : la chaîne de micro-code.

Le détournement de la librairie XZ Utils en mars 2024 ? une porte dérobée insérée avec patience dans la pile de compression de multiples distributions Linux ? a rappelé que la menace peut naître bien avant le runtime, au cœur des binaires signés.

La compromission d'un paquet inodore, intégré par dépendance transitive, suffit désormais à bloquer les entreprises malgré leur SOC dernier cri et très coûteux.

La prolifération des dépendances logicielles.

Une application cloud typique embarque plus de 1 500 paquets tiers, trois ans après la divulgation de Log4Shell, 12 % des applications Java tournent encore sur une version vulnérable de la bibliothèque, preuve que l'inertie circule plus vite que le correctif.

Dans ce contexte, la directive NIS 2 impose, depuis octobre 2024, une sécurisation explicite de la chaîne logiciel, incitant de facto à la tenue d'un SBOM continu, même si le terme ne figure pas noir sur blanc dans le texte : sans inventaire dynamique, pas de preuve de remédiation précoce.

Vers une cartographie vivante.

Les grands groupes se dotent donc de plates-formes d'« observabilité de la provenance » : capture automatique des graphes de dépendances, corrélation avec les flux de CVE, notation de criticité fournisseur.

À court terme, l'enjeu est de passer d'un audit ponctuel (photo figée d'un pipeline) à un jumeau numérique de l'écosystème, recalculé à chaque build.

À long terme, il s'agit d'adosser cette matrice à la fonction Achats, afin qu'une anomalie sur un mainteneur clé déclenche le même processus d'escalade qu'une défaillance financière de fournisseur.

3.2 Modèles de licences et captation de valeur

La souveraineté ne se joue pas qu'au niveau technique, elle s'inscrit dans la micro-économie des contrats.

Longtemps, l'entreprise a raisonné CAPEX : licence perpétuelle, maintenance annuelle, confortée par l'idée qu'un actif logiciel se déprécie comme une machine-outil.

L'irruption du SaaS bouleverse la donne : l'abonnement récurrent transforme le droit d'usage en charge d'exploitation et confère au fournisseur un bouton « off » instantané.

De la licence perpétuelle au modèle d'abonnement forcé.

L'exemple VMware est emblématique : depuis le rachat par Broadcom fin 2023, toute licence perpétuelle a disparu, au profit d'une souscription de trois ans minimum, pénalisée si elle n'est pas renouvelée dans les délais.

Pour le DAF, la courbe paraît plus lisse, pour le DSI, l'effet est un sur-verrouillage tarifaire, car les coûts de migration d'une infrastructure virtualisée équivalent, en main-d'œuvre, à dix ans de support.

La renaissance du « source available ».

En août 2023, HashiCorp a transféré Terraform sous Business Source License, l'outil reste lisible, mais son exploitation commerciale requiert un accord propriétaire.

En réaction, la communauté a « forké » le projet sous le nom OpenTofu, créant une divergence fonctionnelle qui impose aux équipes SRE une décision stratégique « brancher » ou « payer ».

L'incident a popularisé une métrique nouvelle : le community sustainability risk, le jour où la licence change, la dette technique se matérialise.

La monétisation de la fin de vie.

L'arrêt de CentOS 7 au 30 juin 2024 illustre la captation inattendue de valeur : pour conserver un OS stable, l'utilisateur doit soit basculer vers RHEL avec un surcoût de support, soit migrer vers un clone communautaire, opération délicate pour des flottes OT.

La prolongation payante du support s'apparente à une option de maintien dont le prix n'est jamais anticipé dans le business case initial.

Mesurer le coût de sortie avant d'entrer.

Une bonne pratique consiste à calculer un « Cout de sortie » : somme actualisée des frais techniques et juridiques pour rompre le contrat, divisée par la valeur actualisée des gains attendus.

Si le rapport dépasse 40 % de la valeur créée, le projet est réputé non souverain et doit être compensé par des garanties contractuelles équivalentes.

3.3 Cas d'école : migrations inverses coûteuses et faillite d'éditeurs critiques

En 2022, une PME américaine a rapatrié son logiciel stratégique dans son data-center.

700 000 $ d'investissements matériels, mais 2 millions $ d'OPEX économisés dès 2024.

Le cofondateur affirme désormais une trajectoire d'économie de 10 millions $ sur cinq ans : preuve qu'un retour on-premises reste viable si les équipes possèdent la compétence et le capital tampon.

Sans compter des équipes internes désormais mobilisables pour des projets afin de créer de la compétitivité.

Le 16 août 2023, Google a retiré son moteur MQTT managé.

Les industriels ont dû reconfigurer des millions de capteurs, souvent embarqués dans des machines où la mise à jour OTA n'était pas prévue.

Les fabricants ont doublé leurs coûts de connectivité sur un an pour maintenir la continuité des flux télémétriques. Leçon : quand le fournisseur retire un service, la clause de réversibilité vaut autant que la capacité réelle des équipements à changer de endpoint.

Faillite d'un acteur critique :

En avril 2024, un prestataire central dans le domaine de la sante est victime d'un ransomware : 12,9 millions de dossiers de santé sont exfiltrés.

Faute de soutien public, la société se place sous administration judiciaire, laissant pharmacies et hôpitaux sans solution de substitution.

Les clients ont dû déclencher un plan d'urgence pour rapatrier leurs données sur l'opérateur rival, avec perte partielle d'historique de dispensation.

Le coût silencieux des migrations inverses.

Ces récits partagent un invariant : le « vendor lock-in » ne devient visible qu'au moment de la sortie.

Les coûts se décomposent en rachat de licences ou de matériel, main-d'œuvre de bascule, double exploitation transitoire, dépréciation d'actifs non réutilisables.

Chez un grand compte, la somme représente fréquemment l'équivalent de deux ans d'économies promises à l'entrée.

L'indice interne de dépendance comme garde-fou.

Quelques groupes du CAC 40 ont donc créé un Vendor Sovereignty Score :

- 30 % : criticité fonctionnelle (niveau d'arrêt si le service tombe)

- 25 % : portabilité (formats de données ouverts, API standard)

- 20 % : santé financière et gouvernance éditeur

- 15 % : coût contractuel de sortie (pénalités, recyclage de licences)

- 10 % : adéquation aux exigences réglementaires (NIS 2, DORA, RGPD)

Toute initiative dont le score dépasse 70 sur 100 déclenches une revue exécutive et l'obligation d'un plan B technique documenté.

La souveraineté se construit d'abord dans la clarté : inventaire des dépendances, compréhension fine des modèles de capture de valeur, évaluation transparente du coût de sortie.

Un simple composant, un changement de licence ou la faillite d'un fournisseur peuvent perturber la délivrance de soins, bloquer une chaîne industrielle ou faire exploser un budget numérique.

Dans les chapitres suivants, nous verrons comment l'open source industriel, le multi-cloud orchestré et les architectures Zéro Trust transforment cette cartographie du risque en trajectoire de résilience : de la clause contractuelle à la clé de chiffrement, de la communauté de développeurs au conseil d'administration.

La souveraineté n'est pas un slogan de cybersécurité : c'est une discipline économique qui pèse, à horizon triennal, sur la compétitivité autant que le bilan carbone.

Les organisations qui prendront ce virage disposeront d'un avantage durable, les autres, tôt ou tard, découvriront que la dépendance est une dette dont les intérêts composent plus vite que la croissance.

Chapitre 4 – Données : capital informationnel sous pression

4.1 Classification, sensibilité et valeur économique des données

La mutation de l'économie vers l'intangible est désormais chiffrée : en 2025, 90 % de la capitalisation reposent sur des actifs immatériels (SP) : essentiellement des corpus de données propriétaires et les droits qui leur sont attachés.

Dans le même temps, la quantité de données atteindra 393,8 zettaoctets en 2028, soit presque dix fois le volume de 2018.

Autrement dit : la valeur numérique double plus vite que le PIB mondial, mais il échappe de plus en plus aux mécanismes de contrôle traditionnels.

NB : les tendances à l'IA de réutiliser l'IA sans capacité à l'identifier pourrait à amener à encore plus de données mais avec une valeur inversement qualitative.

Classifier ou périr.

Le premier verrou de souveraineté consiste à séparer l'essentiel de l'accessoire. La norme ISO/IEC 27001 :2022 rappelle quatre niveaux de confidentialité : public, interne, confidentiel, restreint, fondés sur la combinaison CIA (Confidentialité, Intégrité, Disponibilité), chaque classe détermine les modalités de chiffrement, de journalisation et de rétention.

Sans ce balisage, aucune politique de sécurité ne résiste plus de vingt-quatre heures à un audit.

Multi-réglementation, multi-vecteurs.

Les schémas sectoriels (HIPAA pour la santé, PCI-DSS pour la carte bancaire, NIST 800-53 pour le secteur public US, RGPD pour les données personnelles) imposent leur propre granularité.

