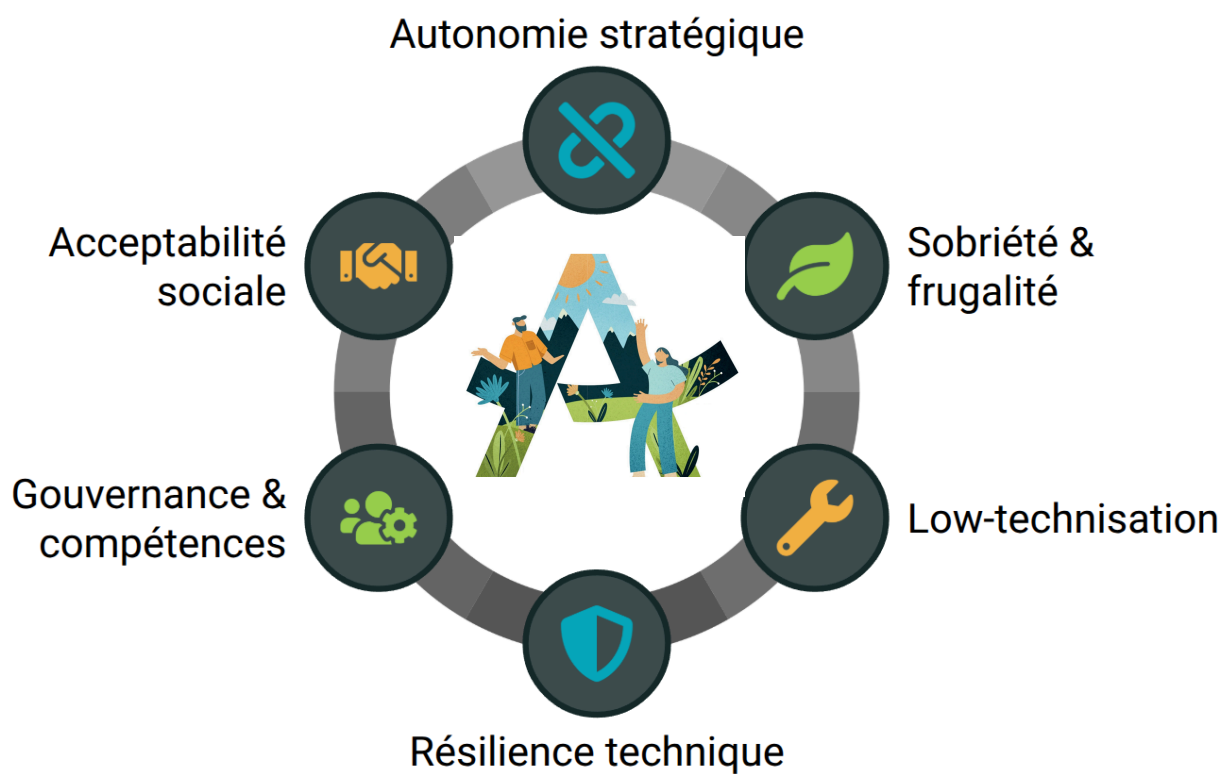


Sobriété et robustesse : repenser notre approche d'un Système d'Information soutenable

Clément Marche, Nuageo

Version relecture



Sommaire commenté

Introduction - Marseille, 2030 : un train part à l'heure pendant qu'une région cloud s'effondre. Personne ne remarque rien, et c'est le but.

Première partie. Le diagnostic

1. L'empreinte, nécessaire mais insuffisante - Le numérique responsable a couvert l'empreinte. Restent les choix qu'on ne questionne pas, et la solidité de ce qu'on construit.

2. La soutenabilité faible du numérique - Optimiser sans questionner le cadre, consomme en silence la marge du SI : ce qu'il garde en réserve pour tenir sous contrainte, sous cinq formes qui ne se rachètent pas dans l'urgence. Les conditions stables qui rendaient ce pari rationnel ont disparu.

Deuxième partie. La thèse

3. La robustesse comme condition de soutenabilité forte - Maintenir la fonction pendant et en amont du choc. Ça se paie en sous-optimalité, et c'est le prix de la durée.

4. Le filtre du bien commun - On ne peut pas tout rendre robuste sans reproduire l'excès qu'on dénonce. La santé commune décide de ce qui mérite l'effort.

Troisième partie. Mise en œuvre

5. Six leviers pour un SI soutenable - Les gestes par lesquels une DSI cesse de consommer sa marge, sous ses cinq formes.

6. Commencer : voir ce qu'on ne voyait pas - Exposer le SI aux chocs, concevoir sous contrainte, évaluer honnêtement. Six mois pour remédier aux vulnérabilités les plus béantes.

7. Ce que ça change pour le DSI - Tenir la trajectoire change le métier : de gestionnaire de performance à garant de la marge, celle qui fait tenir le service sur la durée.

Conclusion - Quand la robustesse fonctionne, il ne se passe rien. Tout ça pour ça ? :)

Introduction

Gare de Marseille, 6h47, un jeudi de 2030. Léa ajuste sa veste sur le quai. Le TGV de 6h54 pour Paris l'attend. Réunion à 10h avec un investisseur, pour un dossier qui peut faire basculer les six prochains mois de la petite entreprise qu'elle a créée. Les écrans d'information clignotent, une fois, deux fois, puis s'éteignent. Dans le micro, la voix cafouille avant de disparaître. Autour, les regards se croisent. « C'est pas possible. » « J'ai trois rendez-vous à Paris aujourd'hui. » Une mère calme son fils qui demande ce qu'il se passe. Un peu plus loin, un homme âgé se tourne vers une agente en gilet rouge : son application mobile n'affiche plus rien, et les panneaux restent noirs. Léa sent ce froid familial au creux du ventre, celui des projets qui basculent. Elle ne sait pas qu'à cet instant, une région cloud vient de lâcher en Europe centrale, emportant une partie des systèmes informatiques dont sa journée dépend.

Sept minutes plus tard, les écrans se rallument. Texte brut, sans les couleurs ni les animations habituelles. Son téléphone vibre dans sa poche. Pas une notification : le Wi-Fi de la gare est coupé. C'est un SMS, envoyé directement par le réseau mobile : « *Votre TGV 6h54 pour Paris : voie 4, à l'heure.* » Elle ouvre l'application : les cartes temps réel ne chargent plus, mais l'essentiel s'affiche en texte : itinéraire, numéro de voiture, billet. Dans son malheur, quelque chose semble tenir le coup.

Le TGV 6h54 pour Paris partira à l'heure. Dans le train, le contrôleur avance dans le wagon avec un terminal qui semble tout droit sorti d'une autre décennie, et il valide les billets sans sourciller. Deux gares plus loin, un chef de quai sort une liste d'embarquement imprimée le matin même, on embarque à l'ancienne. L'agente en gilet rouge, elle, a sa propre liste papier, et elle accompagne les voyageurs qui semblent les plus déroutés. Le train roule. Les conversations, d'abord inquiètes, glissent vers l'étonnement. « Ça tient. » « C'est bizarre, mais ça tient. » Léa relit ses notes. Elle arrivera à temps.

Ce qui s'est joué pendant les sept minutes où elle avait peur, c'est ceci. Quelques années plus tôt, dans une DSI dont elle ne connaîtra jamais l'existence, quelqu'un a défendu un budget pour un datacenter de secours régional. Quelqu'un a exigé un mode local dans l'application. Quelqu'un a imposé un exercice trimestriel sur une ligne test, en conditions réelles, pour ne jamais découvrir la panne en pleine crise. Quelqu'un a refusé de remplacer un parc de terminaux qui fonctionnait encore, même quand un fournisseur expliquait qu'il fallait passer à la nouvelle génération. Quelqu'un a protégé une équipe technique interne, capable de reprendre la main si un prestataire ne répondait plus. Quelqu'un a défendu qu'un numéro vert avec un humain au bout reste ouvert, pour les voyageurs qui ne se débrouilleraient pas seuls. Quelqu'un a tenu cette trajectoire quand tous les autres parlaient d'optimisation et de réduction de coûts.

Pourquoi ce train est-il parti ? Parce qu'en amont, le système d'information qui le pilote a été pensé comme un système robuste, engagé sur le chemin de la soutenabilité forte. Deux notions qui reviendront dès la fin du premier chapitre. C'est la clé d'un SI qui tient dans un monde qui fluctue. Comment on y arrive ? C'est l'objet de ce manifeste. Il

s'adresse à celles et ceux qui pilotent un SI et pressentent que l'optimisation les a conduits dans une impasse, sans avoir encore les mots pour le défendre devant leur direction. Il vise à aider celles et ceux qui doivent convaincre, avec un détour obligé pour commencer : comprendre pourquoi le numérique responsable, tel qu'on le pratique aujourd'hui, ne produit pas ce train-là. C'est le travail des deux premiers chapitres.

PREMIÈRE PARTIE. Le diagnostic

Le train de Léa qui part à l'heure, malgré tout, est une promesse. Ce qui la tient, ce sont des choix faits des années en amont, à rebours de la logique dominante : un mode local dans l'application, des terminaux qu'on n'a pas remplacés, une équipe capable de reprendre la main. Chacun a coûté un arbitrage contre l'optimisation - celle qui pilote les SI, qui pousse à centraliser, renouveler, externaliser. Et la seule démarche qui, depuis quinze ans, invite les DSI à regarder plus loin que la performance, le numérique responsable, ne rattrape pas ce manque : elle mesure, sensibilise, écoconçoit, mais elle travaille l'empreinte, pas la solidité de ce qu'on construit. C'est un acquis réel, et rien ici ne propose de le jeter. Reste que rien dans cet outillage ne fait partir ce train-là. D'où le détour qui ouvre ce livre : regarder en face ce qu'on fait déjà - optimiser, et compenser l'empreinte - avant de dire ce qu'il faut changer pour tenir la promesse.

Cette première partie établit le diagnostic en deux temps. D'abord ce que le Numérique Responsable (NR) a réellement couvert, et ce qu'il a laissé intact : les choix de numérisation, la solidité de ce qu'on construit. Ensuite ce que cette absence produit : une logique d'optimisation qui opère en soutenabilité faible, le chapitre 2 posera le terme, et qui consomme, sans la voir, la marge dont dépend la capacité du SI à soutenir les usages de son organisation sur la durée.

Chapitre 1. L'empreinte, nécessaire mais insuffisante

Retour en 2026, loin du quai de Marseille. Le numérique responsable s'est installé dans certaines organisations, dans la réglementation, dans les pratiques. Certes, cela reste parfois modeste mais les évolutions sont réelles. Un écosystème structuré a émergé pour accompagner les organisations dans la mesure et la réduction de leur empreinte environnementale numérique. Des référentiels existent : le RGEN (référentiel général d'écoconception de services numériques) pour les services numériques, l'AFNOR SPEC 2314 pour l'IA, etc. Des compétences se développent, des postes se créent. Mais est-ce que cela suffira pour faire partir le train de Léa en 2030 ?

Et c'est là que le bât blesse : cette dynamique, aussi réelle soit-elle, s'est concentrée sur une fraction de ce que le mot « responsable » promet.

Un cadre plus ambitieux qu'on ne le croit

Le numérique responsable, tel qu'il a été posé par ses acteurs historiques, ne se réduit pas à l'empreinte carbone. GreenIT a ouvert le sujet au début des années 2010 en montrant que le numérique n'avait rien d'immatériel : métaux critiques, énergie, eau, biodiversité, cycle de vie complet des équipements. L'impact social couvre l'accessibilité, l'inclusion, la fracture numérique, les conditions de travail dans les chaînes d'approvisionnement ou dans les conditions de traitement en fin de vie. Les questionnements éthiques interrogent les données personnelles, l'économie de l'attention, les dark patterns. La question des usages se pose à travers le filtre des 3U : Utile, Utilisable, Utilisé.

La définition de l'INR (Institut du Numérique Responsable) montre l'étendue de l'ambition d'origine : *« réduction de l'empreinte économique, sociale et environnementale du numérique, capacité du numérique à réduire l'empreinte de l'humanité, création de valeur responsable pour réussir l'inclusion de toutes et tous »*.

Le périmètre est large. Trop large, peut-être, pour les moyens qu'on lui a donnés. Mais c'est le périmètre revendiqué.

Alors qu'en a-t-on fait ?

On n'a fait qu'effleurer la surface : par facilité, angle mort ou habitude

Dans la pratique, la démarche s'est concentrée sur les aspects environnementaux : les plus accessibles, ceux qui ne remettent pas en cause les habitudes.

La sensibilisation d'abord, autour des Fresques et des ateliers qui, dans beaucoup d'organisations, étaient à la fois le point de départ et la finalité du sujet. La mesure, via des bilans carbone dont les conclusions restaient souvent lettre morte. Le recyclage via des politiques de gestion des DEEE. Plus ambitieuses déjà, les démarches d'écoconception ou l'allongement de la durée de vie des terminaux.

La hiérarchie d'action publiée par la DINUM au début des années 2020 (*Guide de bonnes pratiques NR*, DINUM et MiNumEco, 2021) plaçait pourtant l'allongement de durée de vie

du matériel en haut de la pile, et les éco-gestes individuels en bas. Dans la pratique observée, l'ordre s'inverse souvent et ce sont les pratiques marginales qui sont les plus répandues : vidons nos boîtes mails, ça réglera le problème. Non ?

Le GreenOps illustre bien le plafond de verre. Une DSI lance un programme de juste dimensionnements (right-sizing) cloud : on identifie les instances surdimensionnées, on redimensionne, on coupe les ressources inutilisées. La facture baisse de 20 %. Le bilan carbone s'améliore : gagnant-gagnant ? Six mois plus tard, le budget libéré a financé trois nouveaux projets, et la consommation totale a dépassé son niveau de départ. On a optimisé sans questionner l'usage global. On a fait mieux, pas moins : un bel exemple d'effet rebond.

Cependant, ces choix ne sont pas à dramatiser : les actions engagées vont dans le bon sens, et que de progrès depuis cinq ans sur le sujet ! Mais ce n'est que le début. On optimise l'existant sans interroger ce qu'on fait, ni la solidité de ce qu'on construit.

Pourtant, les chiffres qui suivent justifieraient largement l'effort à fournir. Ils justifieraient même qu'il soit bien plus important ! Le numérique en France représente 11 % de la consommation électrique (ADEME, 2025), 4,4 % des émissions de gaz à effet de serre, soit 29,5 MtCO₂e (ADEME, janvier 2025, données 2022), et 2,2 % de la consommation d'eau (iNUM, 2020). Pour fixer les ordres de grandeur : 11 % de l'électricité, c'est environ 50 TWh, la production annuelle de huit réacteurs nucléaires ; 29,5 MtCO₂e, c'est près de la moitié des émissions annuelles de la circulation automobile française. La fabrication des terminaux concentre environ 84 % de leur empreinte carbone propre (ADEME, 2025). Le Shift Project, en octobre 2025, chiffre la consommation électrique des datacenters mondiaux à 420 TWh en 2024 contre 120 TWh en 2005, et projette 1 250 à 1 500 TWh à l'horizon 2030 si la tendance se maintient. Dit autrement : les datacenters du monde consomment déjà presque autant d'électricité que la France entière, et pourraient en consommer trois fois plus qu'elle en 2030.

Le cas Microsoft vaut qu'on s'y arrête. Les émissions liées aux achats, équipements et services grimpent depuis 2020. La consommation électrique, elle, a été multipliée par 2,8 entre 2020 et 2024, passant de 10,8 à 29,8 TWh (rapports environnementaux Microsoft 2024 et 2025), soit à peu près la consommation électrique annuelle de l'Irlande. Tout cela alors que Microsoft s'est engagé en 2020 à être « carbon negative » d'ici 2030 : un bilan carbone négatif, c'est-à-dire retirer de l'atmosphère plus de carbone qu'on n'en émet. La cause principale est la croissance du cloud et l'adoption massive des modèles d'intelligence artificielle générative. La non-augmentation des émissions entre 2023 et 2024 tient presque uniquement à une réduction du scope 2, les émissions liées à l'électricité achetée. Cette baisse vient de contrats d'achat d'électricité renouvelable, comptabilisés selon la méthode dite market-based : on retient l'électricité que l'entreprise a contractualisée, pas celle qui circule réellement dans les câbles qui alimentent ses datacenters (méthode location-based). Microsoft progresse sur un indicateur quand la plupart des autres se dégradent. C'est la soutenabilité faible en action, avant même qu'on ait posé le concept.

L'AFNOR SPEC 2314 (juin 2024) définit un « système d'IA frugal » selon deux conditions cumulatives :

- La nécessité de recourir à l'IA plutôt qu'à une solution moins énergivore a été démontrée ; les bonnes pratiques d'efficacité sont adoptées ;
- Les usages et besoins ont été préalablement questionnés et visent à rester dans les limites planétaires.

Le document de l'AFNOR réunit ainsi sous un seul mot ce que nous distinguons ici pour rendre la séquence explicite : la sobriété (questionner le besoin) d'abord, la frugalité (optimiser la réponse) ensuite. Pour rendre l'enjeu concret, un prompt envoyé à un grand modèle de langage consomme quelques wattheures. Mille utilisateurs, cinquante prompts par jour ouvré, deux cent cinquante jours par an : de l'équivalent d'une famille française à une trentaine de foyers, selon le modèle et la longueur des requêtes. Rendre ce système plus efficient est nécessaire. Mais si l'usage lui-même n'a pas passé le filtre de la pertinence, on a un système efficient au service d'une utilité souvent faible.

La majorité de ces calculs se basent sur des données de 2022 : avant l'arrivée de l'IA générative qui se déploie massivement et qui accélérera encore la tendance tant que les investissements annoncés soutiendront cette croissance.

En France, les datacenters pourraient représenter environ 4 % de la consommation électrique en 2035 (23 à 28 TWh selon les scénarios), contre 2 % aujourd'hui (RTE, *Bilan prévisionnel 2025-2035*). La dynamique se lit mieux encore dans les raccordements : en mai 2026, près de 18 GW de puissance étaient réservés auprès de RTE pour environ quatre-vingts projets de datacenters, contre 5 GW fin 2024. Réserver n'est pas consommer, mais l'échelle a changé en dix-huit mois, pas en dix ans (RTE, mai 2026). Pendant ce temps, Google affiche +48 % d'émissions depuis 2019 et Microsoft +30 % depuis 2020, corrélés à l'essor de l'IA générative (*Google Environmental Report 2024, Microsoft 2024 Environmental Sustainability Report*).

Bref : la tendance est à la hausse, qu'on arrive à la décrire précisément ou non, et les démarches NR existantes ne l'inversent pas. Elles la freinent, peut-être, localement mais la structure du système pousse dans l'autre sens. Le Shift Project le résume : les émissions des datacenters croissent de 9 % par an (pré IA générative) quand il faudrait les réduire de 5 %. L'effet rebond le confirme : quand on optimise le coût unitaire d'un service numérique, la consommation globale augmente, que ce soit parce que le service est plus accessible, ou que le budget est réutilisé pour de nouveaux projets qui ont eux aussi un impact. L'ADEME l'a documenté sur le télétravail et sur plusieurs cas d'usage numériques (IT4Green, 2025).

Un paradoxe aggrave le tableau. Le NR mesure l'empreinte d'un SI dont la part externalisée croît chaque année (Cloud, SaaS, IA générative, etc.). Or l'organisation n'a que peu de leviers sur le PUE du datacenter de son hyperscaler, sur son mix énergétique, sur la conception de ses serveurs, encore moins quand elle consomme des services SaaS. Elle mesure (lorsque les données sont disponibles) une empreinte qu'elle maîtrise finalement

de moins en moins. Le bilan carbone peut servir de critère d'arbitrage entre fournisseurs ou entre localisations de datacenters : c'est un outil de choix stratégique, mais la plupart des organisations ne l'utilisent pas ainsi. Il reste un exercice de reporting, pas un outil de décision. Son usage légitime, celui qu'on pratique en diagnostic, reste la comparaison d'ordres de grandeur au moment d'un choix.

Ce travail n'est pas inutile. Simplement, il est insuffisant en l'état. Le mot « responsable » promet davantage. Responsable de ce qu'on choisit de numériser, pas seulement de l'empreinte de ce qu'on produit. Responsable de la dépendance qu'on installe parfois sans le voir. Responsable des personnes qui subissent cette numérisation sans l'avoir choisie. Responsable vis à vis des générations futures à qui nous devons rendre des comptes sur le gâchis de ressources et des impacts associés.

