



Souveraineté d'entreprise



Souveraineté numérique

Yann-Eric DEVARS

Table des matières

Avant-propos	6
Partie I – Les problématiques : décryptage des vulnérabilités et des dépendances	15
Chapitre 1 – La souveraineté, une exigence stratégique	15
1.1 Évolution historique : de la simple disponibilité à la souveraineté complète	15
1.2 Risques macro-économiques : cyber- instabilité, ruptures d’approvisionnement, extraterritorialité des lois	18
1.3 Quand la dépendance technologique devient un risque systémique.....	20
Chapitre 2 – Pressions réglementaires et géopolitiques.....	24
2.1 RGPD, NIS 2, DORA : panorama des obligations européennes.....	24
2.2 Cloud Act, FISA : l’effet extraterritorial des régulations non européennes	26
2.3 Vers des blocs numériques : fragmentation ou redéfinition de l’Internet ?	29
Chapitre 3 – Chaînes d’approvisionnement et « vendor lock-in »	32
3.1 Cartographie des dépendances matérielles et logicielles	32
3.2 Modèles de licences et captation de valeur...	35

3.3 Cas d'école : migrations inverses coûteuses et faillite d'éditeurs critiques	38
Chapitre 4 – Données : capital informationnel sous pression	42
4.1 Classification, sensibilité et valeur économique des données	42
4.2 Impacts des flux transfrontaliers sur la confidentialité.....	45
4.3 Gouvernance, éthique et enjeux de sobriété numérique	46
Chapitre 5 – Dilution de la maîtrise opérationnelle..	50
5.1 Externalisation, cloud public, SaaS : entre agilité et perte de contrôle.....	50
5.2 Shadow IT et prolifération des API tierces.....	52
5.3 Obsolescence des compétences internes et talent gap en cybersécurité	53
Partie II – Les solutions : gouvernance, architecture et trajectoire de souveraineté.....	58
Chapitre 6 – Construire une gouvernance de la souveraineté.....	58
6.1 Rôle du conseil d'administration et des comités stratégiques	59
6.2 Alignement DSI -> direction générale -> juridique	61
6.3 Indicateurs de pilotage : de la dépendance à la résilience mesurable	63

Chapitre 7 – Architectures de confiance et cloud souverain	68
7.1 Multi-cloud orchestré : éviter le verrouillage sans perdre l'élasticité.....	68
7.2 Confidential Computing, chiffrement end-to-end et HSM souverains	71
7.3 Retour d'expérience : monter un cloud privé de confiance à l'échelle.....	74
Chapitre 8 – Open source, standardisation et mutualisation	79
8.1 Modèles économiques de l'open source souverain	79
8.2 Interopérabilité par les standards ouverts : ODF, OpenAPI, Gaia-X.....	81
8.3 Communautés, fondations et partenariats académiques	83
Chapitre 9 – Sécurisation renforcée et gestion des identités.....	89
9.1 Zero Trust : principes et contraintes de mise en œuvre	90
9.2 Identité numérique et fédération souveraine .	92
9.3 Automatisation de la réponse aux incidents : SOAR et IA de défense	94
Chapitre 10 – Trajectoire de transformation et conduite du changement.....	99

10.1 Audit de maturité souveraine : grille d'évaluation pas-à-pas	99
10.2 Feuille de route triennale : quick wins, chantiers structurants, capitalisation	102
Année 1 – Créer la traction	102
Année 2 – Structurer et industrialiser	103
Année 3 – Étendre et capitaliser	104
10.3 Gestion des compétences : re-skilling, attractivité et culture de la souveraineté	106
Et maintenant	112

Avant-propos

Les entreprises de la fin de l'ère industrielle, encore engourdis 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 1^{er} 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.