La même base peut donc cumuler jusqu'à six statuts juridiques, chacun assorti d'obligations contradictoires (chiffrement irréversible versus capacité d'effacement).

D'où l'émergence des data stewards chargés de croiser classification technique et obligations réglementaires : une fonction qui, dans certains groupes du CAC 40, relève déjà du comité des risques.

Combien vaut une colonne SQL ? Le marché noir donne une réponse cynique : carte bancaire complète, 10 à 240 $, permis de conduire 150 $, passeport US 50 $, soit quelques centimes par attribut lorsque l'information est vendue en lot.

Le delta entre le prix criminel et l'amende RGPD (jusqu'à 4 % du CA mondial) matérialise la prime de gouvernance dont jouissent les entreprises capables de contenir les fuites.

Le coût du manquement. Selon l'édition 2025 du rapport IBM Cost of a Data Breach, la violation moyenne se chiffre à 4,44 millions USD, la proportion grimpe à 10,22 millions aux États-Unis.

Plus instructif : 51 % de la facture proviennent de la perte d'opportunités commerciales, preuve que la valeur se niche moins dans la donnée elle-même que dans la confiance qu'elle inspire.

Pression réglementaire croissante. Côté européen, le cumul des amendes RGPD dépasse 6,2 milliards € à fin juillet 2025, tendance +34 % sur douze mois.

Plus la donnée est sensible, plus l'arbitre facture l'imprudence, incitant à passer d'une logique de "mise en conformité" ponctuelle à une logique d'inventaire permanent piloté par IA, les Data Protection Cockpits fleurissent dans les tableaux de bord exécutifs.

4.2 Impacts des flux transfrontaliers sur la confidentialité

Le Data Act rebat les cartes internes UE.

Tout fournisseur devra fournir, sur demande, un extract de données "dans un format structuré, couramment utilisé et lisible par machine" et s'engager sur la réversibilité.

La portabilité cesse d'être un droit théorique, elle devient exigible, donc budgétée.

Extraterritorialité persistante.

Le CLOUD Act américain, toujours sans équivalent en Europe, rappelle qu'une assignation fédérale peut forcer un hyperscaler à livrer les données d'une filiale française, même hébergées à Paris, aveu réitéré par Microsoft devant l'Assemblée nationale en mai 2025.

Asie : durcissement chinois, approche indienne "liste noire".

Toute donnée jugée "importante" par le régulateur de Pékin nécessite un audit de sécurité avant export, le périmètre exact reste flou (bien sûr), mais inclut souvent les schémas d'acheminement logistique et les datasets d'IA.

À New Delhi, la loi autorise les transferts partout sauf vers les pays "blacklistés" dont la liste révisable sans préavis.

La certitude juridique recule, le coût d'assurance monte.

Effet domino sur la cartographie SI.

Chaque fois qu'une localisation obligatoire surgit, les architectes doivent répliquer les entrepôts, dupliquer les pipelines ETL, revoir les modèles de gouvernance.

Le processus nécessite une mobilisation de moyens CAPEX et OPEX non négligeables qui peut mettre à mal les organisations les plus fragiles.

4.3 Gouvernance, éthique et enjeux de sobriété numérique

Gérer, c'est arbitrer.

La gouvernance de la donnée ne se limite plus au data lineage, elle englobe l'éthique, la résilience et l'empreinte carbone.

Les grands comptes adoptent des Data Councils où le CDO dialogue avec le Chief Sustainability Officer et le CISO.

La règle n°1 : tout nouvel usage doit prouver une valeur métier et un "ROI carbone" positif mesuré en grammes CO_2/Mo stocké.

AI Act : l'éthique passe en production.

Depuis février 2025, les obligations de transparence s'appliquent déjà aux modèles génériques, dès août 2026 les systèmes à haut risque devront fournir journaux, données d'entraînement et métriques de biais.

Ceci implique de conserver certaines données pour traçabilité, tout en appliquant la minimisation.

Sobriété numérique : le facteur énergétique.

L'IEA projette une consommation électrique des data centers à 945 TWh en 2030, pour comparer : ceci correspond à l'ensembles des consommations électriques du Japon.

Attention, les charges liées à l'IA quadrupleraient sur la période.

Dans le même temps, le Shift Project rappelle que la production de matériel et la multiplication des redondances pèsent plus lourd que l'usage lui-même dans le bilan carbone global.

Le principe de lean data (moins de copies, plus de qualité) gagne donc les roadmaps des systèmes d'information.

Du "privacy by design" au "sobriety by design".

Les équipes d'ingénierie introduisent des métriques d'efficience, temps de rétention glissante, compression sans perte, tiering automatique vers le stockage sur bande et déclenchent des alertes réglementaires lorsque le seuil de pertinence s'estompe.

Cette approche, longtemps cantonnée à la DSI, devient un critère de notation extra-financière : les agences ESG intègrent l'empreinte numérique dans le pilier E dès la campagne 2026.

Éthique de la donnée : le facteur humain.

La multiplication des data trusts : dispositifs où un tiers fiduciaire administre les droits d'usage pour le compte des individus, préfigure une responsabilisation collective.

Les data stewards devront arbitrer entre l'exigence analytique (modèles prédictifs), la conformité (droit à l'oubli) et la sobriété (droit à l'effacement anticipé).

La compétence devient rare, elle migre du juridique vers l'ingénierie sociale du changement.

La donnée est simultanément ressource, responsabilité et résidu : ressource parce qu'elle alimente l'avantage compétitif, car sa fuite se paie en millions et en réputation, résidu enfin, parce qu'elle encombre serveurs et bilans carbone lorsqu'elle n'est plus utile.

Classer, localiser, gouverner et alléger, tels sont les quatre verbes cardinaux de la souveraineté documentaire.

À l'heure où chaque zettaoctet nouveau ajoute une strate de vulnérabilité, la valeur d'une application ne se mesure plus seulement à la pertinence de son algorithme, mais à la maîtrise de sa chaîne de données.

Le chapitre 5 examinera comment la dilution de la maîtrise opérationnelle : externalisation, shadow IT, obsolescence des compétences, amplifie encore cette pression.

Chapitre 5 – Dilution de la maîtrise opérationnelle

5.1 Externalisation, cloud public, SaaS : entre agilité et perte de contrôle

L'entreprise moderne a d'abord délégué ses baies de disques, puis ses serveurs applicatifs, puis son pipeline de déploiement tout entier, à présent, elle confie même l'orchestration de ses modèles d'IA à des plates-formes serverless.

Le mouvement s'est imposé sous l'étendard de l'agilité : plus de 90 % des organisations utilisent aujourd'hui au moins un service cloud et 60 % d'entre elles y exécutent déjà la moitié de leurs charges critiques, contre 39 % en 2022.

Les budgets suivent : les dépenses mondiales en cloud public devraient s'établir à 1 000 milliards $ en avant 2028.

Pour le comité de direction, ces chiffres racontent une promesse : investissement CAPEX minimal, élasticité quasi instantanée, time-to-market raccourci.

Pourtant, derrière l'effet de levier financier se profile un effet de levier de dépendance.

Les études FinOps rappellent que 20 % des décideurs ne savent toujours pas ventiler leurs coûts réels par produit, et plus de 97 % des applications cloud consommées seraient… non sanctionnées par l'IT, autrement dit, provisionnées sans modèle de gouvernance formel.

La facilité comptable dissimule donc un brouillard de facturation, de conformité et de résilience.

Le risque n'est pas théorique.

Le 7 décembre 2021, une panne réseau dans la région us-east-1 d'AWS a paralysé Netflix, Robinhood, Disney+, les commandes Alexa et des milliers de back-offices logistiques pendant plusieurs heures, le même incident s'est reproduit le 15 décembre.

Rappel : un unique point de défaillance chez un hyperscaler suffit à geler des pans entiers d'économie et l'entreprise cliente n'a aucune maîtrise sur les délais de rétablissement.

Face à cette asymétrie, certains acteurs optent pour la re-patriation partielle : déplacer vers un cloud privé les charges à forte intensité transactionnelle ou sensible en termes de conformité.

Les retours d'expérience divergent, mais le vendor lock-in n'est pas irréversible, pourvu que l'on dispose du capital tampon et des compétences internes.

5.2 Shadow IT et prolifération des API tierces

L'externalisation massive alimente un phénomène connexe : le Shadow IT.

En 2025, une entreprise gère en moyenne 275 applications SaaS et l'IT ne supervise que 26 % de la dépense correspondante.

Gartner estime que ce Shadow IT représente 30 à 40 % des budgets numériques hors contrôle et génère 34 milliards $ de licences inutilisées chaque année dans le seul périmètre États-Unis/Royaume-Uni.

S'y ajoute le coût du risque : le cyber-incident moyen lié à un service non autorisé frôle 4,2 M.

Cette zone grise prolifère via les API dépendant parfois de tiers invisibles : bibliothèques de paiement, services d'identification, connecteurs low-code.