Benoît Petit (Hubblo) a mis les mots sur ce malaise en février 2025, dans une tribune titrée « Le numérique responsable a échoué, mais c'était prévisible ». Sa critique touche juste : cette première génération du NR s'est trop focalisée sur l'optimisation, parfois trop technophile, souvent détachée du propos politique que le sujet portait à l'origine. Le NR est un questionnement sur les pratiques, sur la finalité des usages, et parfois même il peut devenir une porte d'entrée politique pour questionner la raison d'être des organisations qui les déploient. En le réduisant à l'empreinte, on a transformé cette porte d'entrée en cul-de-sac.

Pour que le mot « responsable » retrouve son sens, il faut élargir le cadre. Et pour élargir le cadre, il faut d'abord comprendre pourquoi celui qu'on a utilisé jusqu'ici ne pouvait pas suffire.

L'angle mort social

96 000. C'est le nombre de saisines reçues par la Défenseure des droits en 2024 sur les services publics dématérialisés (*Rapport annuel 2024 de la Défenseure des droits*, mars 2025). Le rétrécissement le plus marqué du NR concerne pourtant cette dimension sociale, qui couvre au moins trois réalités très différentes et aucune n'est réellement traitée.

Les conditions d'extraction et de fabrication d'abord. Travail des enfants dans les mines de cobalt en RDC, minerais de conflit, exploitation humaine, viols, conditions dangereuses dans les usines d'assemblage. On en parle pendant les formations, pendant les ateliers de sensibilisation mais au-delà de quelques clauses d'achats chez les acteurs les plus matures, quelle réalité ces questions ont-elles ? et quelles réalités pourraient-elles avoir ? Les politiques bas carbone occultent ces impacts non climatiques, comme le constate le Cigref dans son rapport sur l'approche low-tech (février 2026).

La fracture numérique et la dématérialisation subie, ensuite. La dématérialisation, c'est le remplacement des guichets physiques et des procédures papier par des démarches exclusivement en ligne, sans alternative maintenue. Plus de huit millions de personnes en France, soit 15,4 % de la population des 15 ans et plus, sont en situation d'illectronisme

(INSEE, *Insee Première* n° 1953, juin 2023, données 2021). À cela s'ajoutent environ 28 % des internautes avec des capacités numériques faibles sur au moins un des cinq domaines de base (recherche d'information, communication en ligne, utilisation de logiciels, protection des données personnelles, résolution de problèmes), selon la même étude. Et ce ne sont pas seulement des « personnes âgées » ou des habitants de « zones blanches », comme on nous le rétorque souvent : ce sont aussi des jeunes dépourvus de compétences administratives, des personnes en situation de handicap face à des sites non conformes, des allocataires radiés parce qu'un mail de convocation n'a jamais été ouvert. La dématérialisation à marche forcée produit de l'exclusion. C'est l'inverse de ce qu'un numérique « responsable » devrait produire.

Plus silencieusement, la perte de compétences. Quand un processus est entièrement numérisé et que plus personne ne sait l'exécuter autrement, on crée une dépendance invisible. Le mécanisme est progressif : adoption, intégration, dépendance, atrophie. Une organisation dont les communications passent par Teams, les documents par SharePoint, les processus RH par un SaaS unique, a progressivement désappris à fonctionner autrement. Elle ne s'en rend compte qu'au moment où ça casse. C'est une forme d'illectronisme opérationnel : une dépendance au sentier qui ne se révèle qu'au moment où l'outil tombe. Il est central, et il n'est presque jamais nommé dans les démarches NR classiques. La raison est simple : c'est un risque qui ne se voit pas tant qu'il n'est pas réalisé. Personne ne mesure une compétence qui s'est lentement effacée.

Au final, le NR dans sa version pratiquée est cantonné à une discipline d'optimisation environnementale du SI. Du Green IT où la « sobriété » se limite à « faire autant avec moins ».

La question des choix

Quand on demande aux équipes SI d'identifier les services critiques de leur organisation (ceux sans lesquels l'organisation ne fonctionne plus), la liste est souvent longue. Quand on leur demande ensuite lesquels ont fait l'objet d'un choix explicite, documenté, arbitré collectivement au-delà du critère technique ou financier, la liste se raccourcit nettement. La numérisation s'est faite par opportunité, par mimétisme sectoriel, tendance sociétale ou nécessité, rarement par réflexion systémique.

Le cadre du NR, tel que généralement appliqué dans les organisations, ne fait qu'effleurer cette question. Le tout premier critère du RGEN demande pourtant : « Ce service numérique est-il nécessaire ? » pose un filtre pertinent en amont de l'écoconception. Mais dans la pratique, ce sont les premières cases qu'on coche sans réellement s'arrêter sur le sujet. On passe directement au « comment rendre ce service moins impactant » sans jamais revenir sur le « fallait-il le numériser sous cette forme ? » De la frugalité, mais peu de sobriété.

C'est pourtant la question la plus structurante. Interroger le besoin, c'est justement poser ces questions avant de construire : au service de quelle finalité ? Compatible avec quelles limites ? Quels usages méritent qu'on leur consacre des ressources rares : énergie,

compétences, dépendance ? Quels usages méritent que des gens se blessent, saignent, transpirent et meurent ?

Ce sont des questions de gestion que n'importe quel(le) DSI confronté(e) à des budgets contraints devrait se poser. Et si ces DSI ne se les posent pas pour des raisons environnementales ou sociales, ils devraient le faire pour des raisons de continuité d'activité.

Empreinte parfois juste effleurée, dimension sociale souvent ignorée, choix rarement arbitrés : ces trois angles morts appellent une définition. Que faut-il, au juste, pour qu'un SI soit soutenable ?

Soutenabilité du SI : de l'atténuation à l'adaptation

La soutenabilité, c'est la capacité d'un système à tenir dans la durée sans épuiser les ressources dont il dépend. Sa version forte ajoute une condition : certaines de ces ressources n'ont pas de substitut, aucune accumulation ailleurs ne les rachète si elles s'épuisent. Un savoir-faire critique dissous quand une équipe part n'est pas rattrapé par une enveloppe budgétaire. Des données détruites sans sauvegarde ne reviennent pas, et la sauvegarde ne se construit pas pendant la panne, ni après. Elle se construit avant.

Un SI soutenable, dans cette lecture, ne se contente donc pas de limiter son impact environnemental. Il maintient ses fonctions essentielles à travers les chocs, et il fonctionne sans engranger de dette - environnementale, sociale ou technique - qui devra être payée plus tard, ou par d'autres.

On peut ainsi résumer la situation du NR en trois cercles concentriques.

- Le premier, bien couvert : l'empreinte environnementale du SI, le sujet le mieux balisé, celui où les référentiels et les outils existent déjà.
- Le deuxième, effleuré sans être approfondi : les choix de numérisation et leurs conséquences sociales.
- Le troisième, largement ignoré : la soutenabilité du modèle lui-même.

Les deux premiers cercles : Réduire l'empreinte - mesurer, écoconcevoir, sensibiliser, questionner les usages, tout ce que les pages précédentes ont décrit - relève de l'atténuation : on agit sur la cause. C'est nécessaire. Mais l'atténuation ne dit rien de ce qui se passe quand le choc est déjà là. À ce moment, il ne s'agit plus d'atténuer, mais de s'adapter.

C'est là que le troisième cercle entre en jeu : est-ce que le SI tient dans la durée, malgré les chocs et les fluctuations d'un monde incertain ? Cette question a un nom : la robustesse, au sens où le biologiste Olivier Hamant l'emploie. Elle désigne la capacité d'un système à maintenir sa fonction malgré les fluctuations, sans attendre le choc pour s'y préparer. La

résilience, elle, suppose le choc puis le retour à la situation nominale : elle tient à condition que le choc s'arrête.

Concrètement : est-ce que les équipes gardent la capacité de fonctionner quand un outil tombe ? Est-ce qu'on conserve la possibilité de changer de fournisseur, de rapatrier ses données, de revenir en arrière ? Est-ce qu'on mesure le coût complet de la dépendance - pas le seul prix de la licence, mais le coût de migration si on doit partir, le coût de l'indisponibilité si le service tombe, le coût de la renégociation quand les tarifs grimpent de 30 % ?

Les chiffres commencent à donner corps à cette fragilité. Les interruptions critiques chez les trois principaux fournisseurs de cloud public - AWS, Microsoft, Google - ont progressé de 18 % en 2024 (Parametrix, 2025). Les dépendances invisibles s'empilent : composants matériels, chaînes d'approvisionnement, cadres juridiques extraterritoriaux. L'Indice de Résilience Numérique (IRN), lancé à Bercy le 26 janvier 2026 par l'association Digital Resilience Initiative (licence CC BY-NC-ND), propose un référentiel ouvert pour mesurer et piloter les dépendances numériques critiques. Le rapport Cigref/INR sur l'approche low-tech (février 2026) invite explicitement à passer d'une logique de performance par la puissance technologique à une logique de performance par la robustesse.

Que ce rapport soit co-publié par l'INR et le Cigref n'est pas anodin : l'un porte le numérique responsable, l'autre la stratégie des directions numériques. Leur convergence dit quelque chose : la robustesse est la dimension manquante du NR.

Que faire quand les crises qu'on cherche à atténuer sont déjà là ? S'adapter. Ou plutôt gagner en adaptabilité, pour viser à la pérennité du SI, des organisations malgré les crises.

Encadré : Pourquoi ce livre dit « soutenable » et pas « durable » ou « responsable »

« Durable » est galvaudé. La confiance du public dans les allégations environnementales des entreprises est passée de 58 % en 2004 à 40 % en 2025 (Greenflex-ADEME). Le mot ne porte plus rien. « Responsable » est trop large : il couvre l'empreinte, l'éthique, l'inclusion, la gouvernance, les achats, donc rien de précis. « Soutenable » renvoie à un cadre théorique (Daly, Costanza) et pose une question opérationnelle : est-ce que ça tient dans la durée, sous contrainte ? C'est un mot qui engage à la preuve, pas à la promesse.

Le NR a couvert le premier tiers (premier cercle) de ce qu'il devrait couvrir. Personne ne devrait revenir en arrière sur la mesure, l'écoconception, la sensibilisation. Le modèle des trois horizons, développé en fin de chapitre suivant, situe le chemin restant dans une grille de lecture qui aide à comprendre pourquoi le NR tel qu'il se pratique n'est qu'un horizon de transition.

La question n'est plus seulement « notre numérique est-il sobre ou « responsable » ? » mais « est-ce qu'il est réellement soutenable, au sens fort - dans un monde complexe et incertain, que ce soit au niveau environnemental, social, économique, énergétique, géopolitique ».

Attention, cela ne veut pas dire qu'on occulte la question environnementale. La sobriété, qui était le point de départ des démarches NR, devient une conséquence d'une approche plus large de soutenabilité, en rendant le numérique compatible avec les limites planétaires - dans sa construction (équipement, serveurs, logiciels) comme dans ses finalités.

Références

- ADEME/Arcep, *Évaluation de l'empreinte environnementale du numérique en France*, 2022.
- Shift Project, *Planifier la décarbonation du numérique*, octobre 2025.
- AFNOR SPEC 2314, *IA frugale*, juin 2024.
- ADEME/Greenworking, *Caractérisation des effets rebond induits par le télétravail*, 2020.
ADEME, *IT4Green. Évaluation environnementale des effets directs et indirects du numérique*, 2025.
- INSEE, 15,4 % de la population de 15 ans et plus en situation d'illectronisme en 2021, *Insee Première* n°1953, juin 2023.
- Baromètre du numérique 2025, INSEE/Arcep/ANCT, février 2026.
ADEME, *Guide anti-greenwashing*, 2025.
Cigref/INR, *L'approche low-tech au service de la résilience numérique des organisations*, février 2026.

Chapitre 2. La soutenabilité faible du numérique

Le diagnostic est posé : le NR ne couvre qu'une partie de ce qu'il devrait réellement couvrir. Il mesure, sensibilise, écoconçoit. C'est utile, mais insuffisant, parce que la « sobriété » telle qu'elle est pratiquée dans la plupart des démarches NR reste de l'optimisation. On fait la même chose avec moins, ou on se limite à un seul fournisseur. On réduit les coûts sans toucher à la structure. On ne questionne ni la finalité des usages, ni la solidité de ce qu'on construit. C'est ce que l'économie écologique appelle la soutenabilité faible : on optimise dans un cadre qu'on ne remet pas en cause, sans forcément se poser la question des risques associés.

Qu'est-ce que cette logique d'optimisation produit dans un monde devenu fluctuant ? Et que consomme-t-elle silencieusement dans les SI ?

L'optimisation fragilise

Prenons le cas le plus courant. Une DSI consolide tout son parc sur un seul éditeur : bureautique, messagerie, stockage, sécurité endpoint. Les coûts baissent, les compétences se concentrent, le support se simplifie. C'est rationnel. C'est optimisé, homogène. Et c'est justement la configuration qui a produit CrowdStrike en juillet 2024 : un agent de sécurité unique, un système d'exploitation unique, 8,5 millions de machines à l'arrêt.

Prenons la gestion d'équipe. On externalise l'exploitation, on réduit l'effectif interne à trois personnes qui pilotent le prestataire. Le coût au poste baisse. Le jour où le prestataire fait défaut ou change ses conditions, personne en interne ne sait reprendre la main. On a optimisé le budget. On a consommé la compétence.

Prenons maintenant une équipe de quatre personnes, toujours sur la gestion des compétences : une gestion optimisée verrait chacune travailler à 100 % sur son sujet d'expertise. Si l'une d'entre elles est absente (démission subite, arrêt maladie, accident...), 25 % du périmètre est perdu. Une gestion sous-optimale, où chacune travaillerait à 80 % sur son sujet et à 20 % sur celui des autres, maintiendrait au moins une partie du périmètre de la personne manquante.

Prenons la migration cloud. Une DSI accompagnée en 2024 a migré son SI on-premise vers un hyperscaler. Entre autres gains opérationnels, elle mettait en avant le bilan carbone. Les indicateurs montraient moins d'émissions par utilisateur, une meilleure efficacité énergétique. La même année, lorsque ce fournisseur est tombé pendant quelques longues minutes, cette organisation a perdu l'accès à la moitié de ses systèmes et la majorité de ses données. Le bilan carbone s'est amélioré (sur le papier), le SI s'est fragilisé, la dépendance a augmenté. Personne ne mesure cette fragilité parce qu'elle n'est pas encore un objectif opérationnel ou un indicateur formalisé pour beaucoup d'organisations.

Du monde stable au monde fluctuant

La recherche d'optimisation est depuis longtemps la principale (voire la seule) logique de développement des SI.

Optimiser, c'est améliorer un système en supprimant les marges, les doublons, les alternatives, pour maximiser l'efficacité. Mais ce qui reste (énergie, compétences, composants) doit être constant, stable et maîtrisé pour maintenir la viabilité du système. C'est une configuration qui fonctionne dans un monde stable : stabilité du marché, stabilité des chaînes d'approvisionnement, stabilité des cadres réglementaires, stabilité des conditions énergétiques. Sous cette hypothèse, maximiser une métrique revient à maximiser la performance globale : c'est sur cette base que le Lean IT ou le FinOps ont été conçus.

Pour autant, aujourd'hui le monde est de plus en plus imprévisible, complexe, incertain (certains diront VUCA : Volatility, Uncertainty, Complexity & Ambiguity). Les crises, diverses, se multiplient et s'amplifient. Prévoir devient compliqué, risqué même, et optimiser autour de conditions qui bougent sans arrêt l'est encore plus.

La panne électrique ibérique d'avril 2025, l'incendie de Daejeon, le bug CrowdStrike, l'embargo sur les cartes graphiques, l'augmentation du prix de la mémoire vive, les cyberattaques contre les hôpitaux : ces événements sont le fonctionnement nominal d'un monde complexe et interconnecté. La suite du chapitre en reprend plusieurs en détail pour étayer la démonstration.

Le contexte opérationnel d'un SI européen aujourd'hui est fluctuant. Les prix de l'énergie varient d'un à trois sur l'année, les contraintes réglementaires changent tous les deux ans, les fournisseurs cloud peuvent imposer des hausses unilatérales, la disponibilité de certains composants peut être interrompue par une décision politique extérieure ou un événement climatique extrême, le climat a un impact direct sur le fonctionnement des datacenters.

Dans un monde fluctuant, ce qui est optimisé pour un état particulier devient fragile dès qu'on en sort. La marge, le mou, la sous-optimalité, qui passaient pour du gaspillage dans le monde stable, deviennent des conditions de viabilité dans le monde fluctuant. Ce déplacement de cadre est une question de nature, pas de degré, et il invalide la plupart des indicateurs hérités de la décennie 2010. Que sont ces marges pour un SI ? C'est l'objet de la section suivante.

Un SI ultra-optimisé est un SI ultra-fragile. **Monde stable = SI optimisé possible. Monde incertain = SI robuste nécessaire.**

Ce que l'optimisation consomme sans le voir

Ce qu'on appelle ici « la marge », c'est ce qu'une organisation garde en réserve pour tenir son activité sous contrainte (son SI en particulier), et qui n'a pas de substitut le jour où elle en a besoin. Un équipement se remplace, un contrat se renégocie. La marge, non : une fois

entamée, on ne la rachète pas. On la consomme en optimisant, et aucun budget ne la reconstitue à temps.

Deux exemples : une base de données restaurée depuis une sauvegarde, c'est un actif redondé : ça se rachète. Une équipe qui sait encore faire tourner le SI à la main quand le fournisseur tombe, c'est de la marge : le jour où ce dis moisavoir-faire a disparu, il ne revient pas simplement. D'où la propriété la plus contre-intuitive de la marge : elle ne se stocke pas, elle s'entretient ou elle se perd.

C'est cette marge-là qui se dégrade en silence quand on optimise sans questionner. L'économie écologique a un nom pour ce genre d'objet : le capital critique, forgé par Paul Ekins pour le capital naturel - menacé de disparition irréversible, sans substitut, aux pertes qu'aucune compensation ne rattrape. Un SI le vit plus simplement, comme de la marge, avec un critère indexé sur le temps : un substitut qui existe en théorie mais qu'aucun choc ne laisse le temps de construire n'existe pas. La soutenabilité faible parie que tout se rachète ; la forte préserve ce qui compte et ce qui ne se rachète pas dans le temps.

Cette marge prend cinq formes dans un SI. Préservées, elles font tenir le service sous contrainte ; consommées, elles ne se reconstituent pas par injection de budget ou de technologie alternative. Les voici dans l'ordre où un choc les sollicite.

- La capacité : le taux d'occupation, la redondance, le temps non alloué. Tout ce qui passe pour du gaspillage dans un monde stable et qui devient la capacité d'absorption dès que le monde fluctue.
- Le fonctionnement dégradé : maintenir une fonction limitée mais réelle quand la fonction nominale tombe. Le terminal du contrôleur de l'introduction, qui valide les billets pendant la panne, en est la forme la plus simple.
- La diversité : des fournisseurs, des technologies, des façons de penser. De la marge tenue en réserve sous forme d'alternatives. Une monoculture est performante tant que le pathogène n'arrive pas.
- Le savoir-faire : faire fonctionner, dépanner et faire évoluer le système sans dépendre exclusivement d'un prestataire. Une marge humaine, entretenue au-delà du besoin quotidien.
- La réversibilité : pouvoir changer de fournisseur, rapatrier les données, revenir en arrière. C'est la marge de décision : elle touche à l'autonomie stratégique autant qu'à la robustesse, et sans elle les quatre autres se défendent dans une cage.

Cinq formes d'une même marge, que l'optimisation consomme précisément parce qu'elle les prend pour du gaspillage. Elles ne sont pas égales devant le temps : la capacité se reconstitue hors urgence, on rachète des serveurs et du temps non alloué à froid ; les quatre autres se reconstruisent en années, quand elles se reconstruisent. Aucune des cinq ne revient dans le temps que laisse un choc. C'est le seul critère qui compte ici.