L'analogie change : on ne sécurise plus un château mais un conglomérat de ports commerciaux fortifiés.

Chaque API est une porte de service, chaque porte délègue son verrou à un fournisseur tiers.

La moindre négligence dans la chaîne d'appels peut transformer un incident local en sinistre systémique.

Pourtant, les équipes métiers continuent d'adopter six nouvelles applications SaaS par mois.

Sans gouvernance centralisée, la surface d'attaque croît plus vite que les contrôles et le RSSI se retrouve à colmater rétroactivement des flux qu'il n'a pas validés.

Le piège : les règlements européens (NIS 2, DORA) exigent, en cas d'incident, une capacité à produire sous quatre heures la cartographie des dépendances affectées.

Or 42 % des applications en production ne sont pas répertoriées dans l'inventaire officiel.

5.3 Obsolescence des compétences internes et talent gap en cybersécurité

L'autre face de la médaille est humaine.

La planète compte 5,5 millions de professionnels cyber… mais accuse un déficit de 4,8 millions de postes, en hausse de 19 % sur un an.

Officiellement, 47 % des besoins mondiaux en cybersécurité restent insatisfaits.

Le NIST rappelle qu'en 2025, plus d'un incident significatif sur deux aura pour cause un manque de talents ou une erreur humaine.

Pour contourner la pénurie, les directions privilégient désormais l'IA, la fréquentation des ateliers d'acculturation à l'IA a bondi de 36 % par rapport à la moyenne.

Bon pour l'innovation, ce modèle risque pourtant d'élargir l'écart entre équipes DevOps et équipes SecOps : les premières explorent des modèles génératifs, les secondes manquent de profils capables d'en vérifier la robustesse.

La dynamique salariale ajoute de la tension : après deux années de gel dans la Big Tech, les spécialistes Zero-Trust et API security voient leur

rémunération totale progresser de 11 % en moyenne, contre 3 % pour les administrateurs systèmes généralistes (données internes auteur, 2025).

Les départs volontaires explosent dans les SOC : syndrome de l'alerte permanente, dérégulation du rythme circadien, exposition médiatique en cas d'incident.

L'organisation n'est pas seulement en quête de bras, elle cherche un capital.

L'externalisation prolongée a vidé les équipes internes de compétences sur l'architecture réseau, la containerisation bas niveau, la cryptographie appliquée.

Lorsque survient une panne majeure ou une assignation Cloud Act, le DSI découvre que la "réversibilité" du contrat bute sur l'inexistence d'opérateurs capables de relancer un cluster PostgreSQL hors SaaS ou de réhydrater un blob S3 vers un objet On-Prem.

Les programmes d'insertion accélérée se multiplient : 55 % des responsables recrutent via des filières d'apprentissage, tandis que 75 % disposent encore d'un budget de formation.

Mais les effets sont différés : la montée en compétence d'un analyste SOC junior prend douze à dix-huit mois, tandis qu'un attaquant exploite une CVE critique dès sa divulgation publique grâce à des solutions clef en main dans le DarkWeb en souvent moins de sept jours.

En cumulant externalisation, Shadow IT et pénurie de talents, l'entreprise moderne affronte une dilution accélérée de sa maîtrise opérationnelle.

Le risque n'est plus circonscrit à la DSI, il s'étend au modèle économique :

Dépendance technologique : un incident chez un prestataire unique peut suspendre la facturation, la logistique, le support client.

Opacité budgétaire : 40 % de la dépense numérique échappe au contrôle, faussant le pilotage financier.

Fragilité humaine : l'effritement des compétences internes contraint la stratégie de réversibilité, lèse la conformité NIS 2/DORA et renchérit l'assurance cyber.

La souveraineté, ici, n'est ni idéologique ni protectionniste, elle se mesure en capacité à reprendre la main dans un délai compatible avec la continuité d'activité.

Ceci suppose :

1. Un inventaire vivant des services externalisés (workloads, données, API) et des coûts de bascule associés.

2. Un programme de réduction du Shadow IT couplé à une découverte automatique des SaaS et à un sandbox d'expérimentation cadrée.

3. Un plan de revitalisation des compétences critiques : reverse mentoring, filières d'apprentissage, redéfinition des parcours experts assortis d'incitations de long terme.

Le chapitre 6 détaillera la gouvernance de cette trajectoire : pilotage par indicateurs de dépendance, implication du conseil d'administration et alignement DSI-DAF-DRH autour d'un budget de souveraineté pluriannuel.

Partie II – Les solutions : gouvernance, architecture et trajectoire de souveraineté

Chapitre 6 – Construire une gouvernance de la souveraineté

Lorsque l'entreprise réalise que son indépendance numérique se joue autant dans la salle du conseil que dans le datacenter, la question cesse d'être technique : elle devient culturelle.

Or, toute culture a besoin d'un système de gouvernance pour s'exprimer, d'autant plus lorsqu'elle doit concilier trois forces rarement alignées : l'appétit d'innovation, la peur du risque et l'urgence réglementaire.

Ce chapitre propose donc un fil conducteur : installer le pilotage de la souveraineté dans les organes de décision, tisser un lien organique entre DSI, direction générale et directions juridiques, puis ancrer cet édifice dans un jeu d'indicateurs qui transforment une intention abstraite en progression tangible.

6.1 Rôle du conseil d'administration et des comités stratégiques

Un champ de responsabilité étendu

Le conseil d'administration a longtemps porté la cybersécurité comme un simple item d'agenda.

Avec la souveraineté, il hérite d'une dimension supplémentaire : assurer la maîtrise durable des actifs informationnels, ce qui couvre à la fois la continuité de service, la localisation des données, la réversibilité contractuelle et la protection contre l'extraterritorialité.

Autrement dit, le conseil n'est plus seulement garant d'un seuil de sécurité, il devient gardien d'une capacité stratégique d'autonomie.

Trois leviers d'influence

1. **La charte de souveraineté :** un document de quelques pages, adossé au règlement intérieur, qui définit le périmètre d'application (données, infrastructures, partenariats, compétences) et fixe les principes de décision (préférence aux standards ouverts, obligation de clause de sortie, contrôle des clés de chiffrement, etc.).

Sa force ne tient pas à la précision technique, mais au fait qu'elle émane du plus haut niveau de gouvernance.

2. **Le comité souveraineté :** dérivé du comité audit ou du comité RSE, il fédère administrateurs, spécialistes externes et dirigeants exécutifs.

Sa mission : challenger les dossiers d'investissement pour s'assurer qu'ils intègrent un volet "dépendance" et qu'ils prévoient des plans B réalistes.

3. **La feuille de route annuelle ou triennale :** plutôt qu'un plan figé, le conseil valide une trajectoire en jalons (audit initial, quick wins, chantiers structurants, retours d'expérience) et exige un point d'étape à chaque trimestre.

Cette cadence permet de garder le sujet vivant sans tomber dans la microgestion.

La compétence supervisée

Le conseil n'a pas forcément la technicité requise pour évaluer la partie technique, il doit donc se doter d'experts indépendants, invités réguliers ou membres permanents.

Leur rôle : traduire le jargon opérationnel en scénarios de risques et d'opportunités à la portée des administrateurs.

Cette hybridation des savoirs évite deux écueils : la naïveté (croire que le risque est nul parce que tout fonctionne aujourd'hui) et le catastrophisme (penser qu'il faut rapatrier chaque octet à tout prix).

6.2 Alignement DSI -> direction générale -> juridique

Une triangulation indispensable

La souveraineté s'apparente à une équation à plusieurs inconnues : la DSI veut réduire la dette technique, la direction générale cherche l'avantage concurrentiel (et devrait y être aidé par le DSI), le juridique sécurise la conformité (et devrait également y être aidé par le DSI).

Si chacun avance isolément, le résultat est paradoxal : des infrastructures robustes mais trop chères, des innovations rapides mais invendables, ou des contrats étanches mais bloquants.

Le contrat de réciprocité

Pour sortir de ce triangle d'incompréhension, il faut formaliser un contrat interne :

La DSI s'engage à documenter l'architecture cible, à chiffrer le coût de sortie et à identifier les points de non-négociation (clefs sous contrôle interne, formats ouverts, conditions de surveillance légale, etc.).

Le juridique s'engage à intégrer ces exigences techniques dans les clauses contractuelles et à négocier des mécanismes d'alerte précoce (notifications de changement de licence, audits tiers, droits, etc. ...).

La direction générale arbitre les priorités, valide les budgets et tranche les conflits objectifs entre time-to-market et maîtrise à long terme.

Ce pacte ne tient que s'il est inscrit dans le système de pilotage.

Plusieurs entreprises ont testé les "stand-ups de souveraineté" : réunions courtes, multi-disciplinaires, focalisées sur un backlog de dépendances à résorber.

Le bénéfice principal n'est pas la vélocité, mais la fluidité de l'information : chaque partie perçoit l'impact de ses décisions sur les autres.

Entre libertés locales et cohérence globale

Les métiers réclament souvent la possibilité d'expérimenter un outil SaaS sans passer par la gouvernance centrale.

Accorder cette flexibilité est compatible avec la souveraineté, à condition de poser deux garde-fous :

1. Parcours balisé : tout service externe doit passer par un "sas d'expérimentation" de durée limitée, après quoi il est soit industrialisé, soit supprimé.

2. Patrimoine documentaire minimal : même un POC doit produire un inventaire des données, des dépendances et des licences employées.

Ce socle facilite l'industrialisation future ou la désinstallation ordonnée.

6.3 Indicateurs de pilotage : de la dépendance à la résilience mesurable

Pourquoi mesurer ?

Sans métriques, la souveraineté reste un slogan.

Mais mesurer ne signifie pas empiler des chiffres, il s'agit de choisir des indicateurs lisibles par tous, reflétant l'esprit du cadre fixé par le conseil et suffisamment ancrés dans l'opérationnel pour guider les arbitrages.

Trois familles d'indicateurs

1. Exposition

Indice de concentration fournisseur : à quel point un service critique dépend-il d'un acteur unique ?

Pourcentage de code sous licence propriétaire non négociable : plus cette part est élevée, plus la marge de manœuvre diminue.

Surface API non cartographiée : encore une identification du Shadow IT.

2. Réversibilité

Temps de bascule testé : durée nécessaire pour migrer une charge vers l'alternative prévue (cloud privé, autre fournisseur, solution open-source).

Couverture de clauses de sortie : proportion de contrats intégrant des engagements fermes de migration accompagnée.

Disponibilité de SBOM : taux d'applications possédant un inventaire logiciel à jour, condition sine qua non pour corriger vite.

3. Résilience

Marge opérationnelle de continuité : capacité à tenir l'activité si un fournisseur majeur est indisponible.

Autonomie des compétences : ratio entre les tâches critiques maîtrisées en interne et celles entièrement sous-traitées.

Taux de tests de crise réussis : exercices de panne simulée validant les scénarios de repli.

Visualisation et rythme

Un tableau de bord trop dense décourage l'action.

Beaucoup d'organisations retiennent cinq à sept indicateurs clés, présentés sur une page.

Le rythme, lui, dépend de la maturité : mensuel la première année, trimestriel quand la discipline est rodée.

L'essentiel n'est pas la perfection du chiffre, mais la dynamique : les courbes doivent montrer une tendance à la réduction de la dépendance et à l'augmentation de la résilience.

Le récit pour donner du sens

Les indicateurs chiffrés n'ont d'impact que s'ils s'accompagnent d'un récit : pourquoi avons-nous choisi un double fournisseur pour la signature électronique ? Comment la formation d'une équipe interne PCA ou PRA (selon les moyens allouables) améliore-t-elle notre marge de continuité ?

Raconter ces liens convertit le tableau de bord en levier d'adhésion.

Gouverner la souveraineté, c'est accepter une transformation silencieuse : celle qui déplace le pouvoir de la simple conformité vers la capacité d'orientation stratégique.

Le conseil d'administration y gagne un rôle de sentinelle éclairée, la DSI, la direction générale et le juridique apprennent à fonctionner comme un organe unique, les indicateurs deviennent non des sanctions, mais des cibles claires.

Le chemin est exigeant, mais il confère un atout décisif : l'assurance de ne pas être tributaire d'une décision extérieure pour poursuivre sa trajectoire d'innovation.

Un changement de licence, une tension géopolitique ou une panne d'hyperscaler peuvent rebattre les cartes en une nuit, cette assurance vaut autant qu'un brevet ou qu'un portefeuille client.

Le chapitre 7 ouvrira maintenant la boîte à outils technique : architectures de confiance, stratégies multi-cloud et cloud souverain.

Car la gouvernance, si elle reste conceptuelle, doit trouver un terrain d'application, c'est là que l'ingénierie rencontre la vision, et que la souveraineté cesse d'être une théorie pour devenir un avantage concurrentiel tangible.

Chapitre 7 – Architectures de confiance et cloud souverain

Les chapitres précédents ont montré qu'une gouvernance solide reste lettre morte si l'infrastructure sous-jacente demeure prisonnière d'un modèle d'exploitation opaque ou d'un fournisseur unique.

L'enjeu n'est donc plus simplement de « poser le sujet » au conseil d'administration : il faut traduire l'ambition de souveraineté en choix d'architecture, en gestes d'ingénierie et en routines de pilotage quotidien.

Ce septième chapitre propose un itinéraire en trois étapes : orchestrer plusieurs clouds sans perdre l'élasticité qui fait leur attrait, protéger les données jusque dans la mémoire vive grâce au confidential computing et à des coffres-forts cryptographiques souverains, enfin, tirer les leçons de celles et ceux qui ont déjà bâti un cloud privé de confiance à grande échelle.

7.1 Multi-cloud orchestré : éviter le verrouillage sans perdre l'élasticité

La tentation du multi-cloud est née du même constat que la diversification boursière : ne pas dépendre d'un seul actif.

Pourtant, imposer deux ou trois fournisseurs ne suffit pas, il faut organiser leur coexistence pour qu'elle crée de la valeur.

Autrement dit, multiplier les plateformes doit rimer avec mutualiser l'exploitation.

Le principe d'abstraction

Au-dessus des couches natives des hyperscalers se glisse une strate d'orchestration : Infrastructure as Code pour le déploiement, Policy as Code pour la conformité, Service Enabler pour l'observabilité et la résilience applicative.

Cette superposition agit comme un « langage commun », elle masque les dialectes propriétaires et permet aux équipes de se concentrer sur la logique métier plutôt que sur la syntaxe de chaque cloud provider.

Élasticité conservée, latence maîtrisée

La crainte habituelle est de perdre en agilité : un socle trop générique deviendrait la nouvelle cage dorée.

La solution réside dans la granularité : on abstrait ce qui doit rester portable (réseaux, secrets, déploiements conteneurisés), on laisse chaque fournisseur gérer ce qu'il sait optimiser (accélérateurs IA, services managés à forte valeur ajoutée).

L'effet recherché n'est pas l'homogénéité absolue mais le choix réversible : si une brique devient critique ou trop coûteuse, le plan de replis est déjà industrialisé.

Gouvernance distribuée, visibilité unifiée

Le multi-cloud organisé exige un back-office d'ingénierie de plateforme.

Cette équipe ne « possède » pas les workloads, elle maintient les passerelles : réplicas de registre d'images, logiques de facturation convergentes, métriques alignées.

Un tableau de bord unique recense où tourne chaque service, à quelle échelle, avec quel socle de conformité.

Sans cette visibilité, la pluralité se transforme en opacité.

FinOps et arbitrage temps réel

Une telle architecture ouvre la porte à la mobilité de charges : déplacer un micro-service vers l'infrastructure la plus pertinente au moment T, en fonction de la demande, du instances spot ou d'un impératif réglementaire subitement renforcé.

Ce n'est plus seulement de la continuité d'activité, c'est un levier d'optimisation économique et une assurance contre la captation unilatérale de valeur.

7.2 Confidential Computing, chiffrement end-to-end et HSM souverains

Protéger l'information à l'arrêt et en transit est devenu un réflexe.

Le défi se situe désormais dans la phase d'exécution : quand le processeur manipule des données en clair, une attaque mémoire suffit à déjouer tous les coffres-forts logiques.

D'où l'émergence du confidential computing : des enclaves matérielles qui isolent le calcul d'un système d'exploitation potentiellement compromis.

Enclaves matérielles, racines d'un nouveau modèle de confiance

Les environnements d'exécution protégés créent une bulle dans laquelle le code et les données restent chiffrés, même pour l'hyperviseur.

L'application s'y charge après un rituel d'attestation, le fournisseur de clés ne les libère que si l'environnement prouve son intégrité.

Ainsi, la confiance se déplace du périmètre réseau vers la puce elle-même.

Du chiffrement à trois temps…

1. Au repos : stockage chiffré, segmenté, géolocalisable.

2. En transit : protocoles TLS modernes, mutual TLS entre micro-services, validation stricte des certificats.

3. En usage : enclaves, registres CPU compartimentés, zero-knowledge sur les clés d'API.

… et une quatrième dimension : la gouvernance des secrets.

Les matériels de sécurité matériels (Hardware Security Modules ou HSM) fournissent la racine de confiance, placés sous contrôle

souverain, ils garantissent que la clé maîtresse ne sort jamais du territoire, ni physiquement ni juridiquement.

Clés souveraines, responsabilités partagées

Externaliser une partie de l'infrastructure ne doit pas signifier céder la maîtrise des clés : la gouvernance adopte un modèle dit Bring Your Own Key ou Keep Your Own Key.

Le partage des responsabilités s'ajuste : le fournisseur maintient l'infrastructure, l'entreprise conserve la possession logique des secrets.