La diversité fournisseurs perdue par dix ans de consolidation ne se reconstitue pas en un projet. La compétence partie à la retraite ne se remplace pas par une couche de supervision supplémentaire. La réversibilité contractuelle ne se négocie pas quand le coût de sortie devient inacceptable. Le mode dégradé ne se conçoit pas pendant la panne. Et on ne dé-sature pas une équipe le matin du choc.

Daejeon : quand l'optimisation brûle

Le 26 septembre 2025, dans le datacenter du gouvernement coréen à Daejeon, une batterie au lithium explose. L'incendie dure dix heures. 647 systèmes s'arrêtent. 858 téraoctets de données sont perdus définitivement. Huit ans de travail de 125 000 fonctionnaires. Trois semaines après l'incendie, à peine plus d'un tiers des services étaient restaurés et une partie ne reviendra jamais. Ces téraoctets sont un actif détruit, pas une marge consommée. La marge s'érode en silence et se reconstruit lentement ; l'actif détruit ne revient pas, à aucun prix. La marge, ici, aurait été une sauvegarde à l'échelle du volume, testée, et une équipe qui sait restaurer. C'est cette marge manquante qui a transformé un incendie en perte définitive.

Le datacenter était souverain. Opéré par l'État, soumis au droit coréen, abritant exclusivement des données coréennes. Cette souveraineté n'a strictement rien empêché. Il était même autonome : aucun fournisseur étranger dans la boucle, personne dont dépendre pour le faire tourner. Ça non plus n'a rien empêché. Ce qui manquait était ailleurs. La résilience : revenir après le choc - trois semaines pour restaurer un tiers, une partie qui ne reviendra jamais. Et surtout la robustesse : tenir sa fonction pendant le choc, ne pas s'effondrer d'un bloc. Daejeon n'avait aucune des deux, mais c'est la robustesse qui manquait en amont : sans elle, la résilience n'a plus rien à récupérer.

Ce qui transforme l'incident en démonstration, c'est qu'il est le produit direct de l'optimisation. Le service centralisé (un G-Drive coréen mis en place pour des raisons de sécurité) concentrait les données au seul endroit. Trop gros pour être sauvegardé, mais pas trop gros pour être utilisé. Le datacenter avait été conçu pour quelques centaines de services : il en hébergeait plus de sept cents, ajoutés au fil des années sans réévaluation. Chaque ajout marginal avait du sens mais l'empilement était devenu intenable et aucune décision de refonte n'avait été prise... Parce que tout fonctionnait.

La dérive organisationnelle était à l'œuvre : des incidents plus petits avaient eu lieu sans conduire à requalifier la politique de sauvegarde. Les interdépendances cachées (refroidissement, réseau électrique, règles de sécurité physique) ont multiplié l'impact. Dans les jours suivant l'incendie, des tentatives d'intrusion ont visé les systèmes en cours de restauration : la crise physique s'est prolongée en crise informationnelle.

Le responsable de la cellule de restauration s'est donné la mort dans les semaines qui ont suivi, rapporte la presse coréenne. Cette mort dit ce que coûte l'écart entre la responsabilité confiée et les moyens réels d'agir. La défaillance était systémique, accumulée à tous les niveaux de la chaîne.

L'optimisation qui fragilise : des exemples réels

Daejeon est la version visible d'un mécanisme qu'on retrouve sous d'autres formes dans cinq cas devenus des références :

CrowdStrike, juillet 2024 : la monoculture comme défaut de conception

Un agent de sécurité unique, déployé sur un système d'exploitation unique, propagé par un canal de mise à jour unique : 8,5 millions de machines Windows à l'arrêt simultané. Le détail technique de l'incident, et sa facture, sont traités au chapitre suivant. Ce qui compte ici est l'absence d'alternative. La diversité technologique avait été éliminée par des décennies de consolidation.

Russie 2022-2024 : la décision politique comme rupture, l'extraterritorialité comme arme

AWS, Azure, Google Cloud, SAP et Oracle ont coupé unilatéralement leurs services aux clients russes, sur la base des sanctions américaines (Executive Orders 14024 d'avril 2021 et 14071 d'avril 2022) et européennes (paquets 5 et 6 de 2022). La continuité d'un service cloud ne dépend pas seulement de sa disponibilité technique mais de la volonté du fournisseur de continuer à le rendre.

Spruce Pine, septembre 2024 : la dépendance au-delà du premier ordre

L'ouragan Helene a inondé la mine qui fournit la quasi-totalité du quartz ultra-pur nécessaire à la fabrication des semi-conducteurs. Pendant plusieurs semaines, toute la chaîne d'approvisionnement mondiale dépendait d'un site dont la quasi-totalité des DSI ignoraient l'existence.

Cloudflare, novembre 2025 : la panne invisible de l'infrastructure invisible

Un changement de configuration chez Cloudflare a entraîné une panne en cascade affectant un large pan du web : DNS, anti-DDoS, CDN, WAF, routage applicatif. Une infrastructure utilisée mais absente des cartographies SI de la majorité des organisations est tombée, et un nombre considérable de services sont tombés avec elle. La dépendance la plus dangereuse est souvent celle qu'on n'a pas identifiée.

COVID-19, 2020-2021 : le choc systémique qui découvre les compétences absentes

La pandémie a produit simultanément une pénurie mondiale de semi-conducteurs, une rupture d'approvisionnement sur les équipements IT, un passage brutal au télétravail, un ERP non accessible à distance pour bien des organisations, un support souvent débordé. Le choc n'a pas détruit de SI : il a révélé les compétences qui manquaient, les procédures qu'on n'avait jamais testées, les modes dégradés qu'on n'avait jamais conçus. La crise

sanitaire a agi comme un test de robustesse à l'échelle mondiale, et beaucoup ont échoué à ce test grandeur nature. D'autres l'ont passé de justesse.

Microsoft Office 2025-2026 : la boucle de verrouillage économique

Un septième mécanisme, plus discret, prolonge la série des six : la boucle de verrouillage économique, qui se nourrit d'elle-même. En janvier 2025, Microsoft a augmenté ses tarifs publics Office de 30 % (communiqué Microsoft ; couverture *The Register*, *Zone Numérique*). En 2026, nouvelle hausse. La justification avancée par l'éditeur : les investissements dans l'IA. La suite de la boucle est notre lecture : des composants renchérissés par la demande en IA, refacturés à des clients qui n'ont rien demandé. La boucle se referme. Beaucoup de clients n'utilisent pas les fonctionnalités d'IA intégrées aux suites bureautiques ; tout le monde paie la facture. La dépendance se mesure en coût potentiel de migration, mais aussi en incapacité à refuser une évolution de modèle économique décidée unilatéralement.

Ces sept cas relèvent de mécanismes différents mais valident la même thèse : la marge du SI ne se rachète pas dans l'urgence. L'ampleur des conséquences est rarement proportionnelle à la cause. Elle est proportionnelle au degré de dépendance et à l'absence d'alternatives opérationnelles.

Ces cas sont choisis parce qu'ils montrent le mécanisme, et personne ne tient le registre inverse : celui des organisations qui ont massivement optimisé sans jamais subir de choc. Il en existe, sans doute beaucoup. L'argument de ce livre ne repose donc pas sur une fréquence, qu'on ne connaît pas, mais sur une asymétrie : quand le choc arrive, l'organisation optimisée sans marge n'a plus de coup à jouer. On peut gagner ce pari des années durant. On ne peut pas se rattraper le jour où on le perd.

Egalement, il est important de noter qu'il ne faut pas viser à éviter les chocs, cela mènerait à une surpréparation (insoutenable budgétairement ou dans les ressources qu'elle consomme) ou à une complexité qui mettrait l'organisation plus à risque qu'elle ne l'est initialement. Parfois accepter le choc, et repartir est suffisant. Parfois, l'impact du choc n'est pas acceptable, et c'est là qu'il faut travailler.

Encadré : Les sept couches de dépendance

Ophélie Coelho cartographie les points de passage obligés du numérique ; on en tire sept couches de dépendance : ressource (énergie, matériaux, composants), infrastructure, plateforme, applications, compétences, données, intelligence (algorithmes et modèles). Chaque couche est un point de verrouillage potentiel. Daejeon a démontré l'effondrement simultané de quatre d'entre elles. CrowdStrike a frappé sur la couche application. Le verrouillage VMware opère sur la couche plateforme. Le verrouillage Nvidia opère simultanément sur la couche matériel (GPU H100, Blackwell) et la couche intelligence (écosystème CUDA, cuDNN, TensorRT) : sortir de Nvidia suppose aussi bien un portage technique que la reconstitution d'un stack algorithmique équivalent. C'est cette

interpénétration qui rend le verrouillage particulièrement difficile à lever. La grille rend visible que la dépendance n'est jamais unidimensionnelle, et qu'une stratégie de robustesse doit traiter chaque couche distinctement, mais également l'ensemble des couches dans leur globalité.

Les seuils invisibles : dette technique, verrouillage, compétences

La dégradation de la marge suit une dynamique lente. Le SI connaît ses propres points de bascule :

- La dette technique est gérable tant qu'on en paie les "intérêts" (mise à jour, maintien et transfert de compétences, cyber, etc.) ; au-delà d'un seuil, le legacy devient une boîte qu'on ne peut plus maintenir sereinement. La dette et la marge se ressemblent sans se confondre : la dette est un passif connu, inscrite dans les backlogs, dont on paie les intérêts en maintenance ou en dépendance ; la marge consommée est un actif disparu (ici la connaissance de son SI et la capacité à le maintenir), et personne ne voit qu'elle manque avant d'en avoir besoin (modification, mise à jour, réparation etc.). La chaîne entre les deux est directe : la course à la performance fabrique la dette, et la dette mange la marge : celle du savoir-faire quand plus personne ne comprend le système, celle de la réversibilité quand on n'ose plus le faire évoluer.
- Le verrouillage fournisseur (juridique, contractuel) progresse par crans marginaux (un service, des intégrations, des workflows calés dessus) jusqu'au jour où le coût de sortie dépasse la capacité de le faire effectivement ; c'est alors que le pouvoir de négociation bascule du client au fournisseur.
- La perte de compétences internes est la plus discrète : une équipe se réduit à deux personnes, à une, puis à zéro. C'est l'illectronisme opérationnel nommé au chapitre 1.

Ces trois seuils sont invisibles et indolores tant qu'ils ne sont pas franchis, et un point de bascule franchi sur une dimension précipite les autres.

Ces seuils observés au niveau d'une organisation prennent une toute autre dimension quand on les replace dans la concentration globale du marché. TSMC réalise environ 70 % du marché mondial de la fonderie de semi-conducteurs (TrendForce, 2025). Nvidia détient plus de 90 % des GPU dédiés. 265 milliards d'euros par an de dépenses logicielles et cloud européennes sont captées par des acteurs américains (Asterès/Cigref/Numeum). S'ajoute une nasse juridique extraterritoriale : CLOUD Act, FISA 702, IEEPA/OFAC, Export Administration Regulations, qui transforme la dépendance en levier : elle donne aux États-Unis (ou à d'autres) les moyens légaux de l'activer contre l'utilisateur : couper l'accès, exiger les données, bloquer les exportations, etc. Le cas Nvidia/Chine l'illustre : depuis octobre 2022, les États-Unis ont interdit l'export vers la Chine des puces IA haut de gamme de Nvidia (A100, puis H100/H200). Objectif : freiner l'accès chinois au traitement IA de pointe.

On parle ici d'IA, mais le sujet de la dépendance s'illustre aussi avec le cloud : auditionné au Sénat le 10 juin 2025, le directeur des affaires publiques et juridiques de Microsoft France, Anton Carniaux, a déclaré sous serment ne pas pouvoir garantir que les données des citoyens français ne soient jamais transmises aux autorités américaines sans l'accord des autorités françaises.

Le PRA traite l'incident, pas la soutenabilité

L'objection classique (« on a un PRA, on est couvert ») ne tient pas face au constat qui précède. Le PRA suppose un état normal auquel on revient après l'incident ; la lecture par la marge (ce que le SI garde en réserve pour tenir, et qui ne se rachète pas dans le temps que laisse un choc lorsqu'il advient) questionne cet état lui-même. Par ailleurs, le PRA n'est pas toujours régulièrement testé, ce qui peut réserver des surprises (technique ou organisationnelle) lorsqu'il est activé. Un PRA jamais testé est l'exemple type de la marge nominale : elle existe dans la théorie, pas dans les gestes des équipes. Le jour où le PRA doit s'activer, il risque fort de ne pas fonctionner.

Et le PRA classique ne modélise pas les trois couches de risque qui structurent le monde fluctuant.

- Il ne traite pas l'indisponibilité des intrants : on ne commande pas un serveur de secours quand le quartz ultra-pur n'existe plus, ni un jeu de GPU quand leur export est réglementairement interdit.
- Il ne traite pas la corrélation des risques : le détroit d'Ormuz fermé, El Niño sur les centrales hydroélectriques et de nouvelles restrictions chinoises la même année, c'est un scénario plausible, plus un cas exotique.
- Il ne traite pas (ou rarement) la durée : un RTO de quatre heures n'a plus de sens quand le substrat matériel est indisponible pour des trimestres entiers. La question utile n'est donc plus « sommes-nous capables de revenir en quatre heures ? », mais « comment notre entrepôt fonctionne sans WMS pendant trois mois ? ».

Derrière ces trois limites, une raison de fond : les chocs qui comptent échappent aux calculs qui fondent la gestion des risques. Leur probabilité est mal estimée par construction : trop peu d'observations, et un contexte qui reste rarement cohérence avec l'actualité. Surtout, les pannes ne sont pas indépendantes, les dépendances partagées les corrélient : CrowdStrike n'est pas 8,5 millions d'incidents, c'est un événement unique à 8,5 millions de manifestations. D'où le déplacement que propose ce manifeste : piloter le SI par la conséquence et le maintien de fonction, qu'on maîtrise - plutôt que par la probabilité qui semble difficile à estimer au mieux ou tendre vers 1 à long terme dans un monde plus instable.

Ce qui craque déjà

Les fragilités décrites plus haut ne sont pas que des hypothèses, elles se matérialisent chaque jour. Beaucoup de « fissures » sont rendues visibles par l'IA, qui accélère les usages numériques, le besoin d'infrastructure, l'impact environnemental et social, et qui devient stratégique pour les organisations comme pour les pays.

Sur l'infrastructure : 40 % des datacenters IA seront affectés par des contraintes électriques d'ici 2027 (Gartner, 2024). 26,7 % des datacenters mondiaux seraient exposés à un risque climatique élevé ou modéré d'ici 2050 (XDI, juillet 2025). OpenAI perdrait plus de 11 milliards de dollars par an à horizon 2026 selon des projections internes divulguées (*The Information*, août 2024) ; or les organisations qui ont intégré ces outils le font sur l'hypothèse implicite que leur coût restera stable.

Sur les modèles économiques : dès 2026, les prix des licences IA augmentent par deux voies complémentaires. Frontalement, avec des hausses explicites sur les abonnements professionnels, sur le modèle des hausses Office documentées plus haut.

Silencieusement, par un rétrécissement des seuils d'usage par session : le nombre de tokens, de requêtes ou de messages inclus dans un abonnement donné diminue, alors même que les usages, de leur côté, demandent mécaniquement plus de tokens. L'abonnement à 20 euros reste affiché comme tel, mais son contenu effectif se réduit. L'évolution économique globale est celle d'une hausse masquée.

Sur les compétences : Salesforce, PwC UK et d'autres grandes organisations ont freiné ou arrêté leurs embauches juniors en 2025, estimant l'automatisation IA suffisante pour couvrir ce niveau de tâches (le chapitre 5 revient en détail sur ce qui se joue alors dans la transmission des compétences).

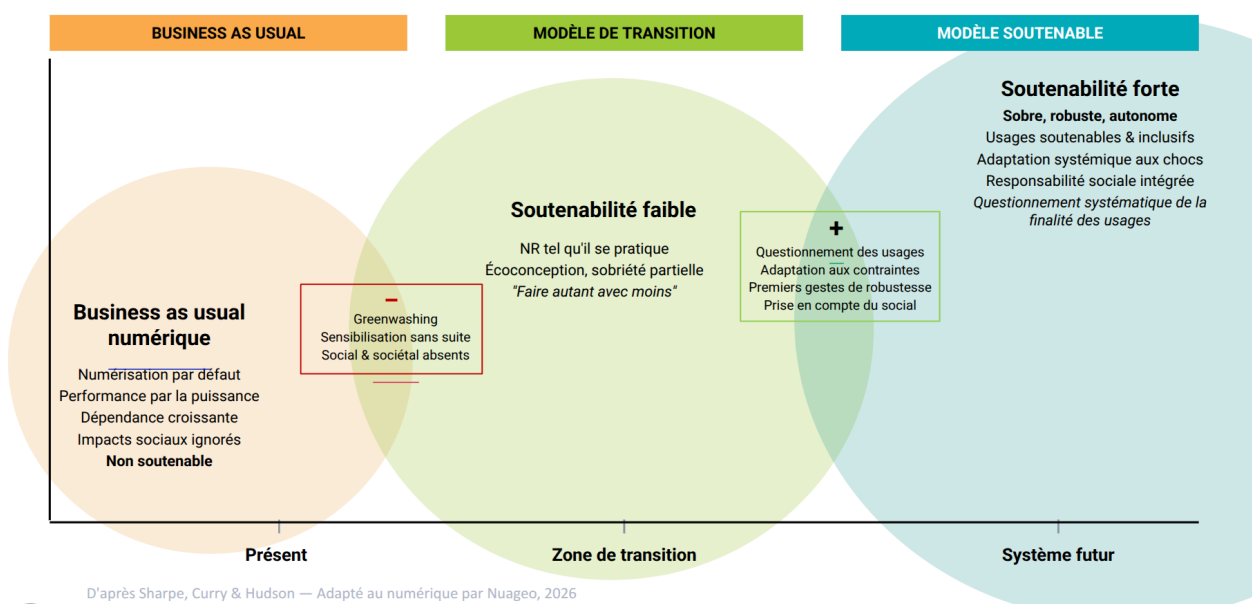
Sur la diversité cognitive : Doshi et Hauser (**Science Advances**, 2024) ont mesuré le mécanisme : les récits écrits avec des idées d'IA sont jugés plus créatifs, surtout chez les auteurs les moins créatifs, mais ils se ressemblent davantage entre eux. L'atrophie cognitive documentée par Microsoft Research (2025) le confirme : plus la confiance dans l'IA est élevée, plus la pensée critique baisse. Le gain est individuel et la perte est collective. Des actions existent. Elles relèvent de la gouvernance et des compétences bien plus que de la technique, nous y reviendrons.

Encadré : Le coût réel d'un prompt

Un prompt consomme entre 0,3 et 3 wattheures selon le modèle et la longueur de la requête, et jusqu'à 10 wattheures pour les modèles les plus volumineux ou les raisonnements longs (Epoch AI, **Estimating the Energy Consumption of a ChatGPT Query**, 2025 ; ordres de grandeur, l'incertitude reste forte). Même en prenant la borne basse, 1000 utilisateurs, 50 prompts par jour ouvré, 250 jours ouvrables représentent environ quatre mégawattheures par an, soit l'équivalent de la consommation d'une famille française. Pris à la borne haute de dix wattheures, ce sont cent vingt-cinq mégawattheures : une trentaine de foyers. L'efficacité de chaque prompt peut s'améliorer indéfiniment sans compenser la croissance du nombre de prompts. C'est une illustration de l'effet rebond : plus l'usage devient simple, plus il se multiplie.

Même les projections institutionnelles restent dans cette logique. Les scénarios ADEME sur les datacenters français (*Prospective d'évolution des consommations des data centers de 2024 à 2060*, 2026) le montrent : 58 % de l'empreinte énergétique de nos usages numériques repose déjà sur des datacenters hors de France. Le scénario Technologies Vertes voit cette part passer de 14 à 30 TWh en 2050. Le Pari Réparateur explose à 231 TWh. On délocalise l'empreinte en espérant l'optimiser. Seul le scénario Génération Frugale descend à 0,57 TWh externalisé, parce qu'il assume une dénumérisation des usages les plus gourmands. C'est d'ailleurs un scénario qui pourrait réconcilier transition écologique (ici baisse de la consommation électrique) et autonomie stratégique (production électrique nationale suffisante pour supporter nos usages). Le constat s'arrête là, maintenant commence la trajectoire : comment tendre vers un numérique soutenable ?