Si l'hyperscaler reçoit une injonction extraterritoriale, il se retrouve obligé d'accéder à la clef pour déchiffrer les données (sur demande au client ou automatiquement) : le client de l'hyperscaler est alors informé de cet accès (à défaut de pouvoir s'y opposer).

Cet aspect juridique est susceptible de changer selon les changements de lois internationales : il restera quoiqu'il en soit, très volatile dans les prochaines années.

Anticiper l'après-quantique

Même si les ordinateurs quantiques universels sont encore embryonnaires, la cryptographie post-quantique entre déjà dans les feuilles de route.

Choisir un HSM de nouvelle génération, c'est s'assurer qu'il pourra évoluer pour gérer les futurs algorithmes sans remplacement massif de matériel.

Dans la stratégie de souveraineté, préparer aujourd'hui le chiffrement de demain évite le rush législatif de la dernière minute.

7.3 Retour d'expérience : monter un cloud privé de confiance à l'échelle

Certaines organisations ont franchi le pas : elles opèrent leur propre nuage, conçu pour dialoguer avec les hyperscalers mais capable, en cas de crise, d'héberger l'ensemble des charges vitales.

Que révèle leur parcours ?

Première étape : cadrer la raison d'être

Un cloud privé n'est pas un trophée technique, c'est un outil de maîtrise.

Les pionniers commencent par définir les services indispensables : calcul, stockage objet, base de données relationnelle, orchestrateur de conteneurs, identité.

Le reste peut rester dans le public.

Cette focalisation évite les dérives budgétaires et accélère la livraison de valeur perçue.

Deuxième étape : industrialiser la construction

Le cœur du chantier réside dans l'automatisation.

Chaque composant, de la couche réseau à la console self-service, est définie par code, versionnée, reproduite sur des environnements de test.

Ce principe d'infrastructure immuable permet de déployer, réparer ou étendre sans reconfiguration manuelle.

L'automate devient le premier opérateur, garant de la cohérence.

Troisième étape : brancher la sécurité dès la genèse

Les flux sont micro-segmentés, observables, chiffrés.

Les identités s'alignent sur un annuaire unique qui fédère le privé et le public.

Les journaux d'audit s'agrègent dans une plateforme de détection d'anomalies où règles et modèles se juxtaposent : heuristiques explicables pour la conformité, apprentissage automatique pour la vitesse de réaction.

Quatrième étape : accompagner les équipes

La réussite ne tient pas aux racks mais aux humains.

Les organisations qui réussissent investissent dans un Cloud Enablement Office : un groupe transversal, à mi-chemin entre la DSI et les lignes métiers.

Sa mission : former, documenter, supporter.

Ce bureau incarne l'interface, il transforme une usine technologique en service consommable.

Cinquième étape : tester la réversibilité grandeur nature

Un cloud privé de confiance doit prouver qu'il peut récupérer une charge critique sous pression.

Les meilleurs retours d'expérience reposent sur des game days : simulations de panne hyperscaler, rapatriement d'un micro-service en direct, restitution des journaux de conformité.

Plus la manœuvre devient routinière, moins elle effraie, plus elle crédibilise la posture souveraine.

Écueils fréquents et parades

Complexité perçue : la multiplication des couches fait craindre une machinerie ingérable.

Parade : standards ouverts, documentation exhaustive, pilotage par API unique.

Coût initial : l'investissement matériel et humain semble élevé.

Parade : approche modulaire, retour sur investissement mesuré non en coûts bruts mais en valeur de résilience.

Culture de service : une infrastructure interne peut sombrer dans la bureaucratie.

Parade : traiter les utilisateurs internes comme des clients externes, adopter des SLA clairs, un portail de tickets, une transparence de facturation.

Liaisons avec le multi-cloud

Le cloud privé ne remplace pas l'existant, il complète.

L'hybridation devient un art de l'équilibre : certaines charges restent chez l'hyperscaler pour tirer parti d'accélérateurs spécialisés, d'autres se replient sur le privé lorsqu'un règlement l'impose ou qu'un incident le nécessite.

Construire une architecture de confiance n'est pas un aboutissement technique, c'est un processus continu.

Le multi-cloud orchestré élargit le champ des possibles, mais il n'a de sens qu'adossé à un chiffrement en profondeur et à une gouvernance robuste des secrets.

Le cloud privé de confiance, lui, sert de filet de sécurité : capable d'absorber la criticité sans sacrifier l'innovation.

L'ensemble forme une mosaïque où chaque pièce trouve sa justification : l'orchestration pour l'agilité, le confidential computing pour l'intégrité, le HSM souverain pour la légitimité, le cloud interne pour la résilience.

Cette mosaïque, une fois assemblée, offre un avantage rarement mesuré dans les feuilles de calcul : la liberté tactique.

La pression réglementaire et la volatilité géopolitique peuvent rebattre les cartes en une nuit, la faculté de choisir, et surtout de changer, vaut davantage que la meilleure des remises commerciales.

Le prochain chapitre abordera l'open source, la standardisation et la mutualisation : autant de vecteurs qui, au-delà des architectures, permettent d'inscrire la souveraineté dans une dynamique d'écosystème et de partage.

Chapitre 8 – Open source, standardisation et mutualisation

8.1 Modèles économiques de l'open source souverain

Dès qu'on parle de souveraineté, la première objection surgit : « l'open source, c'est gratuit, est-il vraiment besoin de financer la pérennité ? »

Question trompeuse, parce que la vraie valeur dans le domaine de la souveraineté ne réside pas dans le prix d'entrée, mais dans la capacité à sortir sans rupture.

Le logiciel libre n'est pas une gratuité, c'est un transfert de pouvoir : la liberté d'étudier, modifier et redistribuer le code redistribue la hiérarchie des rôles, faisant de l'utilisateur un co-architecte potentiel.

Les modèles économiques se structurent autour de cette liberté :

Abonnement de support : l'exemple le plus iconique reste Red Hat, le client achète la connaissance, les correctifs en avance et un engagement de continuité, pas le droit d'usage (enfin pas toujours).

Cette logique transforme le risque technique en contrat de service, donc en ligne budgétaire prévisible plutôt qu'en dette cachée.

Open-core : cœur libre, extensions propriétaires (tableaux de bord, connecteurs, fonctions premium).

La souveraineté consiste à vérifier que les briques critiques (format de données, moteur d'exécution, protocole réseau) restent dans la partie ouverte, afin de garder la faculté de forker si l'éditeur change de licence.

Dual-licence : un même code coexiste sous licence libre et commerciale, utile pour imposer le respect de la marque ou empêcher l'intégration non coopérative d'un concurrent.

Sponsoring public / commande mutualisée : la campagne Public Money / Public Code popularise l'idée que tout logiciel financé par l'impôt doit être versé au bien commun, déclenchant une dynamique de marché inversé : la puissance publique n'achète plus un produit, elle cofinance un espace logiciel partagé.

La Suisse l'a récemment inscrit dans la loi, prouvant la faisabilité politique d'un tel modèle.

La souveraineté y gagne sur trois plans : maîtrise du code, mutualisation des coûts de maintenance et alignement des intérêts entre parties prenantes.

Plus important encore, ces modèles encouragent la création d'OSPO (Open-Source Program Offices) : cellules internes qui assurent la conformité des licences, encouragent la contribution montante et orchestrent la stratégie de libération de code.

Une organisation dotée d'un OSPO (souvent services à mission publique) robuste transforme la collaboration externe en avantage stratégique, car elle gouverne mieux la dette technique, attire les talents qui veulent "donner du sens" et limite la dépendance à un fournisseur unique.

8.2 Interopérabilité par les standards ouverts : ODF, OpenAPI, Gaia-X

La promesse open source s'étiole si les formats restent fermés.

Standardiser, c'est garantir que les données produites aujourd'hui resteront lisibles demain, quel que soit le destinataire ou l'outil.

ODF, la continuité documentaire

Depuis son inscription dans la norme ISO/IEC 26300, l'Open Document Format a démontré qu'un format n'a pas besoin de dominer le marché pour sécuriser un patrimoine : il suffit qu'il soit public et suffisamment outillé pour éviter l'enfermement.

Des administrations portugaises à certaines agences de l'ONU, le choix d'ODF n'a jamais été idéologique, il répond au besoin concret de récupérer un dossier sans dépendre d'une licence périmée.

OpenAPI, la grammaire universelle des micro-services

À mesure que les architectures se décomposent, savoir "parler" à un service devient vital.

L'OpenAPI Specification, portée par la Linux Foundation, formalise la description d'un endpoint HTTP, rendant auto-documentées des API autrefois opaques.

Cette expressivité est souveraine : un consommateur peut changer de prestataire sans réécrire son client, à condition que chacun respecte la même sémantique.

Gaia-X et l'ère des data spaces

L'initiative européenne Gaia-X pousse l'idée plus loin : les standards ne concernent plus seulement le format, mais la confiance autour de la donnée.

Le Trust Framework fournit un langage commun pour attester la provenance, la localisation, la politique d'usage.