Trois horizons, une seule trajectoire



Le modèle des trois horizons, conçu pour la prospective stratégique par Bill Sharpe et ses collègues à partir des années 2000, situe ce que le NR fait, ce qu'il ne fait pas.

L'idée centrale est que dans une période de transition profonde, plusieurs systèmes coexistent. Le système dominant (« Business as usual », notre premier horizon) est en perte de légitimité mais reste dominant en pratique. C'est le numérique par défaut, sans questionnement et sans limite : une loi de Moore - observation que le nombre de transistors sur une puce double environ tous les deux ans, ce qui entraîne une augmentation exponentielle de la puissance de calcul - étendue au-delà des processeurs, qui couvrirait les usages, l'infrastructure et la capitalisation du numérique.

Le système qui prendra le relais existe déjà, sous forme d'expériences et de prototypes : le numérique robuste, qui vise la soutenabilité forte (notre horizon 3). C'est lui qu'on s'efforcera de décrire.

Entre les deux, le système de transition : le numérique « responsable » appliqué partiellement, souvent réduit à de l'optimisation, comme on l'a vu dans ces deux premiers

chapitres. Il relève de la soutenabilité faible (H2) et regroupe des pratiques qui peuvent tirer dans les deux directions.

Une partie des pratiques H2 stabilise le système dominant H1 en le rendant un peu plus acceptable : le NR « premier tiers », qui optimise sans questionner. Une autre partie des pratiques H2 prépare le système à venir H3 en construisant les capacités qu'il exigera : compétences internes, gouvernance, briques techniques, méthodes, etc. Le programme GreenOps du chapitre 1 est typiquement une pratique H2 : selon qu'il plafonne ou non la consommation globale, il stabilise H1 ou prépare H3.

Finalement, dans cet état intermédiaire, la question à se poser : est-ce que ce qu'on construit aujourd'hui tire vers un numérique robuste qui vise la soutenabilité forte, ou consolide un numérique « Business as usual » ?

Le Cigref, dans son rapport sur l'approche low-tech (février 2026, conduit avec l'INR), propose une déclinaison voisine. H1 non soutenable, H2 efficience et optimisation, H3 circularité et cycles du vivant. Ce manifeste s'inscrit dans la même filiation, en y ajoutant une lecture d'ensemble : le SI comme une économie de la marge, où la robustesse au sens d'Olivier Hamant rejoint la soutenabilité forte au sens de Herman Daly.

Encadré : Soutenabilité faible et soutenabilité forte : le cadre théorique

Les termes viennent de l'économie écologique. Solow et Hartwick ont posé dans les années soixante-dix le cadre de la version faible : un développement est soutenable tant que le stock total de capital (naturel + manufacturé) ne diminue pas. Herman Daly et Robert Costanza ont contesté cette équivalence : certains capitaux n'ont pas de substitut, ceux qu'Ekens nomme critiques. Les économistes raisonnent en stocks de capital ; un SI vit la même question sous forme de marge. La transposition est de nous, pas d'eux.

Daly en a tiré trois règles : ne pas prélever les renouvelables plus vite qu'ils ne se régénèrent, ne pas épuiser les non-renouvelables sans avoir construit leur relève, ne pas émettre de polluants au-delà de la capacité d'assimilation des milieux.

Transposées au SI : ne pas consommer les compétences internes plus vite qu'on ne les renouvelle, ne pas retirer un composant sans substitut opérationnel, ne pas accumuler de dette technique au-delà de la capacité de l'équipe à la résorber.

La soutenabilité faible (le paradigme d'optimisation dans lequel le NR opère) consomme silencieusement la marge du SI.

L'alternative : concevoir le SI pour tenir, plus seulement pour performer. Ce cadre a un nom, la robustesse ; il fait passer de la soutenabilité faible à la soutenabilité forte. Reste une question, à poser dès maintenant sur son propre SI : des cinq formes de marge

décrites dans ce chapitre, combien s'érodent en ce moment sans qu'aucun indicateur ne le signale ?

Références

- Daly, *Steady-State Economics*, W. H. Freeman, 1977 ; *Beyond Growth*, Beacon Press, 1996.
- Costanza et al., *Nature*, 1997 ; mise à jour *Global Environmental Change*, 2014.
- Ekins, *Economic Growth and Environmental Sustainability*, Routledge, 2000.
- Sharpe, *Three Horizons: The Patterning of Hope*, Triarchy Press, 2013.
- Doshi & Hauser, « Generative AI enhances individual creativity but reduces the collective diversity of novel content », *Science Advances*, 2024.
- Acemoglu, « The Simple Macroeconomics of AI », MIT Working Paper, 2024.
- ADEME, *Prospective d'évolution des consommations des data centers de 2024 à 2060*, 2026.
- ADEME/Greenworking, *Caractérisation des effets rebond induits par le télétravail*, 2020.
- Shift Project, *Planifier la décarbonation du numérique*, octobre 2025.
- Cigref/INR, *L'approche low-tech au service de la résilience numérique des organisations*, février 2026.
- Perrow, *Normal Accidents*, Princeton University Press, 1984.
- Leveson, *Engineering a Safer World*, MIT Press, 2011.
- Parametrix, *Cloud Outage Risk Report 2024*, mars 2025.
- Coelho, *Géopolitique du numérique*, L'Atelier, 2023.
- Communiqués officiels du Ministère de l'Intérieur et de la Sécurité (Corée du Sud), septembre-octobre 2025 ; analyse consolidée Peccini, *Annexe Daejeon*, octobre 2025.

Note bibliographique. Le modèle IRON proposé par Stephan Peccini (mars 2026) constitue une référence convergente sur le diagnostic de la dépendance numérique. Il diverge sur trois points qui justifient de ne pas en reprendre l'architecture ici : il ne pose pas de filtre du bien commun en amont des arbitrages de robustesse, il n'inclut ni la sobriété ni la low-technisation parmi ses axes opérationnels, et il ne traite pas l'autonomie stratégique comme une dimension systémique articulée à l'architecture.

DEUXIÈME PARTIE. La thèse

Quelque part en 2030. L'été venu, le CHU bascule ses serveurs sur la zone de repli, que l'équipe interne opère elle-même. Dans les services, les protocoles restent accessibles hors écran, et chacun sait quoi faire parce qu'on s'y est exercé. Rien ne s'arrête.

(Récit d'atelier robustesse, développé au chapitre 7.)

Le vivant traverse les chocs depuis 3,8 milliards d'années. Glaciations, météorites, effondrements d'écosystèmes entiers : il est toujours là, sans plan de reprise d'activité, sans fournisseur de secours. Un biologiste, Olivier Hamant, a nommé ce qui le fait tenir : la robustesse. Nos SI, eux, font le pari inverse : le diagnostic qui précède a montré un numérique responsable qui optimise dans un cadre qu'il ne questionne pas, et qui consomme ce faisant des marges qui ne se rachètent pas dans l'urgence. Le monde qui vient est incertain, traversé de crises multiples et imprévisibles : une logique d'optimisation n'est pas taillée pour y faire face. Cette deuxième partie pose la thèse du manifeste en deux chapitres. La robustesse d'abord : maintenir la fonction pendant et en amont du choc, au prix d'une sous-optimalité assumée. C'est elle, le chemin vers la soutenabilité forte. Le filtre ensuite : comme on ne peut pas tout rendre robuste sans reproduire l'excès qu'on dénonce, la santé commune, que le chapitre 4 définit, décide de ce qui mérite l'effort. Un chemin et un filtre. De quoi transformer un constat en démarche.

Chapitre 3. La robustesse comme condition de soutenabilité forte

Le 19 juillet 2024, à 4h09 UTC, une mise à jour de 40 kilooctets a paralysé 8,5 millions de machines Windows dans le monde. L'agent CrowdStrike Falcon, installé au niveau du noyau système, a tenté de lire un fichier de configuration à 21 champs avec un code qui n'en traitait que 20. Accès mémoire hors limites, crash kernel, écran bleu. Hôpitaux, aéroports, banques, administrations : tout ce qui dépendait d'un poste Windows équipé de cet agent s'est arrêté. 5 078 vols annulés. Des salles d'opération reportées. Des chaînes logistiques figées. La facture atteint 5,4 milliards de dollars pour les seules entreprises du Fortune 500 (Parametrix, *CrowdStrike Outage Impact Report*, 2024).

L'incident n'avait rien d'un cygne noir (*concept popularisé par Nassim Nicholas Taleb (Le Cygne noir, 2007) - un événement rare, à très fort impact, imprévisible avant qu'il ne survienne, et rationalisé après coup.*). C'était un composant de sécurité unique, déployé sur un système d'exploitation unique, avec un accès noyau, sans isolation possible. L'architecture était optimisée, cohérente, homogène : un seul outil pour tout le parc, un seul fournisseur, un seul canal de mise à jour. L'optimisation elle-même, par l'homogénéisation, était la faille.

CrowdStrike, Daejeon : deux variations du même mécanisme, posé au chapitre 2.

La soutenabilité faible optimise. La soutenabilité forte exige autre chose : un SI qui maintient ses fonctions essentielles à travers les chocs, donc une marge qui reste présente le jour où le choc arrive. C'est la robustesse qui la garde : elle maintient la fonction, et la marge est ce qu'elle entretient pour y parvenir, son moyen et son prix. Ce chapitre pose le cadre de cette robustesse. Il faut sortir du registre informatique pour comprendre pourquoi : c'est justement ce que fait Olivier Hamant depuis la biologie.

L'inefficience comme condition de survie

Olivier Hamant, biologiste à l'INRAE et directeur de l'Institut Michel Serres, a construit un corpus théorique qui éclaire directement ce paradoxe. Sa thèse tient en une formule : la robustesse du vivant résulte de procédés intrinsèquement inefficaces.

L'un des nombreux exemples qu'il met en avant est la photosynthèse. Son rendement est inférieur à 1 %, là où un panneau solaire atteint 15 %. Le végétal « gaspille » 99 % de l'énergie lumineuse qu'il reçoit. Mais ce gaspillage est le prix de l'adaptabilité : le vivant prospère depuis 3,8 milliards d'années, sous des conditions climatiques qui ont varié de façon considérable. Le panneau photovoltaïque est performant mais fragile. La feuille est sous-optimale mais robuste.

Hamant identifie neuf « déclinaisons de la sous-optimalité » qui fondent la robustesse biologique : hasard, redondance, gaspillage, hétérogénéité, fluctuations, lenteur et hésitation, incohérences, erreurs et imprécisions, inachèvement. Toutes ne sont pas des marges : le hasard, la lenteur, l'inachèvement relèvent d'autre chose qu'une réserve. La robustesse déborde la marge du chapitre 2, et c'est heureux : la marge est ce qu'elle entretient, pas tout ce qu'elle est, ni tout ce qu'elle vise.

Chacune constitue un coût en efficacité qui achète de la robustesse systémique. L'organisme qui tolère de l'imperfection dans ses processus cellulaires, qui maintient des gènes redondants, qui accepte des boucles incohérentes dans ses réseaux moléculaires, survit mieux que celui qui a tout optimisé.

Sa critique de la performance est sans appel : « La performance, c'est le zéro stock, le just in time, le flux tendu. Être performant ne consiste plus à bien faire, mais à fonctionner comme une machine efficace et efficiente. Cette définition est très mortifère. » L'article publié dans *Nature Plants* en 2020 formalise le lien avec le paradoxe de Jevons : les gains d'efficacité conduisent à des effets rebond qui annulent les bénéfices attendus. Le vivant contourne ce piège par la sous-optimalité. Nos SI y plongent tête baissée. Dans *L'Entreprise robuste*, publié en 2025 avec Charbonnier et Enlart, Hamant transpose ces principes au monde organisationnel : la robustesse d'une entreprise ne se mesure pas à sa capacité à optimiser en conditions stables, mais à sa capacité à fonctionner quand les conditions changent.

Robustesse, résilience, antifragilité : une distinction qui change tout

Les trois termes circulent dans le vocabulaire des DSI. On les utilise souvent comme des synonymes. Ce sont des concepts différents, et la confusion a des conséquences pratiques.

La résilience suppose le choc puis le retour à la situation nominale (avant crise, avant choc). Un système résilient encaisse, puis revient à son état antérieur. Le PRA classique est un dispositif de résilience : on planifie le retour à la normale après l'incident. Mais la résilience ne questionne ni les causes du choc, ni la fragilité du système qui l'a subi. Elle est, dans les termes de Hamant, « désastro-dépendante » : il faut d'abord tomber pour se relever. Elle suppose aussi que le choc, ou la crise est temporaire et que le retour à la situation nominale est possible dans un horizon de temps acceptable.

L'antifragilité, concept de Nassim Nicholas Taleb, va plus loin : le système ne se contente pas de résister au choc, il en sort renforcé. Comme les muscles qui se développent sous le stress mécanique, certaines organisations apprennent de leurs crises. Mais l'antifragilité est, elle aussi, désastro-dépendante. Pire : transposée au monde socio-économique, elle devient, selon Hamant, « une incitation à tomber pour sélectionner ceux qui vont se relever, voire sélectionner ceux qui seront encore plus forts après l'échec. C'est absolument toxique. » Le darwinisme organisationnel qui en découle laisse sur le carreau ceux qui n'avaient pas les ressources pour rebondir. Est-ce réellement souhaitable à long terme ?

La robustesse, telle que Hamant la définit, est d'une autre nature. C'est un espace de viabilité dans lequel le système maintient sa fonction malgré les fluctuations, sans exiger de choc préalable. Ni trajectoire de retour après chute, ni sélection darwinienne des survivants. Elle agit en amont et pendant la perturbation, par des mécanismes intrinsèques : la redondance, la diversité, les fluctuations intégrées au fonctionnement

normal. Elle est « joyeuse » parce qu'elle n'attend pas la catastrophe pour se mettre en route.

L'image la plus directe est celle du ski. La résilience et l'antifragilité reviennent à slalomer entre les bosses : ça tient jusqu'à ce qu'on tombe, sur une bosse ou de fatigue. On peut se relever, mais ce n'est pas viable à long terme.

La robustesse vise autre chose : transformer le skieur pour qu'il fonctionne avec les bosses. Améliorer sa technique, muscler ses mollets, assouplir ses genoux. Que la descente bosselée devienne son mode nominal. Et si une bosse est plus haute que les autres ? Il y en aura toujours. Il la prend, il saute, il fait une figure au lieu de tomber. Dans un monde de polycrise permanente, où les chocs se multiplient, se superposent, se nourrissent, la volonté de maîtrise absolue, le slalom, est intenable. La robustesse, cet espace permanent de viabilité où l'on fait avec les bosses, est la seule posture qui tient sur la durée.

Encadré : Trois concepts, trois logiques

Résilience : agit après le choc. Logique de retour au statu quo. Limite : exige de tomber d'abord, ne questionne pas les causes, ni la possibilité qu'un retour à la situation nominale soit possible.

Antifragilité (Taleb) : agit grâce au choc. Logique de renforcement par le désordre. Limite : désastro-dépendante, sélection darwinienne.

Robustesse (Hamant) : agit pendant et en amont. Logique d'espace de viabilité multidirectionnel. Limite : coûte en efficience, exige de renoncer au paradigme de performance.

Sobriété et robustesse : le malentendu à lever

La critique de la sobriété réduite à « faire autant avec moins » ne vise pas la sobriété réelle. Quand on la définit comme l'évitement dès le départ de la demande en énergie, matériaux, terres et eau dans le cadre des limites planétaires (Shift Project, 2024), elle ne se confond plus avec l'optimisation. Et il faut choisir : on ne pourra pas être sobre et faire systématiquement « autant ».

Cette sobriété peut pourtant sembler contradictoire avec la démarche de robustesse, qui est par nature plus consommatrice de ressources (moins optimisée, en somme).

Le malentendu vient de ce qu'on confond robustesse et sur-dimensionnement. Un SI ultra-optimisé, réduit au strict minimum par une optimisation extrême (parfois justifiée par une sobriété de façade), devient fragile face aux imprévus. Une entreprise qui réduit au maximum ses infrastructures cloud pour diminuer sa consommation, puis dont le fournisseur unique tombe en panne, se retrouve à l'arrêt complet. À l'inverse, un SI qui multiplie les systèmes de secours, duplique systématiquement les données en temps réel dans plusieurs datacenters, et empile les couches de sécurité, consomme des ressources

considérables pour une robustesse... de façade. Parce que la complexité qu'il a créée est elle-même source de fragilité.

La sobriété sans robustesse produit de la vulnérabilité.

La robustesse sans sobriété produit de la complexité insoutenable.

Les deux sont des impasses quand elles opèrent seules.

En pratique, la sobriété et la robustesse se renforcent. Tout ce qui est moins consommé est moins dépendant. Tout ce qui n'existe pas n'a pas besoin d'être protégé. **La sobriété réduit la surface de dépendance, et donc le périmètre sur lequel il faut investir en robustesse. La robustesse, elle, donne un critère de tri à la sobriété** : on ne réduit pas n'importe quoi, on préserve ce qui est critique et on allège ce qui ne l'est pas. La séquence est un réglage simultané, guidé par le filtre du bien commun, pas un « sobriété d'abord, robustesse ensuite ».

Nous l'avons vécu à notre échelle. Quand nous avons conçu le site nuageo.fr, nous avons choisi Digital Forest, un hébergeur engagé dans un web alternatif. Un choix aligné avec nos valeurs : écoconception, hébergement cohérent avec nos engagements. En mars 2025, un acte de malveillance a rendu le site indisponible pendant cinq jours. La question s'est posée immédiatement : se tourner vers un géant américain pour un SLA béton, ou assumer ce choix avec ses aléas. Nous avons choisi la confiance. Cinq jours d'indisponibilité pour notre site web, au regard de l'enjeu, c'est raisonnable.

Le même arbitrage bascule dès que le service porte du chiffre d'affaires ou du soin : ce qui est tenable pour un site vitrine ne l'est pas pour une chaîne d'encaissement ou un dossier patient. Mais la situation a rendu visible une tension que beaucoup d'organisations connaissent : le choix éthique n'est pas forcément le choix « techniquement robuste » ; et pour autant la robustesse n'est pas automatiquement dans le choix du plus gros fournisseur.

Dans le cas du site nuageo.fr, l'enjeu n'était pas seulement une préférence écologique. En choisissant un hébergeur indépendant, nous contribuons à maintenir l'écosystème d'alternatives qui rend la diversité possible. Se replier sur un géant américain à chaque incident, c'est consommer à petit feu la marge de diversité du marché : l'existence même de ces acteurs. Ici, accepter cinq jours d'indisponibilité pour un site vitrine, c'est aussi une contribution à un écosystème éthique, alternatif, diversifié... donc plus robuste.

Reste la vraie question : ce qu'on protège, à quel niveau, et ce qu'on accepte de perdre temporairement. Elle occupe tout le chapitre 4, laissons-la encore un peu en suspens.

Avant de choisir quoi protéger, encore faut-il savoir à quoi ressemble un système qui protège.

Du vivant au SI : sept piliers de robustesse

C'est le détour de cette section : transposées aux systèmes d'information, les déclinaisons de sous-optimalité de Hamant se regroupent en sept piliers.

Ces sept piliers forment un système interdépendant, pas une checklist : chaque pilier en contraint un autre. La redondance sans hétérogénéité produit de la duplication stérile. La modularité sans interactions produit de l'isolement. La circularité sans vision systémique se résume à prolonger la vie du matériel sans rien changer d'autre. Tenir 6 piliers sur 7 ne produit pas 6/7ième de robustesse : il suffit d'en manquer un pour que les autres se contredisent. C'est leur articulation qui fait le système, pas leur somme.

L'hétérogénéité d'abord. Diversifier pour ne pas concentrer toutes ses dépendances sur un seul acteur, un seul fournisseur ou une seule technologie. Un SI 100 % Microsoft, 100 % AWS ou 100 % SAP est une monoculture technologique : performante en conditions stables, vulnérable à la première défaillance de l'acteur unique.