À Varsovie, lors du Symposium 2025, les experts ont rappelé : « La donnée se déplace à la vitesse à laquelle on lui fait confiance ».

En d'autres termes, un fichier peut traverser les frontières juridiques si le contrat d'usage reste lisible par machine, interopérable et vérifiable.

Du protocole au contrat dynamique

L'étape suivante, déjà à l'œuvre dans plusieurs pilotes Gaia-X, consiste à lier le contrat d'échange à des politiques en temps réel : un algorithme de recommandation ne peut appeler un dataset santé que si la VM s'exécute dans une enclave certifiée, sinon la requête est refusée à la volée.

L'interopérabilité devient comportementale : même format, mêmes conditions d'usage, même preuve de conformité, quel que soit l'opérateur cloud.

8.3 Communautés, fondations et partenariats académiques

La force d'un écosystème

Une technologie ouverte ne survit pas sans communauté vivante.

Linux Foundation Europe, OW2, Eclipse, Apache : autant d'organismes où entreprises, chercheurs et individus confluent pour codéfinir feuilles de route et répartir la charge de maintenance.

Les grandes organisations y siègent pour trois raisons : veiller à ne pas être mises de côté, attirer les experts et influencer les orientations stratégiques.

Fondations sectorielles et verticalisation

De plus en plus, on observe des fondations verticales : FINOS pour la finance, LF Energy pour l'énergie, LF AI & Data pour l'intelligence artificielle.

Ces coalitions concentrent l'effort sur des référentiels métiers et empêchent la prolifération de solutions ad-hoc.

Pour une entreprise, contribuer signifie réduire le "temps au standard" : ce qu'elle livre aujourd'hui en open source devient la base d'un consensus qui simplifie ses intégrations futures.

Universités et laboratoires comme accélérateurs

Les partenariats académiques complètent la boucle.

Là où l'industrie vise la stabilité, la recherche explore les ruptures : cryptographie post-quantique, compilation différentiable, réseaux déterministes.

Inscrire ces innovations dans un projet open source permet de partager le risque amont et d'accélérer la diffusion aval.

L'université gagne en visibilité, l'entreprise peut dérisquer son prototype, la communauté hérite d'un point de départ solide.

Mutualisation et chaîne de confiance

La mutualisation n'est pas qu'une question financière, elle relève de la chaîne de confiance.

Chaque commit signé, chaque pull request validé, renforce la résilience globale : un bug corrigé pour un acteur profite à tous, un audit de sécurité partagé diminue l'exposition collective.

Les programmes de bug-bounty communautaires démontrent ce cercle vertueux : plutôt que payer seuls une chasse aux vulnérabilités, les contributeurs financent le pot commun et bénéficient des corrections en même temps.

L'enjeu de la gouvernance

Reste la gouvernance : qui décide de la roadmap ?

Pour un projet souverain, la gouvernance doit être méritocratique, transparente et neutre.

Méritocratique pour récompenser la contribution, transparente pour éviter les décisions de couloir, neutre pour empêcher la capture par un acteur dominant.

Lorsqu'un consortium s'érige en gardien, le code de conduite, les règles de vote et la licence deviennent les garde-fous qui garantissent la continuité du projet au-delà des fluctuations de marché.

Exemple de l'ANSSI en France.

Vers un "capital communautaire"

Certaines directions financières commencent à considérer la participation à l'open source comme un capital immatériel : ligne budgétaire justifiée non pas par le chiffre d'affaires immédiat, mais par la réduction de risque, la visibilité marque-employeur et la capacité d'innovation distribuée.

En langage souveraineté, cela se traduit par une phrase simple : « Plus nous contribuons, moins nous dépendons. »

L'open source n'est pas seulement une alternative économique, c'est la matrice organisationnelle qui permet de transformer la dépendance en interdépendance choisie.

Les modèles de soutien (abonnement, open-core, loi Public Code), les standards (ODF, OpenAPI, Gaia-X) et les communautés (fondations, universités, consortiums sectoriels) forment un triptyque cohérent : chacun renforce l'autre pour convertir l'intention de souveraineté en réalité opérationnelle.

En pratique :

Évaluer la criticité des briques libres sur lesquelles repose l'entreprise.

Soutenir financièrement et en ressources les projets stratégiques.

S'asseoir à la table des fondations pour y prendre part au vote.

Aligner les contrats internes sur les standards ouverts pour garantir la portabilité.

Mesurer la contribution (commits, revues, documentation) comme indicateur de maturité souveraine.

Plus l'organisation s'implique, plus elle récolte : une veille technologique amplifiée, une capacité de négociation accrue, une attractivité RH rehaussée, une résilience partagée.

Dans les domaines aussi technologiques que les systèmes d'information, la vitesse d'évolution dépasse la capacité d'un acteur isolé, miser sur l'ouverture revient à investir dans la durabilité collective.

Le chapitre 9 prolongera cette dynamique côté sécurité : Zero Trust, identités fédérées, automatisation de la réponse aux incidents.

Car la confiance bâtie par le code et les standards trouve son plein potentiel lorsqu'elle s'ancre dans des architectures défensives résolument proactives.

Chapitre 9 – Sécurisation renforcée et gestion des identités

Dans la littérature stratégique, on répète que « la donnée est le nouveau pétrole ».

Cette métaphore est commode, mais elle occulte l'essentiel : ce qu'un gisement d'hydrocarbures est au géologue, l'identité numérique l'est au cyber-architecte.

Sans un cadre robuste pour identifier, authentifier et autoriser, toute ressource numérique : serveurs élastiques, algorithmes d'IA, jumeaux industriels, devient un puits sans garde-fou, offert aux déversements toxiques.

Or l'espace numérique contemporain n'est plus un désert : c'est un entrelacs de pipelines, chacun greffé à des terminaux mobiles, des API publiques, des clouds multi-régions.

La sécurité, jadis périmétrique, se réinvente en mouvement, la défense doit se hisser au rythme d'une supply-chain logicielle devenue fractale.

Ce neuvième chapitre explore trois leviers pour reprendre prise : le modèle Zero Trust, la fédération souveraine des identités et l'automatisation de la réponse aux incidents.

9.1 Zero Trust : principes et contraintes de mise en œuvre

Changer d'échelle mentale

Le Zero Trust commence par une rupture cognitive : ne plus supposer qu'un système interne est plus fiable qu'un hôte externe.

On ne parle pas ici de paranoïa institutionnalisée, mais d'un constat empirique : l'attaquant n'entre pas, il est déjà là : Dans la messagerie, dans le conteneur mal configuré, parfois dans l'agent de supervision lui-même.

Le paradigme déplace donc la barrière du château vers une multitude de guérites microscopiques.

Chaque requête devient un événement à interroger : Qui es-tu ? Que veux-tu faire ? Dans quel état se trouve ton terminal ?

Cinq briques cardinales

1. Inventaire vivant : l'organisation doit savoir, en continu, quels actifs existent, qui les possède et dans quel état de patch ils se trouvent.
   Sans cette matrice, toute politique granulaire reste théorique.

2. Authentification forte et continue : l'utilisateur (ou la charge machine) prouve son identité à chaque étape significative, pas uniquement lors de la connexion initiale.

3. Micro-segmentation : chaque service n'expose que les ports nécessaires et parle avec des identités plutôt qu'avec des adresses IP.

4. Chiffrement systématique : trafic interne ou externe, production ou test, peu importe, la confidentialité n'est plus optionnelle.

5. Orchestration de politiques : un moteur de décision central arbitre, en temps quasi réel, la validité d'une session au regard du contexte (localisation, heure, posture du terminal, classification de la donnée).

Les contraintes invisibles

Mettre ces principes en musique révèle très vite des frictions.

Les applications héritées, pensées pour un réseau "plat", n'acceptent pas la segmentation fine sans ré-écriture.

Les bases de données refusent parfois de voir leur port fermé hors d'une liste blanche dynamique.

Les équipes métiers se plaignent de latences nouvelles, les analystes de sécurité croulent sous des journaux d'accès qui doublent chaque trimestre.

Le Zero Trust exige donc une discipline d'ingénierie : cartographier les flux, réduire la fonctionnalité superflue, écrire des playbooks de déploiement qui incluent tests de régression et simulations de panne.

Vers la confiance calculée

Une fois la mécanique rodée, l'organisation découvre un bénéfice subsidiaire : la confiance devient métrique.

Le moteur de politique, nourri par la télémétrie, attribue un score de risque, module les privilèges, ferme la session si un comportement sort des bornes.

La sécurité cesse d'être un binaire (autorisé/interdit) et adopte la nuance : elle négocie, à chaque instant, le degré d'accès nécessaire et suffisant.

9.2 Identité numérique et fédération souveraine

L'identité comme nouvelle frontière

Si l'on croit la maxime Zero Trust (« never trust, always verify »), l'identité se mue en exigence : plus qu'un badge, c'est un contrat contextuel entre deux entités.