La redondance ensuite. Dupliquer les systèmes critiques, les flux de données, les connaissances humaines pour maintenir le service en cas de panne ou d'absence. Des bases de données en miroir, des serveurs de secours, mais aussi des binômes de compétences sur les briques vitales. La redondance ne peut pas être systématique : elle coûte, économiquement et écologiquement, et une redondance généralisée reproduirait sous une autre forme l'excès qu'on cherche à corriger.

La **modularité** et les **interactions** vont ensemble. La modularité découpe le SI en sous-ensembles autonomes pour isoler les défaillances et limiter leur propagation. Quand un module tombe, les autres continuent : c'est le principe des cloisons étanches d'un navire, transposé à l'architecture informatique. Mais une modularité qui isolerait totalement les systèmes les ferait dépérir l'un sans les autres. Les interactions, elles, multiplient les liens entre équipes, briques techniques et parties prenantes pour que l'entraide compense les défaillances. Les API ouvertes, les communautés, l'open source et l'open data créent des circuits de secours que les architectures fermées n'ont pas. Les deux piliers sont en tension : trop de modularité mène à trop d'interaction (ou les rend trop complexes), et trop d'interactions tue l'isolement. La robustesse vit dans l'équilibre des deux.

La **circularité**, ensuite : renoncer au neuf permanent. Allonger la durée de vie des équipements, c'est réduire la dépendance aux chaînes d'approvisionnement mondialisées. Un serveur qui dure une année supplémentaire est un serveur qu'on n'a pas à commander dans un contexte de tensions sur le silicium, le cuivre ou les terres rares.

L'imperfection : renoncer à l'optimisation absolue. Concevoir avec des marges, pas par négligence mais par design. Un taux d'occupation de 70 % sur les serveurs qu'on maîtrise est un amortisseur qui absorbe les pics de charge et les pannes : les 30 % restants ne sont pas du gaspillage, ils font partie du cahier des charges. La perfection à 100 % est fragile par construction.

La **vision systémique** ferme la liste. Appréhender l'ensemble des dépendances techniques, humaines, économiques et écologiques pour que chaque décision renforce la cohérence

globale du SI plutôt qu'elle n'optimise un élément isolé en reportant la fragilité sur les autres.

Encadré : Du château fort au village agile

Le SI monolithique optimisé ressemble à un château fort : pensé pour des besoins connus et maîtrisés, il repose sur la stabilité, l'épaisseur de ses murs et une structure rigide. Il fonctionne tant que le contexte reste stable et son adaptabilité est faible.

Le village agile, un SI orienté microservice, propose une autre approche : souplesse, diversité des quartiers autonomes, capacité à faire collaborer une multitude d'acteurs. Les risques sont répartis, l'adaptation est rapide, la coopération et la redondance absorbent les crises... au prix d'une complexité élevée, qui peut parfois représenter aussi un risque.

Et puis il y a le chalet en bois : minimaliste, simple, durable. La robustesse n'exige pas toujours une architecture microservices complexe. Parfois, une petite application monolithique bien conçue répond parfaitement au besoin, sans la fragilité du château ni la complexité du village.

Encore une fois, pas de solution par défaut, mais une réflexion à avoir pour choisir le type d'approche qui correspond aux usages.

L'agriculture industrielle comme miroir du SI optimisé

L'analogie la plus directe de la robustesse pour une DSI serait peut-être l'agriculture.

L'agriculture industrielle a maximisé le rendement à l'hectare par la monoculture, les intrants chimiques, la mécanisation lourde et la sélection génétique. Les résultats sont spectaculaires en conditions stables : des rendements multipliés par trois ou quatre en quelques décennies. Mais la résilience écosystémique est détruite. Une parcelle de blé en monoculture est vulnérable à un seul pathogène, un seul ravageur, une seule sécheresse. Une agriculture en polyculture, nourrie de fertilisants naturels, produit moins par hectare. Mais elle produit toujours.

Le SI optimisé procède de la même logique. Le chapitre précédent en a détaillé les mécanismes : la « monoculture » CrowdStrike, le verrouillage fournisseur qui progresse par crans, le confort qui désapprend à fonctionner autrement. Le SI en monoculture s'effondre comme un champ de pommes de terre face au mildiou. La polyculture informatique (diversité de fournisseurs, hétérogénéité contrôlée, compétences réparties) produit moins de performance unitaire, coûte plus cher au quotidien, mais elle tient quand le contexte fluctue. C'est exactement le compromis qu'Ulanowicz a quantifié.

Encadré : La fenêtre de vitalité d'Ulanowicz

Robert Ulanowicz et ses collègues ont fourni en 2009 la démonstration mathématique du paradoxe efficience/robustesse, en étudiant les flux d'énergie dans les réseaux écologiques. La soutenabilité d'un système repose sur un équilibre entre efficience

(qu'Ulanowicz nomme « ascendancy ») et réserve (« overhead »), où il range la redondance et la diversité. C'est, dit autrement, la marge.

Trop d'efficience et le système devient fragile, incapable de répondre aux perturbations. Trop de redondance et le système est sous-développé, incapable de fonctionner correctement. L'optimum se situe autour de $\alpha \approx 0,46$, un ratio entre ascendancy et capacité totale. Tous les écosystèmes naturels durables se situent dans cette « fenêtre de vitalité » étroite.

Goerner, Lietaer et Ulanowicz ont étendu ce résultat aux systèmes économiques en 2009. Aucune publication n'a encore appliqué ce cadre formellement aux architectures SI. Si le ratio n'est pas simple à calculer, la réflexion générale est facilement transposable : un SI qui alloue 100 % de ses ressources à la performance (zéro marge, zéro redondance, zéro diversité) est hors de la fenêtre de vitalité. Un SI qui redonde tout est insoutenable économiquement et écologiquement. L'enjeu est de trouver le bon ratio, le bon équilibre, et il n'est pas à 100 % d'efficience.

Combiné aux travaux de Hamant, ce résultat borne la frugalité des deux côtés. Sous-performer, chez Hamant, est la condition de la robustesse : borne basse, celle qui interdit de couper tout le mou. La fenêtre de vitalité fixe la borne haute : trop d'efficience fait sortir du domaine où le système reste viable.

Le pont est structurel

Les mêmes mécanismes opèrent dans les écosystèmes et dans les systèmes d'information. Charles Perrow l'avait démontré dès 1984 dans *Normal Accidents* : dans les systèmes à la fois complexes et fortement couplés, les accidents catastrophiques sont une propriété inhérente du système.

CrowdStrike en est la démonstration vivante : interaction imprévisible entre deux composants, couplage fort, propagation planétaire en quelques minutes. Perrow identifie un paradoxe qui résonne avec Hamant : la redondance elle-même peut accroître la fragilité, en ajoutant de la complexité et en encourageant la prise de risque (à la manière d'un acrobate qui prend plus de risques lorsqu'il sait qu'un filet de sécurité est tendu en dessous). C'est ce qu'on observe dans les architectures SI surchargées de couches de protection.

Le mécanisme n'a pas pris sa retraite avec CrowdStrike. Les 19 et 20 octobre 2025, une défaillance dans l'automatisation DNS de DynamoDB a paralysé la région AWS US-EAST-1 pendant une quinzaine d'heures, cascade comprise : lancement d'instances, répartiteurs de charge, puis plus d'un millier de services grand public et professionnels (post-mortem AWS, analyses ThousandEyes, octobre 2025). Pas d'attaquant, pas de sous-traitant défaillant : une cause interne unique, un couplage serré, un effet mondial.

La réponse de l'ingénierie logicielle existe déjà : le Chaos Engineering, inventé par Netflix, qui consiste à éteindre volontairement en production ce qui marche, pour découvrir où ça

ne marcherait pas. Le changement, lui, relève d'abord de la culture : passer de « que se passe-t-il si ça tombe ? » à « que se passe-t-il quand ça tombe ? »

Deux principes pour le SI

De tout cela, nous tirons deux principes de fonctionnement pour un SI plus robuste. Ils ne sont pas au même rang : le second ne s'applique que là où le premier devient impossible.

1. La non-régression des capacités

L'Organisation maritime internationale impose, depuis des décennies et malgré le GPS, que les officiers de pont sachent encore naviguer au sextant et lire une carte papier. La technologie renforce, elle ne remplace pas. On garde la capacité de faire sans.

C'est le premier principe : une organisation qui s'appuie sur un outil informatique pour un usage donné doit rester capable d'assurer cet usage si l'outil disparaît. Le numérique s'ajoute à une capacité, à un savoir-faire ; il ne doit pas les faire disparaître.

2. La continuité impérative

Restent les cas où l'on ne peut plus se passer du numérique : un système bancaire, un dossier médical informatisé, une ligne de production automatisée. Là, et seulement là, s'applique le second principe. Puisqu'on ne peut pas se passer de l'outil, il faut qu'il ne tombe pas - ou qu'il assure un service minimal quand il tombe. Concrètement : dupliquer plus que nécessaire (sur-redondance), répartir sur plusieurs sites et plusieurs technologies (diversification), prévoir un mode dégradé plutôt qu'un arrêt net.

C'est la continuité impérative.

La séquence

Les deux principes s'enchaînent. On pose d'abord la question de la non-régression : si cet outil disparaissait, saurait-on encore rendre le service ? Tant que la réponse est oui, on protège cette capacité de repli : c'est la voie la plus robuste, et la moins coûteuse, pour l'environnement comme pour le budget. Ce n'est que lorsque la fonction ne peut plus exister sans numérique qu'on passe à la continuité impérative : puisqu'on ne peut plus faire sans, comment éviter que ça lâche ? La séquence force une question que le réflexe technologique fait oublier : avant même de chercher comment sécuriser l'outil, saurait-on faire sans ?

Ces deux principes dessinent d'abord un état d'esprit : accepter que les chocs viennent, garder la capacité de faire sans le numérique, protéger farouchement ce qu'on ne peut pas accepter de perdre. Mais le second principe porte son propre avertissement. La continuité impérative coûte : en ressources, en compétences, en empreinte. Tout rendre robuste, partout, sans choix ni filtre, serait à son tour insoutenable. D'où la question : qu'est-ce qui, dans le SI, mérite qu'on y engage cette ressource rare ?

Références

- Hamant, *La Troisième voie du vivant*, Odile Jacob, 2022. *Antidote au culte de la performance*, Gallimard Tracts, 2023. *L'Entreprise robuste* (avec Charbonnier et Enlart), Odile Jacob, 2025. « Is incoherence required for sustainability? », *The Anthropocene Review*, 2025.
- Citations d'Olivier Hamant en corps de chapitre : entretiens Daily Science (février 2026) et Rumeur Publique.
- ThousandEyes, *AWS Outage Analysis: October 20, 2025* ; post-mortem AWS, octobre-novembre 2025.
- Taleb, *Antifragile*, Random House, 2012.
- Ulanowicz, Goerner, Lietaer & Gomez, « Quantifying sustainability », *Ecological Complexity*, 2009.
- Perrow, *Normal Accidents*, Princeton University Press, 1984.
- Shift Project, *Rapport sur la sobriété numérique*, 2024.
- Parametrix, *CrowdStrike Outage Impact Report*, 2024.

Chapitre 4. Le filtre du bien commun

En atelier FluctuIT (l'atelier d'exposition aux chocs, détaillé au chapitre 6), quand on a fini d'exposer le SI aux chocs et qu'on aborde les leviers de robustesse, la même question revient à chaque fois : qu'est-ce qu'on rend robuste, au juste ?

La tentation est de tout couvrir. Elle est insoutenable. Les marges se paient en budget, en complexité, en ressources environnementales. Si l'on appliquait les principes de robustesse à l'intégralité d'un SI, on reproduirait sous une autre forme l'excès qu'on cherche à corriger. Il faut un filtre et ce filtre ne peut pas être purement technique.

La santé commune comme boussole

Qu'on soit dans une démarche de numérique responsable ou de robustesse, une question revient en filigrane au moment du questionnement des usages : qu'est-ce qui est utile ? Chaque action la présuppose (ou devrait le faire).

Et pourtant, jusque-là, j'ai esquivé la question de la définition de ce qui est utile. Questionner l'utilité, vérifier que les impacts positifs dépassent les impacts négatifs, c'est le cœur du sujet. Mais le faire concrètement est une autre affaire. On se retrouve vite face à des arbitrages politiques, des rapports de force qui dépassent le cadre du système d'information. L'affirmation « quoi qu'il en soit, ce service est indispensable » clôt souvent le débat. Qui est légitime pour questionner ? Jusqu'où creuser ?

Il faut pourtant un cap, car sans critère de tri, la robustesse devient une fin en soi : on déploie de l'énergie pour rendre robustes des systèmes qui ne méritent peut-être pas de l'être, et qui dans certains cas viennent fragiliser le système (par exemple en pesant sur les limites planétaires plus que de raison).

Olivier Hamant propose un concept qui peut servir de boussole : la santé commune. C'est elle que le SI sert, au bout du compte ; le filtre en découle : un usage mérite l'effort de robustesse s'il y contribue. Elle articule trois dimensions indissociables, qui se conditionnent mutuellement.

- La santé humaine : conditions de travail, charge cognitive, équilibre de vie.
- La santé sociale : liens, équité, inclusion, accès aux services.
- La santé des milieux naturels : ressources, émissions, impact sur le vivant.

Un projet qui dégrade l'une de ces dimensions finit par fragiliser les autres. Un SI qui épuise ses utilisateurs génère du turnover qui érode les compétences. Un service qui exclut une partie de la population crée de la dette sociale. Une infrastructure informatique qui ignore les limites planétaires verra arriver sa propre obsolescence lorsque les composants ou les ressources ne seront plus disponibles.

Transposé au SI : qu'est-ce qu'un usage essentiel ?

La question première n'est donc pas « comment renforcer la robustesse ? » mais « que rendre robuste, et pourquoi ? ».

Rendre robuste a un coût : financier, organisationnel, environnemental. Si cette question n'est pas posée, on risque de déployer de l'énergie pour rendre robustes des systèmes qui ne méritent pas de l'être, et qui, dans certains cas, fragilisent l'ensemble en consommant des ressources rares.

Un SI « blindé » dans une entreprise déconnectée du réel, c'est un squelette en titane dans un corps épuisé. On tient debout, mais on avance vers quoi ?

Transposé au SI, le filtre prend la forme de trois questions. Les deux noms cohabitent : le bien commun nomme le filtre ; la santé commune, avec ses trois dimensions, en donne le critère. Un usage mérite d'être robustifié s'il passe ces trois tests.

- Il ne dégrade pas les conditions de travail, la santé physique ou la santé mentale des utilisatrices et utilisateurs.
- Il ne creuse pas les inégalités d'accès ni ne concentre les pouvoirs de façon excessive.
- Il respecte les limites planétaires

Si deux réponses sur trois sont négatives, le projet doit être revu avant tout investissement en robustesse. Une seule réponse négative n'arrête pas le projet : elle désigne ce qu'il faut corriger avant d'investir.

La santé commune ne donne pas de réponses automatiques : elle donne une direction. Un service peut améliorer la santé sociale tout en dégradant la santé des milieux. Un autre peut respecter les limites planétaires mais concentrer les pouvoirs chez un seul acteur. Les arbitrages restent difficiles. Ce qui compte, c'est d'avoir un cap explicite plutôt que de laisser les décisions se prendre par défaut, au fil de l'eau, sans critère.

Encadré : Le triage comme analogie

En médecine de catastrophe, le triage consiste à classer les patients non pas par ordre d'arrivée ni par gravité brute, mais par capacité à bénéficier du soin dans les conditions disponibles. On ne soigne pas tout le monde de la même façon. On concentre les ressources là où elles produisent le plus d'effet, en acceptant de ne pas traiter ce qui ne peut pas l'être ou ce qui guérira seul.

Le filtre du bien commun appliqué au SI procède de la même logique : on ne rend pas tout robuste. On concentre les efforts sur les usages qui bénéficient réellement de la robustesse (ceux qui servent la santé commune) et on accepte de laisser le reste en mode fragile, simplifié ou décommissionné. Le triage concentre les ressources disponibles là où elles comptent. La marge est exactement ce genre de ressource : on ne peut pas l'entretenir partout, on choisit où elle produit le plus d'effet.

Appliquer le filtre : plus facile à énoncer qu'à pratiquer

Le triple filtre est simple à formuler, le pratiquer l'est beaucoup moins. La difficulté vient de ce qu'un outil numérique peut être techniquement irréprochable, économiquement viable à court terme, et contre-productif par construction. Le rendre robuste dans cet état, c'est investir pour consolider un problème plus global.

Prenons un cas courant. Une organisation déploie un chatbot IA sur un service public pour « fluidifier » l'accueil. Le chatbot fonctionne. Il réduit le temps d'attente moyen. Il est écoconçu. Trois indicateurs au vert. Pour autant, les usagers qui n'arrivent pas à formuler leur demande dans les termes que le modèle attend n'ont plus d'alternative humaine : le guichet a été fermé six mois plus tôt. Le service dégrade la santé sociale (exclusion des publics fragiles) pour améliorer une métrique de performance. Faut-il le rendre robuste, ou faut-il d'abord se demander s'il devrait exister sous cette forme ?

Un service cloud qui gère l'attribution de logements sociaux mérite une robustesse maximale : il sert la santé sociale, il n'a pas d'alternative simple, sa défaillance prive des personnes de leurs droits.

Le filtre s'applique aux services plus qu'aux entreprises. La question « faut-il rendre robuste le SI d'un pétrolier ? » se décompose : la paie, la sécurité des sites, la détection de fuites méritent l'effort sans hésitation ; l'optimisation de l'exploration, non, et ce refus n'a rien de technique. Le découpage a une limite qu'il faut regarder en face : service par service, la somme des robustesses renforce l'ensemble, y compris ce qu'on refusait de servir. Quand le désalignement est structurel, la réponse n'appartient plus au filtre mais à la finalité de l'organisation. Le chapitre 7 pose le principe : transformer plutôt que robustifier.

La graduation des réponses est le signe que le filtre fonctionne. Il ne dit pas oui ou non. Il dit : à quel niveau d'investissement en robustesse, pour quel niveau de service, au bénéfice de qui.

Parfois, le bon niveau d'investissement est zéro. Le critère mobilise deux questions déjà posées : ce service sert-il la santé commune, et que se passe-t-il s'il tombe ? Quand la chute ne menace ni la fonction essentielle ni l'organisation, la bonne réponse est de ne rien construire. D'autant que chaque parade ajoute sa propre complexité : un mécanisme de bascule, par exemple, c'est du code, des procédures et des exercices qui peuvent eux-mêmes lâcher. On tombe, on se relève, et ce n'est pas un échec de la démarche : c'est la démarche. Pour reprendre la métaphore du ski, on ne cherche pas à faire tout le monde des skieurs professionnels de hors-piste. Sur une pente où la chute se paie d'un bleu, on y va même avec un niveau de préparation faible. Sur celle où elle se paie d'une avalanche, on s'encorde. S'encorder sur une piste verte c'est ne plus avancer.

Ne pas robustifier est alors un choix assumé. Le droit de “laisser tomber” s'acquiert en ayant posé la question des conséquences. Un système non essentiel laissé simple c'est aussi de la marge rendue disponible ailleurs : du budget, de l'attention, de la simplicité. Et

la simplicité, on le verra au chapitre suivant avec la low-technisation, est elle-même une forme de robustesse.

Ivan Illich avait nommé ce mécanisme dès 1973 dans *La Convivialité* : au-delà d'un certain degré de développement, un outil cesse de servir l'autonomie de ses utilisateurs et commence à les asservir. Louis Derrac parle de « numérique acceptable » : un numérique dont on peut collectivement accepter les impacts parce qu'ils restent proportionnés aux bénéfices et compatibles avec les limites. C'est exactement ce que le triple filtre opérationnalise.

De la question à la méthode

Soyons honnêtes : poser les bonnes questions ne suffit pas à trancher les arbitrages. Il faut aussi une méthode, même imparfaite. Ce qui suit est ce que nous utilisons en mission, condensé en encadré pour que le manifeste reste un manifeste.

Encadré : Trois étapes d'un filtre en mission

Cartographier les impacts. Pour tout projet SI, identifier les impacts négatifs (consommation de ressources, exclusion de publics, création de dépendance, complexité non nécessaire) et les impacts positifs (contribution à la mission, amélioration des conditions de travail, renforcement de l'autonomie, création de liens ou de communs). L'exercice n'a pas besoin d'être exhaustif pour être utile, mais il a besoin d'être honnête.