Pour qu'il vive, encore faut-il un registre fiable, des attributs vérifiables et un protocole d'échange interopérable.

Self-Sovereign Identity (SSI) : promesse et prudence

Le courant SSI propose de replacer le contrôle des attributs personnels dans les mains de l'individu.

Un utilisateur présente la preuve d'un droit (âge, diplôme, permission d'accéder) sans divulguer davantage.

Techniquement élégant, le modèle se confronte à deux réalités :

Les régulateurs exigent une traçabilité minimale pour lutter contre la fraude et le blanchiment.

Les entreprises doivent garantir la révocation rapide d'un droit si l'employé quitte l'organisation.

L'équation se résout donc par un compromis : SSI pour la portabilité, gouvernance centralisée pour la révocation.

On parle alors de fédération souveraine : des fédérations d'identité qui dialoguent entre elles tout en conservant l'ancrage juridique de leurs jetons.

Fédération intra-groupe, puis inter-gouvernementale

À l'échelle d'un groupe international, la première marche consiste à unifier les annuaires internes : une identité, une authentification, un ensemble de rôles, quelle que soit la filiale.

Vient ensuite la fédération externe : partenaires industriels, sous-traitants, voire administrations.

L'avantage souverain apparaît lorsque l'entreprise peut, en un clic, basculer la confiance d'un partenaire vers un autre, sans re-créer des comptes ni exposer un login partagé.

Confidentialité et minimalisme

Plus la fédération grandit, plus l'appétit des services pour les attributs augmente.

Le principe d'attribut minimal devient un garde-fou : ne partager qu'une information prouvée pertinente (par exemple "est-employé-actif", pas la date de naissance), signer la preuve, chiffrer le contenu.

Ainsi, un identifiant perd sa valeur hors du périmètre prévu.

C'est l'anti-thèse du login unique.

9.3 Automatisation de la réponse aux incidents : SOAR et IA de défense

Du réflexe au réflexe orchestré

À l'ère de la détection temps réel, l'analyste humain se trouve saturé, la menace se mesure en millisecondes, la réaction manuelle en minutes.

Les plateformes SOAR (Security Orchestration, Automation and Response) surgissent comme chefs d'orchestre : elles ingèrent alertes, les corrèlent, enrichissent le contexte, puis déclenchent des playbooks automatisés.

Playbooks vivants

Un playbook n'est pas un script figé, c'est un arbre de décision vivant, mis à jour à chaque débriefing d'incident.

Il isole un segment réseau, révoque un jeton, alerte le responsable conformité, ouvre un canal et initie donc les conditions de salle de crise.

Son efficacité tient à la justesse du contexte : si l'annuaire de référence ou la CMDB est obsolète, l'automate coupe parfois la mauvaise branche.

Maintenir la vérité d'inventaire devient donc un acte de défense active.

Intelligence artificielle : promesse d'anticipation

L'essor de l'IA embarque deux facettes :

L'IA d'observation repère des anomalies subtiles dans un océan de journaux (changement d'empreinte de code, latence inhabituelle, chaîne d'API non habituelle).

L'IA générative élabore, à la volée, un résumé d'attaque, propose un correctif, génère même un pull request pour un micro-patch.

Mais la prudence s'impose : un modèle peut biaiser, halluciner, se tromper de priorité.

La bonne pratique consiste à marier vitesse machine et supervision humaine : l'algorithme détecte, l'analyste confirme, le SOAR déploie le remède.

Apprentissage continu et boucle d'amélioration

Chaque incident clos nourrit la base d'entraînement.

Les indicateurs ne se limitent plus au temps moyen de détection, on mesure le debrief to deploy : délai entre la leçon tirée et la mise à jour du playbook, reflet tangible de la résilience apprenante.

Vers la cyber-observabilité intégrale

À l'horizon, on entrevoit la fusion entre télémétrie système, journal applicatif et empreinte utilisateur.

La défense affiche sous un même graphe, les dérives de comportement.

Là où l'œil humain sillonnait des dashboards, le moteur IA tisse une carte heuristique, pointe un écart, propose de fermer le port qui deviendra la faille demain.

Zéro Trust, fédération d'identité, automatisation : trois strates, une même ambition.

La première bâtit la trame d'un réseau où le privilège n'est jamais acquis, la deuxième fournit la monnaie d'échange, un jeton d'identité fiable et minimaliste, la troisième orchestre la défense, transforme l'alerte en action sans déléguer la stratégie à l'algorithme.

Ensemble, elles redéfinissent la surface de contrôle : elle n'est plus l'enceinte du data-center ni la seule application critique, mais chaque requête, chaque morceau de code, chaque décision d'accès.

La souveraineté, sous cet angle, n'est pas un repli sur soi, c'est une faculté à naviguer dans un océan de dépendances sans s'y dissoudre.

Elle se construit par couches successives : un modèle d'accès granulaire, un passeport numérique fédéré, un réflexe défensif amplifié par la machine.

Le chapitre 10 tirera le fil jusqu'à la conduite du changement : comment traduire ces mécanismes techniques en feuille de route humaine, gouverner la montée en compétences et inscrire la résilience dans la culture quotidienne.

Chapitre 10 – Trajectoire de transformation et conduite du changement

10.1 Audit de maturité souveraine : grille d'évaluation pas-à-pas

Avant tout projet de rééquilibrage, il faut un diagnostic lucide.

L'audit de maturité souveraine n'est ni un "pen-test" déguisé, ni un rapport d'audit financier, c'est un miroir opérationnel qui révèle les dépendances invisibles et souvent visibles mais reniées, mesure la capacité de repli et décèle les blocages culturels.

Il s'organise autour de cinq axes, chacun scoré de 0 à 5, la somme, sur 25, dessine la position de départ.

1. Gouvernance et stratégie

0 : aucune mention formelle de la souveraineté dans les organes de décision.

3 : charte approuvée, calendrier de reporting, budget dédié mais encore cantonné à la DSI.

5 : feuille de route validée par le conseil, indicateurs suivis en comité stratégique, arbitrages budgétaires tranchés au prisme de la dépendance.

2. Architecture et réversibilité

- 0 : infrastructures mono-fournisseur, pas de plan de sortie.
- 3 : multi-cloud orchestré, catalogues de services classifiés selon leur criticité, tests de restauration annuels.
- 5 : cloud privé de confiance prêt à absorber les charges vitales, exercices de bascule trimestriels, couverture automatisée des SBOM.

3. Données et conformité

- 0 : inventaire manuel, flux transfrontaliers non documentés.
- 3 : classification à quatre niveaux, pilotage des flux par politiques, gouvernance inter-fonctions.
- 5 : traçabilité temps réel, chiffrement end-to-end piloté par clés souveraines, démonstration d'effacement sélectif en moins de 24 h.

4. Sécurité et identité

- 0 : périmètre plat, authentification périmétrique.
- 3 : Zero Trust partiel (accès distants), fédération d'identité interne, détection d'anomalies centralisée.
- 5 : Zero Trust complet, passeport d'identité souverain, SOAR orchestrant réponse et post-mortem.

5. Compétences et culture

- 0 : dépendance totale à des intégrateurs externes.
- 3 : équipe cœur de plateforme, programme de formation en cours, budgets de formation sécurisés.
- 5 : filière d'expertise souveraineté interne active, contributions open source récurrentes, indicateurs RH alignés sur la rétention.

Le bilan n'est pas une sanction, c'est la possibilité de création d'une cible.

En pratique, un score global entre 8 et 12 signale un niveau "apprenti" : l'organisation commence à parler souveraineté mais ne sait pas encore la pratiquer.

Entre 13 et 18, elle entre dans la phase "artisan" : les briques existent, l'alignement reste fragile.

Au-delà de 19, elle devient "orchestrateur", capable d'imposer à ses fournisseurs des clauses de sortie et de partager ses bonnes pratiques.

Le but n'est pas d'atteindre mécaniquement 25 / 25, mais de choisir les axes qui créent le plus de valeur et d'y concentrer l'effort.

10.2 Feuille de route triennale : quick wins, chantiers structurants, capitalisation

Trois ans : un horizon suffisamment long pour transformer la culture, assez court pour rester lisible au conseil.

La feuille de route emprunte la logique "volant d'inertie" : engrenger des victoires rapides qui alimentent l'élan politique, puis investir cet élan

dans des chantiers lourds, enfin capitaliser pour enclencher un cycle vertueux.

Année 1 – Créer la traction

Quick wins techniques

Rationaliser le Shadow IT : recensement automatique des SaaS, désactivation des doublons, économie de licences visible sur la ligne budgétaire.

Pilote Zero Trust périmètre nomade : déployer l'authentification forte, micro-segmenter l'accès VPN, mesurer la chute des tentatives d'intrusion.

Migration des documents stratégiques vers un format ouvert : bascule silencieuse vers ODF ou Markdown, démonstration de continuité hors abonnement.

Quick wins organisationnels

Charte souveraineté signée : deux pages, diffusées du COMEX au terrain.