Filtrer. Le projet a-t-il une utilité alignée avec la raison d'être de l'organisation et compatible avec les limites planétaires ? Si non, arrêter. Si oui, les impacts positifs sont-ils supérieurs aux impacts négatifs ? Si non, adapter ou arrêter. Si oui, cadrer avec un budget carbone, des critères de robustesse, des modes dégradés définis et une revue périodique.

Tester. Soumettre le projet à des scénarios de fluctuation : énergie +50 %, fournisseur défaillant pendant trois mois, compétences clés indisponibles, crise prolongée. Si le projet ne passe pas ces tests, il n'est pas robuste, et l'investir en robustesse ne changera rien si ses fondations sont fragiles.

D'autres méthodes convergent. Le Shift Project a proposé en 2024 une démarche d'évaluation des projets d'IA, transposable à tout projet SI. Son apport : elle commence par une trajectoire de référence (que se passe-t-il si on ne fait rien ?), caractérise le besoin réel avant d'explorer les solutions techniques, et pose l'abandon comme une option légitime. Un projet incompatible avec un budget carbone cohérent après optimisation mérite d'être reformulé ou arrêté.

En diagnostic, lors de missions Nuageo, nous ajoutons une question préalable à ces trois étapes, la « question zéro » : le service numérique concerné a-t-il une utilité vérifiable pour la mission de l'organisation ? Si la réponse est non ou incertaine, la recommandation est de reformuler avant d'investir quoi que ce soit en robustesse. Le principe de

non-régression sert ensuite de test concret. Si l'ERP, le CRM ou l'outil collaboratif disparaissait demain matin, les fonctions vitales de l'organisation pourraient-elles continuer ? Si la réponse est non et qu'aucune alternative n'existe, on est face à une dépendance critique qui exige un investissement (en temps, en argent, en compétences etc.) immédiat. Si la réponse est oui, le développement de la robustesse de ce service est peut-être moins prioritaire qu'on ne le pensait.

L'incendie du datacenter gouvernemental de Daejeon, traité au chapitre 2, montre ce qui arrive quand aucun de ces filtres n'a été appliqué : une violation intégrale du principe de non-régression, où le contrôle national de l'infrastructure, sans robustesse, n'était qu'une souveraineté de papier. Les bonnes questions n'ont pas été posées.

Dans le même esprit, l'association Designers Éthiques propose un arbre de décision pour mesurer la pertinence d'un service numérique avant sa conception : besoin réel, accessibilité, impacts sociaux et environnementaux. C'est une méthode voisine du triple filtre de la santé commune, conçue initialement pour la conception plus que pour la robustesse.

S'assurer de répondre à la bonne question

La méthode et les outils sont là. Reste un piège que la méthode ne couvre pas : poser la mauvaise question.

« Dans le monde de la performance, on répond vite à de mauvaises questions. » Hamant pose le diagnostic (Hamant, *L'Entreprise robuste*, 2025). Appliqué au SI, le piège est omniprésent.

« Comment optimiser notre datacenter ? » On améliore le PUE, on installe un refroidissement à eau, on déploie une IA de gestion thermique. Bonne réponse technique. Mais la question préalable est peut-être : ce datacenter sert-il notre mission ? Avons-nous besoin de stocker toutes ces données ?

« Comment automatiser ce processus ? » On déploie du RPA, des workflows, de l'IA générative. Mais la question préalable est peut-être : cette automatisation améliore-t-elle les conditions de travail ou précarise-t-elle des emplois ? Que se passe-t-il quand l'outil tombe ?

On se pose des questions techniques qui conduisent trop souvent à éluder les questions de finalité. Et chaque réponse technique qui ignore la finalité renforce un système qui n'a peut-être pas de raison d'être sous cette forme. Appréhender le SI par le prisme de la robustesse est une occasion de poser ces questions de finalité au niveau de la direction générale.

Trois méritent d'être formulées sans détour.

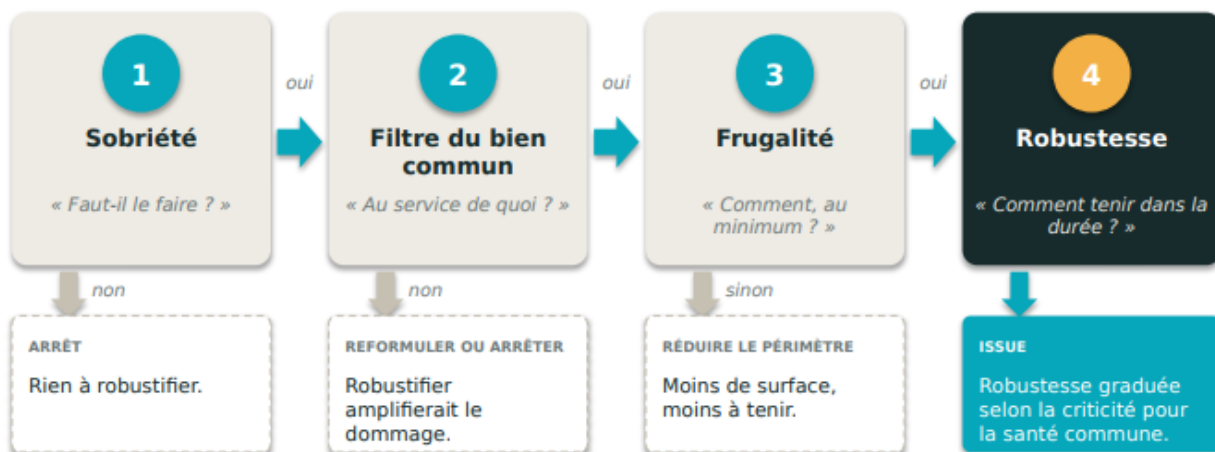
1. **Quel est le sens réel de nos activités ?** Améliorent-elles concrètement la vie des gens et l'état des milieux naturels, ou relèvent-elles d'une recherche de profit à court terme ?

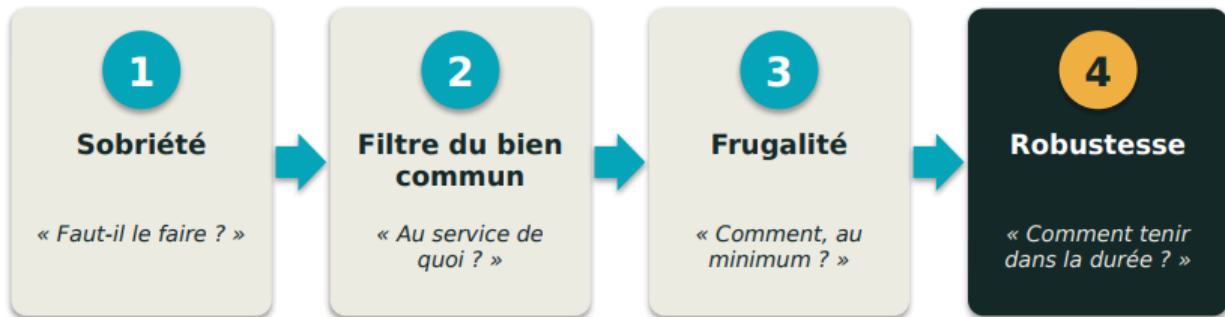
2. **Quelles sont nos priorités réelles ?** La rentabilité immédiate ou la pérennité à long terme ?
3. **Notre modèle est-il adaptable ?** Sommes-nous capables d'ajuster nos trajectoires face aux contraintes qui s'annoncent : énergie, approvisionnements, réglementation, compétences ?

Ces questions peuvent révéler que certaines activités ne méritent pas d'être rendues robustes parce qu'elles ne servent pas la santé commune. Investir dans la robustesse d'une plateforme de dropshipping de produits jetables, c'est techniquement possible. C'est aussi pérenniser des impacts négatifs qui ne tiennent pas sur le long terme. En rendant robuste ce type d'usage, on amplifie la destruction de ce qu'on prétend protéger.

La conséquence logique du filtre est que certains services doivent être simplifiés, réduits ou arrêtés. Sur les cent vingt applications référencées dans la cartographie d'une ETI industrielle que nous accompagnons, une trentaine n'avaient plus d'utilisateur identifié. Personne n'avait pris la décision de les éteindre, par inertie ou par crainte d'un impact non documenté. Le patrimoine applicatif évolue par addition, rarement par soustraction. Le décommissionnement est un acte de gestion.

Le filtre du bien commun prolonge la séquence posée au chapitre 1 : sobriété d'abord, frugalité ensuite. Il y ajoute une dimension : ce service sert-il la santé commune ?





Chaque étape conditionne la suivante : on ne robustifie que ce qui a passé les filtres précédents.

La séquence de tri complète devient : sobriété (faut-il le faire ?) → filtre bien commun (au service de quoi ?) → frugalité (comment au minimum ?) → robustesse (comment tenir dans la durée ?). Chaque étape élimine des projets. C'est le but d'une démarche de soutenabilité forte appliquée au SI.

C'est bien les étapes 1 et 2 qui sont les plus importants et poire splus complexe à re en place, d'autant plus à l'échelle d'une DSI seule, ou même d'une organisation seule.

Un numérique au service de l'organisation et du bien commun. Qualifier l'utilité avant la solution, prioriser ce qui sert. Sinon, réduire, simplifier ou arrêter.

Un mot pour lever une confusion possible, le but premier est d'être soutenable : un SI qui tient dans la durée sans épuiser ce dont il dépend. La robustesse n'en est pas une alternative, elle en est la condition manquante : un SI optimisé pour la seule empreinte reste en soutenabilité faible et donc insoutenable au premier choc. On n'a pas à choisir entre robuste et soutenable ; on devient soutenable, notamment, parce qu'on se rend robuste. Le filtre du bien commun, lui, donne une direction à cette robustesse.

La latitude réelle pour imposer ce filtre dans les organisations est limitée, je le sais. Les DSI n'ont pas toujours la légitimité de questionner les choix métiers. Les arbitrages budgétaires court-termistes résistent aux raisonnements systémiques. Pour autant, ne pas poser la question revient à laisser le SI se construire sans cap, techniquement robuste peut-être, mais au service de quoi ? Une robustesse sans filtre de finalité est aveugle, une sorte de "robust-washing". Avec ce filtre, elle devient une démarche sincère vers la soutenabilité forte.

Nous venons de voir ce qu'il fallait ou non rendre robuste. Reste le comment.

Références

- Hamant, Negrutiu, Riem, Santé commune (concept développé dans *L'Entreprise robuste*, Odile Jacob, 2025).
- Shift Project, *Déployer la sobriété numérique : IA*, 2024.
- Illich, *La Convivialité*, Seuil, 1973.
- Derrac, *Numérique acceptable*, 2024.
- AFNOR SPEC 2314, *IA frugale*, juin 2024.

TROISIÈME PARTIE. Mise en œuvre

“Quelque part en 2030, dans une banque mutualiste : l'ouverture d'un compte en agence ne dépend plus d'un réseau qui répond, et quatre coopératives entretiennent ensemble un socle technique mis en commun.”

** Récit d'atelier, déroulé au chapitre 7.**

Le numérique responsable optimise dans un cadre qu'il ne questionne pas : c'est de la soutenabilité faible. Le monde qui vient, lui, est incertain, traversé de crises multiples, et une logique d'optimisation n'est pas taillée pour y faire face. La cible est la soutenabilité forte : un SI qui maintient ses fonctions essentielles à travers les chocs, au service de la santé commune. Le chemin pour y parvenir : une démarche de robustesse, cadrée par le filtre du bien commun. Reste tout le travail : traduire ce cadre en gestes qu'une DSI peut réaliser au quotidien et porter dans une organisation. C'est l'objet de cette troisième partie.

Six leviers d'abord, chacun au service de la marge posée au chapitre 2. Puis trois gestes initiaux pour voir ce qu'on ne voyait pas et fermer les vulnérabilités les plus béantes. Enfin ce que cette trajectoire change pour la personne qui la porte, parce que c'est elle qui tiendra ou non dans la durée.

Chapitre 5. Six leviers pour un SI soutenable

Le comment tient en six leviers. Ils traduisent la robustesse en gestes opérationnels pour une DSI, en s'appuyant sur le cadre posé au chapitre 3 (non-régression et continuité impérative) et sur le filtre du chapitre 4 (qu'est-ce qu'on rend robuste, au service de la santé commune).

Les voici :

- **Autonomie stratégique** : réduire les dépendances techniques et contractuelles pour rester maître de ses trajectoires.
- **Résilience technique** : concevoir des systèmes qui continuent à rendre le service attendu, même partiellement, en cas de problème majeur.
- **Gouvernance et compétences** : décider vite, au bon niveau, avec des compétences partagées.
- **Sobriété et frugalité** : questionner le besoin avant d'optimiser la réponse et opérer dans le cadre des limites planétaires.
- **Low-technisation** : couvrir le besoin par des solutions simples, réparables, modulaires, lorsque l'usage ne justifie pas la complexité.
- **Acceptabilité sociale** : ancrer la conception dans l'usage réel des personnes auxquelles le service s'adresse, en maintenant l'accessibilité et l'équité, pour toutes et tous de manière pérenne.

Ces leviers sont interdépendants : la robustesse provient de leur cohérence, pas de l'excellence sur un seul. Ils représentent les gestes par lesquels une organisation cesse de consommer sa marge, sous les cinq formes posées au chapitre 2 : la capacité, le fonctionnement dégradé, la diversité, le savoir-faire, la réversibilité. C'est ce qui en fait la traduction opérationnelle de la soutenabilité forte.

Levier 1. Autonomie stratégique

« Réduire les dépendances techniques et contractuelles pour rester maître des trajectoires technologiques. »

Définition. L'autonomie stratégique consiste à réduire les verrouillages techniques, contractuels et juridictionnels qui rendent une organisation incapable de modifier ses choix technologiques sans engager des coûts ou des délais hors de proportion. Deux des cinq formes de la marge se jouent ici : la diversité des fournisseurs et la réversibilité.

L'enjeu est d'identifier les dépendances qui mettent réellement en risque les processus dont l'organisation ne peut pas se passer et de préparer des alternatives crédibles. Chasser tous les fournisseurs propriétaires ou non européens serait illusoire et contre-productif, correspondant à une approche quasi survivaliste du SI. La question utile est « de quoi sommes-nous dépendants au point de ne pas pouvoir nous en passer ? ».

Cette dépendance se mesure sur plusieurs dimensions.

- Une dépendance technique : peut-on migrer vers une autre solution sans réécrire l'ensemble du SI ?
- Une dépendance juridictionnelle : les données et les services sont-ils soumis à des législations extraterritoriales qui peuvent un jour poser problème ?
- Une dépendance économique (parfois contractuelle) : a-t-on les moyens financiers d'une migration sans mettre l'organisation en danger ?
- Une dépendance de compétences : les équipes sauraient-elles exploiter une alternative ?
- Et une dernière dimension, plus rarement questionnée : la dépendance énergétique et matérielle. Que fait-on si les composants ne sont plus livrés, si l'électricité devient intermittente ? La chaîne d'approvisionnement du numérique repose sur des fondations que la plupart des DSI ne contrôlent pas.

Exemple : GendBuntu. La Gendarmerie nationale a migré à partir de 2008 des dizaines de milliers de postes vers une distribution Linux interne, baptisée GendBuntu. Le motif était pragmatique : dépendre entièrement d'un éditeur étranger pour l'équipement informatique des forces de l'ordre constituait un risque trop élevé. Toutes les organisations n'ont pas ce besoin, mais toutes gagneraient à se poser la question dans leurs propres termes : quel service informatique, si on le perdait demain matin, rendrait notre mission principale irréalisable ?

Le rachat de VMware par Broadcom illustre le revers : des hausses de 300 à 500 % sur des contrats existants, et jusqu'à 1 050 % allégués par AT&T dans la procédure qui l'a opposée à Broadcom. Quand la diversité des fournisseurs a été éliminée par dix ans de consolidation, le verrouillage ne se voit qu'au moment où il est exploité. Se libérer alors d'une telle dépendance est complexe, cher, et douloureux, pour autant pas impossible : deux ans après le rachat, une partie des clients VMware avait engagé ou achevé sa migration vers des alternatives. La réversibilité existe, à un coût mais ce coût se décide bien avant la hausse, au moment du choix d'architecture et de la signature du contrat. Le vrai levier est ailleurs : ne jamais laisser la dépendance se refermer, garder une alternative crédible, sécuriser les conditions de sortie au moment de la contractualisation.

Se lancer dans une démarche d'autonomie stratégique peut commencer par un diagnostic en trois temps.

- Le premier est l'identification et la cartographie des services critiques : ceux sans lesquels l'organisation ne fonctionne plus - au niveau métier, financier, qui la met en risque au niveau réglementaire, ou qui a un impact direct sur les bénéficiaires (salle d'opération, CAF, site SEVESO, etc.). La question centrale à se poser : quels sont les usages critiques de mon organisation qui ne peuvent pas fonctionner sans outil informatique ?
- Le deuxième temps est l'évaluation du niveau de dépendance des services critiques. On remonte les dépendances couche par couche : ressource, infrastructure, plateforme, applications, compétences, données, intelligence. À la fin, on obtient une liste des dépendances de chaque service.
- Le troisième temps est l'arbitrage. Certaines dépendances sont acceptables : on les assume et on les rend visibles. D'autres ne le sont pas, et les actions visent soit à sécuriser la dépendance par des dispositifs concrets (clauses de réversibilité contractuelle, export régulier et testé des données dans un format ouvert, couche d'abstraction type API), soit à migrer (voire à arrêter le service), car on n'assume pas la dépendance et le risque associé.

Au bout de ce diagnostic, aucune organisation n'a remplacé une solution par une autre : le but est d'avoir une vision claire de ce qui est critique et du niveau de dépendance acceptable ou non, pour chacune de ces briques. Aucune dépendance n'est laissée invisible.

L'Open source et reconditionnement. Le logiciel libre apporte trois propriétés utiles : accès au code source, absence de verrouillage contractuel, mutualisation des efforts via une communauté. Encore faut-il les compétences pour les exploiter. L'affaire XZ Utils (mars 2024) a rappelé que la solidité d'un commun vient de la communauté qui le porte : une backdoor introduite par un contributeur infiltré sur deux ans a failli se propager à l'ensemble des distributions Linux majeures, détectée *in extremis* par un ingénieur hors du projet.

Indicateurs :

- Part du budget SI dépendante d'un fournisseur unique (Exemple de repère : pas plus de 40 % chez un même fournisseur sur les services vitaux)
- Délai estimé de migration vers un fournisseur alternatif par brique critique (repère : moins de six mois)
- Export complet ET réutilisation des données effectivement testé (oui ou non ; la réponse est presque toujours non au premier diagnostic)

Levier 2. Résilience technique

« Concevoir des systèmes qui continuent à rendre le service attendu, même partiellement en cas de problème majeur. »

Définition. On conserve ici le terme de résilience technique, parce qu'il est ancré dans le vocabulaire de l'ingénierie logicielle, tout en l'inscrivant dans le cadre de la robustesse posé au chapitre 3. La résilience technique est la capacité d'un système à continuer de rendre, au moins partiellement, le service attendu quand l'un de ses composants tombe. Tout redonder serait coûteux, contre-productif et environnementalement insoutenable. Elle consiste à pratiquer une redondance sélective sur les services vitaux, à isoler les défaillances pour éviter les effets domino, et à définir des modes dégradés acceptables, testés régulièrement. C'est un des piliers opérationnels du principe de continuité impérative posé au chapitre 3 : quand le numérique ne peut pas être contourné, la robustesse intervient en seconde ligne.

Deux formes de marge se jouent ici : le fonctionnement dégradé, qu'on prévoit avant d'en avoir besoin, et la capacité, dont l'indicateur de ce levier (un taux d'occupation cible de 70 %) est la traduction directe.

Exemple : BNP Paribas et la deuxième région cloud. Fin 2024, BNP Paribas a annoncé l'extension pour dix ans de son partenariat avec IBM Cloud, en y ajoutant une deuxième région cloud dédiée au plan de reprise d'activité. Le contexte direct était celui de la mise en conformité avec DORA, le règlement européen sur la résilience opérationnelle des services financiers. Le contexte plus profond était celui d'une montée en risque systémique qui rend la continuité des services bancaires non négociable. La décision est notable pour deux raisons. D'une part, l'investissement est significatif mais limité aux services réellement vitaux : la redondance n'est pas appliquée à l'ensemble du SI, elle est ciblée par criticité. D'autre part, le couple « fournisseur unique avec deux régions » reste exposé à un risque qu'une vraie diversification de fournisseurs aurait réduit. La résilience technique gagne, la démarche complète de robustesse reste à construire. C'est précisément pourquoi les leviers ne s'appliquent pas isolément.

Exemple : Netflix et le Chaos Engineering. Netflix a inventé le Chaos Engineering en 2010, lors de sa migration vers AWS. Le principe : injecter délibérément des pannes en production pour vérifier que le système les absorbe. Chaos Monkey tue aléatoirement des instances, Chaos Gorilla désactive des zones de disponibilité entières, Chaos Kong simule la perte d'une région AWS complète. La logique culturelle qui sous-tend ces outils est plus tranchée que les outils eux-mêmes. Netflix a admis, comme axiome opérationnel, que les pannes étaient inévitables et qu'il fallait s'organiser pour qu'elles soient un événement banal. Le service de streaming a basculé plusieurs fois entre régions AWS sans que les utilisateurs s'en aperçoivent parce que l'équipe avait payé d'avance le coût de la robustesse, en éteignant volontairement ce qui marchait, pour découvrir où ça ne marcherait pas en cas de vrai incident.

Patterns d'architecture. Plusieurs approches techniques mettent en œuvre la résilience par conception :

- *Circuit breakers* : couper l'appel à un service défaillant pour empêcher la propagation

- *Load shedding* : délester les requêtes les moins critiques quand la charge dépasse la capacité
- *Fallback* : servir une réponse dégradée mais cohérente quand la réponse normale est indisponible
- *Graceful degradation* : maintenir un service partiel quand certaines fonctions tombent

Encore une fois, ce sont des approches qui existent mais qui sont sous-utilisées en dehors des grandes plateformes, parce qu'elles coûtent en effort à la conception et ne se voient pas tant qu'aucune panne n'arrive.

Indicateurs :

- Fréquence des tests de bascule effectivement réalisés (repère : au moins une fois par trimestre sur les services vitaux)
- Taux d'occupation cible des infrastructures (repère : ~70 % en nominal pour conserver une marge d'absorption)

Levier 3. Gouvernance et compétences

« **Décider vite, au bon niveau, avec des compétences partagées.** »

Définition. Travailler la robustesse au niveau organisationnel est aussi déterminant que de la travailler au niveau technique. Un SI techniquement résilient, piloté par une organisation rigide ou centralisée, reste fragile parce que les décisions ne pourront pas être prises assez vite quand la crise surviendra. Ce levier porte sur deux dimensions complémentaires : la capacité de décider et d'agir au bon niveau, en situation normale comme en crise, ce qui inclut la co-décision en amont avec les parties prenantes sur les choix structurants ; et la préservation des compétences humaines qui rendent l'organisation autonome et fonctionnelle.

La forme de marge visée est la plus discrète des cinq : le savoir-faire des équipes internes.

Exemple : la convention IA de la MAIF. Fin 2024, la MAIF a réuni une convention de trente salariés tirés au sort pour co-définir les conditions d'usage de l'IA générative dans l'entreprise. La démarche croise les enjeux d'éthique, de conditions de travail et de performance. Le résultat n'a pas pris la forme d'une charte unilatérale rédigée par la DSI ou la DRH. Il a pris la forme d'un cadre négocié, partagé, qui engage les participants et qui rend les décisions ultérieures plus solides parce qu'elles ne s'imposent pas par le haut. Ce type de dispositif est encore rare. Il est l'un des rares exemples publics d'une gouvernance numérique qui prend au sérieux la question « pour qui faisons-nous ce que nous faisons ? ».

Exemple : TSB, la migration ratée. En 2018, la banque britannique TSB a tenté de migrer 5,4 millions de clients de l'ancien SI Lloyds vers une plateforme Sabis. L'opération a échoué en production. Près de deux millions de clients ont perdu l'accès à leurs comptes pendant des semaines. Dans les mois qui ont suivi, les enquêtes ont montré que la

connaissance fine du SI cœur avait été largement déléguée au prestataire : quand il a fallu reprendre la main en urgence, la maîtrise interne manquait. L'externalisation totale d'une compétence critique revient à céder une marge que l'organisation ne peut pas racheter au moment où elle en a besoin.

Le facteur de bus : Terme issu du développement logiciel : le nombre de personnes qui pourraient être renversées par un bus avant qu'un projet ne devienne ingérable, faute de relais pour reprendre leur savoir.

Un facteur de bus à « 1 » signifie qu'une seule personne détient le savoir critique. Si elle part, tombe malade ou démissionne, personne ne peut prendre le relais. En atelier FluctuIT, on observe régulièrement des organisations qui ont réagi à un incident en internalisant progressivement leurs compétences critiques et en mettant en place des binômes sur chaque brique sensible. En deux ou trois ans, leur facteur de bus moyen passe de « 1 » à « 3 » sur les systèmes vitaux. L'investissement n'est pas négligeable mais il réduit le risque réel et renforce l'organisation au-delà de sa capacité à vivre les chocs.

La mesure vaut aussi pour les dépendances externes : un fournisseur unique sans réversibilité testée, une TMA dont personne en interne ne connaît le contenu, une brique propriétaire sans alternative éprouvée sont des facteurs de bus à « 1 », à l'échelle de l'organisation entière.

Diversité cognitive. L'homogénéisation cognitive est un risque de gouvernance autant qu'un risque cognitif. Si toute l'organisation pense à travers le même outil, la capacité de diagnostic en crise s'appauvrit. Le facteur de bus peut être à 10 sur le code, mais à 1 sur la pensée. C'est ce risque-là, le moins visible, qui s'installe le plus vite quand les outils d'aide à penser (IA générative) sont massivement utilisés.

Et l'outil n'est que la moitié du problème ; l'autre moitié tient au recrutement. Une équipe où tout le monde sort des mêmes écoles, a suivi les mêmes formations, a enchaîné les mêmes missions pense déjà de la même façon avant d'ouvrir le moindre logiciel. L'IA générative ne crée pas cette homogénéité, elle la parachève : elle pose un moule commun par-dessus des profils déjà semblables. La diversité cognitive se joue donc à deux niveaux : qui l'on recrute, et avec quoi on les fait penser.

L'IA accélère ce qu'on sait faire mais freine ce qu'on apprend. Une étude contrôlée d'Anthropic (2026) a mesuré l'effet sur cinquante-deux développeurs : l'usage systématique d'un assistant de code dégrade la maîtrise des concepts. Le sujet n'est pourtant pas « IA ou pas IA » : les développeurs qui utilisent l'IA pour poser des questions conceptuelles, sans lui déléguer le code, retiennent nettement mieux et sont presque aussi rapides. Mais cette discipline suppose un cadre organisationnel. L'organisation qui pousse à « livrer au plus vite » avec l'IA crée les conditions exactes de la délégation totale, celle qui limite le plus l'apprentissage. Les tâches simples qui formaient les juniors ont été captées par l'IA : tests unitaires, corrections mineures, fonctionnalités élémentaires.

L'angle robustesse dépasse la conjoncture : un secteur qui cesse de former ses juniors fabrique sa pénurie de seniors à cinq ou dix ans. C'est de la marge de savoir-faire qui disparaît petit à petit. En robustesse SI, le principe de non-régression se transpose aussi aux compétences : l'équipe peut-elle diagnostiquer un incident sans ses outils IA ? Quelles compétences chaque outil déployé court-circuite-t-il ?

Indicateur :

- Facteur de bus moyen sur les systèmes vitaux (repère : pas en dessous de 3)

Levier 4. Sobriété et frugalité

« Questionner le besoin avant d'optimiser la réponse et opérer dans le cadre des limites planétaires. »

Définition.

Ce levier articule deux gestes qu'il est utile de séparer.

La **sobriété** interroge le besoin lui-même. Avant toute construction numérique, elle pose la question : cet usage a-t-il sa place dans la mission de l'organisation ? Le besoin est-il réel ou supposé ? Un autre mode de réponse, non numérique, conviendrait-il aussi bien ? La sobriété peut conduire à ne rien construire du tout.

La **frugalité**, elle, optimise la réponse une fois le besoin validé. Elle relève de l'écoconception, de l'efficience, de la rationalisation des moyens techniques. Confondre les deux revient à améliorer l'efficacité de services qui n'auraient peut-être pas dû exister. Optimiser un service inutile reste un gaspillage. Plus efficient, certes, mais un gaspillage quand même.

L'ordre des deux gestes compte. Sobriété d'abord : faut-il le faire ? Frugalité ensuite : comment au minimum ? Inversé, l'enchaînement consolide les usages au lieu de les questionner. C'est ce qui se produit dans la majorité des démarches NR contemporaines : l'écoconception est traitée avant la pertinence, et la pertinence n'est presque jamais traitée du tout.

Ce levier agit autrement que les cinq autres : il réduit le périmètre de ce qu'il faudra défendre, au lieu de défendre une forme de marge en propre. Un service qui n'existe pas n'exige aucune marge : rien à concevoir en mode dégradé, aucun fournisseur dont dépendre, aucune compétence à entretenir. D'autres leviers réduisent la dette de robustesse, la low-technisation en tête, en retirant de la complexité à défendre. La sobriété est la seule qui la supprime à la source : pas de service, pas de dette.

Exemple : SNCF Connect. SNCF Connect est l'un des rares services numériques publics français à avoir atteint un score de 82/100 au RGESN, le référentiel général d'écoconception des services numériques (audit Temesis, mai 2025). L'écoconception est intégrée aux sprints de développement. Les exigences environnementales sont inscrites dans les critères projets.

Ce cas documente la frugalité, beaucoup moins la sobriété. Le score RGENS prouve l'écoconception ; il ne dit rien du questionnement du besoin. Si SNCF Connect passe aussi le filtre de la sobriété, c'est par son lien avec sa finalité : faciliter l'accès au train en France contribue à la mobilité bas carbone, la question « ce service mérite-t-il d'exister numériquement ? » a une réponse positive immédiate. Pour la sobriété elle-même, pas de cas public de renoncement en exemple, et pour cause : un service qu'une organisation a choisi de ne pas construire ne laisse pas beaucoup de traces observables de l'extérieur.

Dans les missions de diagnostic que nous conduisons, la question « ce service est-il vraiment utile à la mission de l'organisation ? » génère souvent des échanges difficiles, comme nous l'avons évoqué dans le chapitre 4. Beaucoup d'organisations accumulent des fonctionnalités, des applications et des données sans jamais en réinterroger la pertinence. Quand la question est posée, les équipes SI rappellent un fait que tout le monde connaît : questionner le besoin, c'est questionner les choix métiers. La DSI n'a pas toujours la légitimité de le faire. C'est ce qui explique que tant d'organisations se rabattent sur la frugalité technique, plus confortable car non politique, et les actions sont à leur main.

Cas complémentaire : l'effet rebond. La frugalité sans sobriété peut conduire à un effet rebond, déjà défini au chapitre 1. C'est ce qui s'est passé sur le télétravail, dont les gains environnementaux individuels ont été fortement érodés (31 % en moyenne, ADEME/Greenworking, 2020), sur le cloud et sur l'IA générative.

Pourquoi cette érosion ? Parce que pendant la journée de télétravail, la voiture qu'on ne prend plus pour aller au bureau sert à d'autres trajets - courses, école, rendez-vous : sur près de 4 800 km de navette évités par an, l'étude en voit revenir environ 1 200 en déplacements personnels. Le logement, occupé et chauffé toute la journée, consomme davantage. La visioconférence remplace la salle de réunion physique en présentiel, par du flux vidéo en télétravail. Et, à plus long terme, pouvoir télétravailler autorise à habiter plus loin, ce qui rallonge la navette les jours de présence.

La frugalité sans plafond est contreproductive mais avec une démarche sincère de sobriété, elle devient une arme redoutable.

AFNOR SPEC 2314. La spécification AFNOR SPEC 2314, présentée au chapitre 1, inscrit ce couple sobriété-frugalité dans la définition même du « système d'IA frugal ». Le référentiel d'écoconception de l'IA du collectif Green IT pousse la séquence un cran plus loin : sa toute première fiche invite à envisager de se passer d'IA.

Indicateurs :

1. Nombre d'équipements (PC, téléphones etc.) à remplacer pour bénéficier d'un nouveau service
2. Pourcentage de services ayant fait l'objet d'un arbitrage explicite sur leur pertinence en amont de la conception
3. Existence d'un plafond global de consommation cloud par direction métier, articulé au budget environnemental de l'organisation quand il existe

Levier 5. Low-technisation

« Couvrir le besoin par des solutions simples, réparables et modulaires lorsque l'usage ne justifie pas la complexité. »

Définition. La low-technisation consiste à répondre au besoin avec le niveau de technologie le plus simple qui suffit, et à justifier la complexité avant de l'adopter - jamais l'inverse. Des solutions simples, réparables, modulaires : le Cigref parle de « techno-discernement ». On calibre la technologie sur le besoin, pas le besoin sur la technologie.

Là où la sobriété demande **faut-il le faire ?** et la frugalité **comment le faire au minimum ?**, la low-technisation demande **à quel niveau de technologie ?**. Entre les deux, elle choisit le degré de sophistication de la réponse et le revoit souvent à la baisse.

Sa différence propre ne s'arrête pas là. La low-technisation ne vise pas que l'empreinte. Une solution simple, réparable, modulaire est aussi plus robuste et plus autonome : moins de dépendances, moins de couches, moins de points de rupture. C'est ce qui la rattache directement à la robustesse et ce qui justifie qu'elle soit un levier à part entière, pas une variante de la frugalité.

L'IA générative appliquée aux tâches du quotidien illustre ce réflexe d'arbitrage. Elle ressemble au vol Paris-Nice de la productivité. On prend l'avion pour gagner du temps. Sauf qu'une heure de vol, c'est en réalité quatre heures de trajet avec les aéroports, 158 kilos de CO₂ par passager, et une arrivée fatiguée malgré le « temps gagné ». Cinq heures de train, c'est 2,1 kilos de CO₂, cinq heures pour penser, échanger, travailler, et une arrivée enrichie du temps prétendument perdu. Utiliser une IA générative pour chaque tâche quotidienne provoque un effet rebond : on traite plus de sujets dans la journée, mais avec plus de charge mentale pour vérifier que tout est correct, un rôle de superviseur qui épuise, moins de réflexion, moins de départs page blanche. On devient le carburant de l'IA dans une logique de production continue. La low-technisation, ici, consiste à choisir le train quand le train suffit, pas à s'interdire l'outil.

Est-ce qu'une blockchain est systématiquement nécessaire pour tenir un registre sécurisé ? Pas forcément. Une base de données signée suffit la plupart du temps. Pour une liste d'invités à un petit déjeuner d'entreprise, un tableur fait l'affaire. Pour un anniversaire de dix personnes, un papier et un crayon. La blockchain trouve son sens quand trois conditions se cumulent : plusieurs acteurs indépendants, pas de tiers de confiance disponible, pas de confiance mutuelle préexistante. Hors de ces conditions, elle paie une complexité pour un service qu'une solution plus simple rendrait aussi bien.

La low-technisation est une discipline d'arbitrage qui applique au numérique le principe d'économie de moyens : la solution adéquate est la plus simple qui rend le service attendu, dans les conditions attendues. Toute complexité supplémentaire doit être payée par un bénéfice supplémentaire identifiable. Elle a aussi un effet collatéral souvent ignoré : un système plus simple est compréhensible par plus de personnes au sein d'une DSI, ce qui

augmente le facteur de bus de l'organisation et réduit la dépendance à un petit nombre d'experts.

Ce levier conditionne les cinq formes de marge plus qu'il n'en défend une en propre : une brique que plus personne ne maîtrise en interne (un vieux moteur de règles, un ETL propriétaire dont le dernier expert est parti) devient intouchable. On n'ose plus la modifier, on construit autour, et chaque contournement ajoute une couche de complexité qui rapproche le jour où il faudra tout remplacer d'un bloc. La simplicité est ce qui rend la marge tenable dans la durée.

Exemple : CHU de Rouen. L'attaque par rançongiciel qui a frappé le CHU de Rouen en novembre 2019 reste l'un des cas pédagogiques les plus précis. Pendant plusieurs semaines, l'hôpital a fonctionné en mode papier intégral pour la prescription médicamenteuse, la transmission entre équipes, l'admission et la sortie des patients. Les soignants ont ressorti des classeurs anciens, recréé des feuilles, organisé des relais entre services à la voix. Les soins ont été maintenus. Avec une qualité dégradée, des temps allongés, de la fatigue accumulée, mais maintenus. Les retours d'expérience publiés ensuite ont insisté sur deux points. Premier point : la continuité a tenu parce qu'il restait, dans l'organisation, une mémoire collective du « comment on faisait avant ». Cette mémoire n'avait pas été détruite mais sans démarche volontaire de maintien, elle aurait pu l'être. Second point : aucune des procédures papier n'avait été tenue à jour comme un livrable de continuité. Elles ont été reconstituées en urgence, à partir de souvenirs et d'archives, par les équipes elles-mêmes. Si l'attaque s'était produite cinq ans plus tard, après le départ des soignants encore familiers du fonctionnement non numérique, le résultat aurait pu être très différent.

Dans la même veine, le Centre Hospitalier de Cannes enfin a tiré les leçons de sa propre cyberattaque en préparant des « kits guichet sans SI »

Lors d'un atelier FluctuIT, un participant partageait un dispositif du même ordre. L'ERP qui gère ses magasins est un point de défaillance unique : s'il tombe, plus d'encaissement. Sa solution : envoyer chaque semaine par mail une liste de prix et des templates de factures à imprimer. En cas de panne, les ventes continuent sur papier, et sont reprises ensuite dans l'outil. Le coût de ce dispositif est quasi nul. Le gain en continuité est considérable.

Ce que produit un SI low-tech par conception : diversification des infrastructures, sobriété, formation continue, simplification technique, redondance ciblée, maintien des capacités manuelles. Le futur du SI robuste tient dans moins de dépendances critiques au service d'usages qui ont du sens.

Recommandations institutionnelles. Le rapport Cigref/INR de février 2026 sur l'approche low-tech propose plusieurs mesures concrètes que les DSI peuvent mobiliser : OS durcis et allégés pour les postes critiques, recours à la VHF (Very High Frequency, bande 30–300 MHz, utilisée en radio professionnelle et maritime pour les communications sans infrastructure opérateur) ou aux bandes hautes fréquences pour les services vitaux en situation d'isolement, connectivité minimale par LoRa pour les cas de dégradation réseau

prolongée. Ces mesures existent toutes dans le monde militaire, dans les opérations humanitaires, dans les services de secours mais elles sont rares dans les SI civils, parce que personne ne pense à les commander avant d'en avoir besoin.

Indicateur :

- Pourcentage des processus vitaux dotés d'un mode dégradé non numérique (ou avec des solutions numériques simples, locales, maîtrisées) défini, documenté, à jour et testé au moins une fois par an. Au moment du diagnostic initial : presque toujours inférieur à 10 %. Après deux à trois ans de démarche : 50 à 60 %, sans investissement matériel majeur.

Levier 6. Acceptabilité sociale

« **Assurer l'accessibilité et l'équité des services, pour toutes et tous de manière pérenne.**
»

Définition. Un SI techniquement résilient mais qui exclut les 15,4 % de la population française en situation d'illectronisme (INSEE, données 2021) ou qui discrimine certains publics via ses algorithmes n'est robuste qu'en façade. L'acceptabilité sociale est la condition pour que les services rendus par le SI soient effectivement utilisés par celles et ceux à qui ils s'adressent. Elle a deux faces. Une face d'accessibilité : les services restent utilisables par les publics éloignés du numérique, par les personnes en situation de handicap, par celles dont l'équipement est ancien ou la connexion limitée. Et une face de mode dégradé acceptable : quand le service nominal tombe, le mode de remplacement est compréhensible, accessible, et conçu avec ses usagers. Sans cette deuxième face, la résilience technique produit des modes dégradés qui restent inutilisés au moment où ils devraient prendre le relais : de la marge fantôme dans un sens. L'acceptabilité est ce qui rend la marge effective, pour tous les publics.