OSPO léger : un chargé de mission et deux référents techniques, mandatés pour cartographier les dépendances open source.

Dashboard MVP : cinq indicateurs clés partagés en comité risques.

Année 2 – Structurer et industrialiser

Chantiers structurants

Cloud privé de confiance (MVP) : cluster Kubernetes interne, stockage objet chiffré, pipeline CI/CD miroir. Objectif : absorber un service critique en test de bascule.

Fédération d'identité partenaires : protocole OIDC, wallet eIDAS v2, attributs minimaux.

Phase pilote avec un écosystème limité.

Politique Data LifeCycle : créer l'outil interne de tiering et d'effacement, adosser la sobriété numérique aux règles d'archivage.

Capital humain

Parcours re-skilling : 15 % de l'effectif IT formés à la containerisation, certification interne "Architecte de confiance".

Communauté de pratique : rituels mensuels, revue de code open source, visibilité des contributions sur l'intranet RH.

Année 3 – Étendre et capitaliser

Extension technique

Multi-cloud orchestré complet : passer de deux zones critiques à l'ensemble du portefeuille applicatif, avec routage dynamique.

Confidential Computing standard : enclaves généralisées pour tout workload requérant niveau "restreint".

SOAR en production : couverture 24/7, playbooks vivants, boucle post-incident vers backlog DevSecOps.

Capitalisation et diffusion

Reporting intégré ESG : la souveraineté devient un chapitre officiel du rapport RSE, avec métriques carbone et dépendance numérique.

Partenariats académiques : bourses doctorales, projets de chaire, attractivité RH accrue.

Transfert au comité risques : le pilotage se fond dans la gouvernance entreprise, la DSI n'est plus seule à porter le sujet.

La feuille de route n'est pas linéaire : chaque cycle trimestriel réévalue les priorités, quitte à avancer un chantier ou en repousser un autre.

Ce pragmatisme rassure le financier (grip budgétaire), le juriste (agilité réglementaire) et le métier (livraison régulière de valeur).

10.3 Gestion des compétences : re-skilling, attractivité et culture de la souveraineté

La technologie se déploie à la vitesse des neurones, pas des rack-servers.

Sans compétences internalisées, le cloud privé reste une coquille vide, le Zero Trust un projet pilote éternel, l'OSPO un trompe-l'œil.

La souveraineté n'est donc pas seulement une affaire de choix d'outils, mais de transformation des profils.

Trois cercles de talent

1. Noyau d'architecture : architectes d'entreprise, SRE, ingénieurs cybersécu.

Ils définissent la cible, rédigent la doctrine, arbitrent les exceptions.

2. Population de relais : chefs de projet, développeurs, analystes data.

Ils déclinent la doctrine dans chaque chantier.

3. Ambassadeurs métier : responsables opérationnels, product owners, fonctions support.

Ils transforment la souveraineté en valeur métier, vulgarisent l'intérêt.

Le plan de re-skilling

Cartographier les lacunes : pour chaque rôle critique, préciser la compétence absente (Infrastructure as Code, cryptographie appliquée, FinOps, CI/CD sécurisé).

Cet inventaire nourrit un skills backlog comme on alimente une backlog agile : tâche, effort, dépendances.

Formations hybrides : 30 % e-learning, 30 % ateliers pair-à-pair, 40 % projets réels coachés.

Le programme s'étale sur douze mois, module court par module court, chaque séquence se conclut par un livrable concret (module Terraform dans le Git interne, fiche pratique sur le wiki maison).

Mentorat inversé : le talent n'est pas toujours où on l'attend.

Un ingénieur de vingt-cinq ans, rompu au bug bounty, coachera un administrateur réseau senior, en retour, il absorbera la culture du legacy et du risque opérationnel. L'échange croisé brise les silos générationnels.

Mobilité interne valorisée : un développeur qui migre vers l'OSPO se voit crédité d'un bonus variable indexé sur les contributions open source, pas uniquement sur la vélocité des livraisons.

Ainsi, la gouvernance n'est plus une "voie de garage", mais un tremplin reconnu.

Attirer et retenir

Marque employeur "souveraineté" : conférences, articles de blog sous licence libre, participation aux hackathons publics.

Le message est clair : "Ici, vous codez pour libérer, pas pour enfermer."

Cette narration attire les profils en quête de sens, rarissimes dans un marché saturé.

Politique contributive : deux jours par mois peuvent être consacrés à un projet open source stratégique.

L'entreprise ne perd pas du temps, elle gagne un carnet d'adresses communautaire et des correctifs que ses propres équipes n'auraient jamais eu la bande passante de produire.

Rétention par la responsabilité : au lieu d'un package salarial démesuré, offrir un droit de parole dans la roadmap et un accès aux instances de décision.

Les ingénieurs seniors ne partent pas pour quelques billets de plus, mais parce qu'ils n'influent plus.

Donnez-leur la main sur la souveraineté, ils resteront.

Installer la culture

La culture ne se déclare pas, elle se pratique.

Trois rituels cimentent l'esprit souverain :

Revue mensuelle des dépendances : 60 minutes, tous projets confondus, pour passer au crible les nouveaux paquets, licences, API tierces.

La transparence désamorce le blâme.

Game Day Souveraineté : simulation d'une coupure de région cloud ou d'une révocation de licence critique.

On découvre les points de friction et on apprend à collaborer sous tension.

Fête des contributions : chaque trimestre, un after-work (non obligatoire, les gens ont des familles) où l'on célèbre les pull requests acceptées, les premiers tests de bascule réussis, la plus belle clause de sortie négociée.

La reconnaissance alimente la motivation.

La transformation souveraine ne suit pas une ligne droite, elle procède par spirales.

Le diagnostic révèle, la feuille de route oriente, la compétence incarne.

Petit à petit, le tissu organisationnel absorbe une nouvelle norme : on ne juge plus un projet à la seule vélocité ou au seul coût, mais à sa capacité d'autonomie.

Quand cette métrique devient réflexe, la souveraineté cesse d'être un objectif, elle devient un angle d'attaque naturel, un filtre stratégique, une partie intégrante de la culture d'entreprise.

À l'issue de ce parcours, le lecteur dispose d'une vue complète : comprendre les risques (Partie I) et activer les leviers de gouvernance, d'architecture et de conduite du changement (Partie II).

Reste à ancrer ce savoir dans l'action quotidienne : c'est là que se joue, en silence, le véritable avantage concurrentiel pour demain.

Et maintenant …

Le moment d'agir n'est pas 2030, il est maintenant, avant que la prochaine faille zero-day, le prochain arrêt d'usine ou la prochaine clause extraterritoriale ne transforme la dépendance en crise ouverte.

Cinq décisions, simples à formuler, exigeantes à tenir, peuvent faire la différence.

1. Inscrire la souveraineté au rang des objectifs stratégiques. Pas comme un volet de la cybersécurité, mais comme un critère de compétitivité comparable à l'innovation produit ou à la rentabilité financière.

2. Allouer un budget pluriannuel dédié.
La souveraineté est un investissement, pas un coût de mise en conformité.
Elle requiert des CAPEX (infrastructure de confiance) et, surtout, des OPEX de long terme (support open source, up-skilling, contribution communautaire).

3. Nommer un responsable exécutif transversal.
CDO, CTO ou nouvellement "Chief Sovereignty Officer", ou même CIO dans les PME, peu importe le titre : il doit avoir autorité pour arbitrer entre ligne métier, IT et juridique, et siège au comité exécutif.

4. Mesurer, réviser, communiquer.

Choisissez une poignée d'indicateurs : surface de dépendance, temps de bascule testé, pourcentage de code maîtrisé, taux de contribution open source.

Affichez-les trimestriellement, sans complaisance, comme on affiche un chiffre d'affaires ou un bilan carbone.

5. Cultiver la compétence comme un capital.

Financer des chaires académiques, ouvrir le code non stratégique, offrir aux ingénieurs la possibilité de peser sur la roadmap.

Un talent qui comprend les enjeux de souveraineté et se sent partie prenante restera plus fidèle qu'aucun bonus à court terme ne pourrait l'acheter.

Dans l'histoire industrielle, la compétitivité s'est longtemps jouée sur l'accès aux matières premières, puis aux capitaux, puis au marché mondial.

Désormais, elle se joue sur la plasticité structurée : cette capacité à maintenir la cohérence de l'organisation tout en réallouant, presque à la volée, ses ressources numériques.

Les pages qui précèdent vous ont offert la cartographie, les outils, les trajectoires.

Il ne manque plus qu'un acte de leadership : choisir, dès aujourd'hui, de gouverner votre capital informationnel avec la même rigueur que votre capital financier.

Le reste n'est qu'exécution, exigeante, certes, mais désormais éclairée.

Retrouvez des ressources souveraines et entièrement écrites en Français sur le site DYNAMAP SI : www.dynamap.fr

Yann-Eric DEVARS – Fondateur Solve DSI