Exemple : France Services. Le réseau France Services, déployé à partir de 2019, regroupe aujourd'hui environ 2 800 points de proximité sur le territoire. C'est l'exemple le plus visible en France d'une démarche conçue pour rattraper l'effet d'exclusion produit par la dématérialisation des services publics. Chaque point France Services accueille les usagers qui ne peuvent pas (ou ne savent pas) réaliser seuls leurs démarches en ligne. Ils y trouvent un agent formé et un poste informatique partagé. C'est, dans un sens, la face publique du principe de non-régression : la dématérialisation ne doit pas détruire le service rendu antérieurement, et quand elle risque de le détruire, l'organisation doit financer le canal humain qui restitue l'accès. Le réseau est imparfait. Il est sous-doté. Il dépend des budgets et de la formation continue de ses agents. Mais il existe. Et à ce titre, il représente un gain d'acceptabilité sociale qui n'aurait pas existé sans une volonté politique explicite de le construire.

Exemple : l'algorithme de la CNAF. En 2023, La Quadrature du Net et plusieurs rédactions journalistiques ont obtenu le code source de l'algorithme de scoring utilisé par la Caisse nationale des allocations familiales pour cibler les contrôles. L'analyse a montré que l'algorithme attribuait des scores de risque plus élevés aux mères célibataires, aux personnes en situation de handicap et aux foyers précaires : autrement dit, selon l'analyse de La Quadrature du Net, qu'il pénalisait précisément les publics les plus dépendants des prestations sociales. Le cas est important pour le levier acceptabilité sociale parce qu'il montre l'exact opposé d'une démarche réussie. Un service numérique peut être performant, fiable, scalable, conforme aux meilleures pratiques d'ingénierie, et produire un dommage social systématique invisible pour ses concepteurs. L'acceptabilité sociale est une condition de qualité du service au même titre que la disponibilité ou la sécurité. Et elle suppose, comme conditions méthodologiques, l'audit indépendant des systèmes algorithmiques, la transparence publique sur leurs critères, et la possibilité de contester un score auprès d'un humain.

Co-construction des modes dégradés. Dans un atelier FluctuIT récent conduit auprès d'un bailleur social, on a demandé aux locataires eux-mêmes de prioriser les services qui devaient continuer à fonctionner en mode dégradé lors d'une panne prolongée. Les résultats ont surpris l'équipe IT. La priorité numéro un des locataires n'était pas l'application mobile de signalement des incidents, à laquelle l'équipe consacrait beaucoup d'attention. C'était la possibilité de joindre quelqu'un par téléphone, à un horaire élargi, pour les situations urgentes. Les arbitrages de mode dégradé conçus côté IT et ceux conçus côté usagers ne convergent presque jamais spontanément.

L'IA générative comme contrainte systémique. L'IA générative s'impose partout. Du groupe WhatsApp associatif aux réunions Teams en entreprise. « Pour voir ce que ça donne. » « Pour ne pas être à la traîne. » « Pour rester compétitif. » Le déploiement se fait souvent sans usage identifié, sans valeur ajoutée démontrée, sans mesure d'impact. On est « trop pressés de ne pas paraître dépassés », selon la formule reprise par la coopérative Commown. 31 % des TPE-PME françaises utilisaient l'IA générative en 2025, le double d'un an plus tôt (Bpifrance). Le mimétisme remplace la stratégie.

Pour autant, bannir l'IA générative serait tout aussi insuffisant. Les personnes qui l'adoptent ne font pas « un mauvais choix ». Elles font souvent le seul choix possible pour essayer de répondre à l'exigence de performance de la structure dans laquelle elles se trouvent. Parfois, la charge mentale explose, et l'outil est la seule manière de tout faire tenir dans une journée. Le parallèle avec la fast fashion vaut : SHEIN cartonne moins par inconscience des consommateurs que par contrainte économique et sociale. L'acceptabilité sociale d'un mode dégradé (accepter de faire moins, ou moins vite) suppose de revoir les conditions dans lesquelles un humain peut fonctionner sans s'épuiser. Accepter la sous-optimalité au sens de Hamant, c'est accepter qu'un travail « suffisamment bon » dans des conditions soutenables vaut mieux qu'un travail « optimal » au prix de l'épuisement.

Obsolescence subie. La fin de support de Windows 10 en 2025 et celle de SAP ECC prévue en 2027 illustrent une autre face de l'acceptabilité : l'obsolescence programmée par l'éditeur, subie par l'utilisateur. Quand le calendrier de remplacement est dicté de l'extérieur, l'acceptabilité sociale de la migration dépend de la capacité de l'organisation à l'anticiper plutôt qu'à l'improviser. Une migration anticipée se prépare avec les utilisateurs sur dix-huit mois. Une migration subie se fait dans l'urgence et se paye en frustration.

Indicateurs :

- Taux de satisfaction des usagers en mode dégradé (mesuré, pas supposé)
- Existence d'un canal humain de recours pour chaque service numérique critique (la mention d'un numéro vert dans un coin de page ne compte pas)
- Score RGAA réel (audité, pas auto-déclaré) sur les services destinés aux publics éloignés du numérique

La cohérence des six leviers

Le chapitre 3 comparait le SI optimisé à un champ en monoculture et l'histoire a fourni la démonstration grandeur nature : au milieu du XIXe siècle, l'Irlande dépendait d'une seule variété de pomme de terre, l'Irish Lumper. Un seul pathogène, le mildiou, a suffi à provoquer environ un million de morts et deux millions d'émigrés entre 1845 et 1852. La variété était performante, le rendement à l'hectare était bon, la culture était simple : pour autant la catastrophe est venue de l'absence de diversité.

Un SI qui repose sur un seul cloud, un seul éditeur de bureautique, un seul ERP, un seul outil de sécurité endpoint est dans la même situation. Il fonctionne tant que le pathogène n'arrive pas. Les six leviers de ce chapitre sont les six variétés qui auraient sauvé l'Irlande. Chacun pris seul ne produit qu'une sécurité locale. Ensemble, ils produisent une propriété que la performance unitaire d'aucun levier ne peut atteindre : la robustesse de l'ensemble.

Les couplages rendent cette interdépendance concrète. L'autonomie stratégique sans gouvernance n'est qu'un changement de fournisseur ; sans bien commun, elle mène au survivalisme. La sobriété sans acceptabilité sociale produit des services frugaux que beaucoup n'utilisent pas et qu'on rétablit en pleine version six mois plus tard sous la pression des métiers ; sans low-technisation, elle finit en greenwashing par optimisation. La résilience technique sans low-technisation et sobriété construit une redondance si coûteuse qu'elle devient elle-même une source de fragilité ; sans gouvernance, elle vire à la sophistication aveugle et à la gabegie de ressources. À chaque fois, l'effort sur un levier seul est insuffisant ou contre-productif.

Encadré : Du discours de conviction au discours de risque

Le langage dans lequel on présente la démarche aux directions générales détermine en grande partie son adoption. Les arguments idéologiques (« réduire notre dépendance aux GAFAM », « préserver les compétences humaines », « investir dans le libre », « respecter les limites planétaires ») rencontrent une réception variable selon la sensibilité des décideurs.

Les arguments de continuité opérationnelle, eux, parlent à toutes les directions, parce qu'ils traduisent la même substance dans le langage du risque. Le tableau qui suit donne quelques équivalences que nous utilisons en mission, avec des entrées sur les enjeux de souveraineté et des entrées sur les enjeux environnementaux. Aucune n'est manipulatrice : les deux formulations disent la même chose, dans deux cadres de référence différents.

Formulation idéologique	Formulation robustesse
Réduire notre dépendance à Microsoft	Éviter un CrowdStrike chez nous
Allonger la durée de vie des équipements	Sécuriser nos approvisionnements face aux tensions sur les composants
Préserver les compétences humaines face à l'automatisation	Maintenir notre capacité à fonctionner si l'IA devient indisponible ou trop chère
Migrer vers un cloud souverain	Tenir face aux ruptures géopolitiques d'approvisionnement cloud
Investir dans le libre	Disposer d'un plan B testé pour chaque brique critique
Former en interne plutôt qu'externaliser	Préserver le facteur de bus sur les briques vitales
Réduire notre empreinte carbone IT	Sécuriser nos coûts énergétiques face aux hausses et aux tensions sur le mix
Écoconcevoir nos services	Réduire la complexité qui alourdit les coûts de maintenance et la dette technique
Respecter les limites planétaires	Anticiper les contraintes d'approvisionnement en eau, en énergie et en composants
Réduire la dépendance à l'IA générative	Maîtriser nos coûts d'inférence et éviter l'atrophie des compétences internes

La direction générale n'a pas besoin d'adopter le cadre de pensée de la soutenabilité forte pour autoriser les investissements qui en relèvent. C'est aussi à cela que sert le cadre des six leviers : produire des arbitrages opérationnels qui tiennent dans les deux registres. Le tableau vaut aussi pour le concept central de ce manifeste : la marge du SI se défend

comme un actif qui ne se rachète pas dans l'urgence. Les clients de VMware ont payé son absence en hausses de 300 à 1 050 %.

Aucun des six leviers n'est nouveau, ils existent dans le paysage informatique, parfois depuis longtemps. Ce qui est nouveau, c'est leur articulation dans un cadre cohérent qui les relie à la marge du SI et au filtre du bien commun, et la lecture qui en découle : le SI tout entier comme une économie de la marge.

L'autonomie stratégique sans bien commun mène au survivalisme. La résilience technique sans gouvernance mène à la sophistication aveugle et à la gabegie de ressources. La sobriété sans low-technisation mène au greenwashing par optimisation.

La question suivante sera donc : comment se lancer ? C'est ce que traite le chapitre suivant.

Références

- Perrow, *Normal Accidents*, Princeton University Press, 1984.
- Cigref/INR, *L'approche low-tech au service de la résilience numérique des organisations*, février 2026.
- AFNOR SPEC 2314, *IA frugale*, juin 2024.
- DORA, Règlement (UE) 2022/2554, Résilience opérationnelle numérique du secteur financier.
- Loi n° 2020-105 du 10 février 2020 (AGEC), article 58 sur les achats publics issus du réemploi.

Chapitre 6. Commencer : voir ce qu'on ne voyait pas

Les premières actions de robustesse tiennent dans une séance de travail, un ou deux ateliers, et quelques décisions qu'une DSI peut prendre en quelques semaines, bref une approche atteignable et pragmatique. Ce qui est long, c'est l'ancrage culturel qui vient derrière : plusieurs années. Ce chapitre traite des premiers pas et la trajectoire longue, qui se compte en années, est l'objet du chapitre suivant.

Une organisation ne voit pas ses angles morts. Ses indicateurs ont été fabriqués par le cadre qui a fabriqué le SI : ils mesurent la performance de ce qui existe, pas la solidité de ce qui manque. Ce qui rend visible ce qui manque, c'est l'exposition aux chocs.

Reste à savoir ce qu'on cherche : finalement, le plus marquant est l'état de la marge posée au chapitre 2, sous ses cinq formes : que reste-t-il de notre capacité d'absorption, de nos modes dégradés, de notre diversité, de notre savoir-faire, de notre réversibilité ? Un diagnostic qui ne répond pas à ces cinq questions mesure autre chose que la soutenabilité forte du SI.

Trois gestes suffisent à ouvrir le sujet.

- Exposer le SI à des chocs plausibles, et regarder ce qui tombe.
- Apprendre à concevoir un SI « sous contraintes », qu'elles soient économiques, géopolitiques, environnementales, sociales, réglementaires ou énergétiques pour identifier les premières bonnes pratiques
- Et finalement évaluer de manière réaliste le niveau de soutenabilité de son SI et où sont les marges si elles existent encore.

Aucun des trois ne demande d'outil propriétaire, et c'est heureux : une méthode de robustesse qui dépendrait d'un seul cabinet - même Nuageo - aurait un facteur de bus à un.

Premier geste : exposer le SI à ce qu'il n'a pas prévu

On n'apprend rien d'un système d'information en l'interrogeant avec les indicateurs qui l'ont produit. Il faut le confronter à ce qu'il n'a pas prévu.

En pratique : on réunit dans une salle une dizaine de personnes (DSI, métiers, sécurité, achats, parfois direction générale), et on prépare une série de fluctuations plausibles tirées de l'actualité du secteur.

Chacun confronte le scénario aux usages et processus dont il a la charge. Les discussions qui en sortent sont presque toujours plus structurantes que les conclusions. C'est dans le « quoi, ça nous tomberait dessus aussi ? » que les angles morts apparaissent.

N'importe quelle équipe peut fabriquer ses propres chocs à partir des six mois d'actualité de son secteur.

Ce que l'exercice fait remonter, séance après séance, se ressemble beaucoup d'une organisation à l'autre :

Le redémarrage est plus risqué que la panne. Le 28 avril 2025, en moins de cinq secondes, l'Espagne perd 15 GW, environ 60 % de sa demande électrique à cet instant. Le réseau s'effondre. Pendant plusieurs heures, des dizaines de millions de personnes découvrent ce que veut dire la dépendance à l'électricité, et donc au numérique : terminaux de paiement muets, feux éteints, services publics paralysés. En séance, on projette une coupure de 48 heures sur l'organisation, et la salle discute aussitôt des groupes électrogènes. Presque personne ne pose la question du retour. Or trois jours d'autonomie protègent l'alimentation locale, pas les services cloud. Si internet tombe, le SSO et la MFA tombent avec lui, et l'on se retrouve devant une porte fermée dont la clé est derrière la porte. La séquence de remise en route, avec ses dépendances circulaires, est le moment le plus dangereux du scénario. Personne ne l'a répétée.

La dépendance la plus dangereuse est celle qu'on n'a pas formalisée. En novembre 2025, un changement de configuration chez Cloudflare fait tomber un large pan du web. En atelier, il produit toujours le même silence, suivi de la même question : combien de nos services dépendent d'un fournisseur dont nous ignorons la criticité jusqu'au jour où il tombe ? La cartographie SI répond rarement. Elle n'a jamais été faite pour ça.

Un commun peut être capturé. En 2021, Elastic modifie la licence d'Elasticsearch et de Kibana, deux briques jusque-là sous Apache 2.0. Les organisations qui avaient bâti leur stack de recherche dessus ont eu peu de temps pour choisir entre accepter les nouvelles conditions ou migrer vers le fork OpenSearch. La question généralisée est brutale : que ferions-nous si une brique open source dont nous dépendons changeait de licence demain matin ? Quels projets faudrait-il réécrire, avec quelles compétences ? Le libre protège du verrouillage contractuel. Il ne protège pas de la dépendance qu'on a laissée s'installer sans compétence en face.

On ne sait plus faire ce que la machine fait. En février 2020, le tribunal de La Haye ordonne l'arrêt de SyRI, le dispositif algorithmique de détection de fraude sociale de l'État néerlandais, jugé disproportionné au regard de la vie privée. Transposé à une organisation ordinaire : un système d'IA en production est déclaré non conforme et doit être retiré sous trente jours. Que deviennent les processus qui en dépendent ? Quelles fonctions tournaient avant qu'il existe, et existent-elles encore en interne ? C'est là que la salle se tait. La question porte désormais sur ce qu'on a désappris, plus sur la panne.

Ces quatre constats illustrent les formes de la marge, chacune prise en défaut par un choc différent : le mode dégradé qu'on n'a jamais répété, la diversité de fournisseurs qu'on n'a jamais cartographiée, la réversibilité qu'on croyait acquise parce que le code était ouvert, le savoir-faire qu'on a laissé s'éteindre pendant que l'outil tournait. La cinquième forme, la capacité, traverse les quatre : c'est elle qu'on voit partout comme de la dépense inutile.

Encadré - Ce que produit la séance

Une matrice à deux entrées, croisant la sensibilité de l'organisation à chaque type de choc (forte, moyenne, faible) et son niveau de préparation réel (aucune, partielle, testée). Les chocs à forte sensibilité et préparation nulle sont les urgences. Ceux à forte sensibilité et préparation testée sont des acquis : on les entretient, on ne les reconstruit pas. Ceux à faible sensibilité peuvent attendre, quel que soit l'état de préparation. La case qui décide de tout est celle du milieu : forte sensibilité, préparation partielle. C'est là qu'un investissement modéré produit les gains les plus visibles, et c'est elle qui donne la feuille de route.

Notre instrumentation pour cet atelier s'appelle FluctuIT : 45 chocs documentés, sourcés, répartis en sept catégories, publiés sous licence Creative Commons avec Franck Pramotton. Les premières personnes facilitatrices ont été formées à l'animation pour que la démarche ne dépende pas d'un seul cabinet. C'est, en soi, un acte de robustesse, et c'est aussi la seule cohérence possible quand on écrit un livre qui reproche aux organisations leurs points de défaillance uniques.

Deuxième geste : concevoir sous contrainte, sans échappatoire

Cartographier les fragilités ne dit pas quoi faire. Le deuxième geste répond à ça : prendre un projet SI réel (un nouveau service, une refonte d'architecture, une migration en préparation) et le faire passer sous des contraintes qui s'empilent, sans jamais les lever.

Trois contraintes suffisent, et elles se cumulent. La pénurie physique d'abord : coupures d'électricité, rationnement de matériel, hausse durable du prix de l'énergie, à concevoir comme permanentes et non passagères. La fracture humaine ensuite : perte de compétences clés, marché saturé sur les profils techniques, impossibilité de recruter à court terme. Le sevrage logiciel enfin : une brique SaaS majeure change de licence, un fournisseur cloud devient politiquement indisponible, une dépendance open source est abandonnée.

La valeur de l'exercice tient dans ce qu'on interdit. Les équipes proposent d'abord, invariablement, les mêmes quatre échappatoires, et chacune est bloquée sur place. « On achète un deuxième datacenter » : le budget est gelé. « On recrute » : le marché est saturé, tout le monde cherche les mêmes profils au même moment. « On migre vers un autre cloud » : ce n'est pas préparé, c'est impossible en dix-huit mois. « On fait un PRA » : il existe déjà, et il n'a jamais été testé.

Ces quatre phrases sont le réflexe du métier. Certes, elles fonctionnent toutes dans un monde stable, et il serait injuste de les traiter comme de la paresse : ce sont les réponses qu'on a apprises, celles qui ont marché pendant vingt ans, celles qu'un COMEX comprend sans qu'on ait à les expliquer. Aucune ne survit à une contrainte réelle. Les bloquer d'entrée est la seule façon d'obtenir autre chose qu'un budget rêvé. Ce qui vient ensuite est plus lent, plus pauvre, plus concret. Et réalisable.

Deux tests valident chaque réponse. Le test de non-régression : si le numérique disparaît, l'organisation est-elle dans une situation pire qu'avant ? Le test de continuité impérative : quand le numérique est inévitable, le mode dégradé est-il explicitement conçu, et testé ?

L'exercice se clôt par un récit. Une demi-page au présent, où l'équipe décrit son organisation cinq ans plus tard, après avoir traversé les trois chocs et en être sortie transformée. Ça produit un effet que ni un cahier des charges ni une grille de critères ne produisent : ça oblige à formuler la robustesse comme un état désirable, et même plausible. Tout sauf une liste de parades défensives. Quatre de ces récits sont repris au chapitre suivant.

Nous animons ce geste sous le nom de Robustesse par Conception, en prolongement direct du précédent : le premier part des chocs pour trouver les angles morts, le second part d'un projet pour concevoir sa robustesse dès l'origine. La forme importe moins que la règle : des contraintes qui s'empilent, et des échappatoires fermées.

Troisième geste : évaluer honnêtement

Le troisième geste est le plus modeste : faire un point sur des questions qu'on laisse souvent de côté

Encadré - Huit questions, et ce qu'elles révèlent

Huit questions à poser en comité de direction. En séance, la plupart des comités ne savent répondre précisément à aucune. C'est le résultat de l'exercice, pas son échec. Une organisation qui ignore où elle en est sur ces huit points n'a pas un problème d'investissement. Elle a un problème de visibilité, et c'est par là qu'il faut commencer.

Une question par levier, plus une sur la finalité des usages, plus un test de non-régression.

2. **Finalité des usages / Bien commun.** Quel service numérique avons-nous reformulé, simplifié ou arrêté parce qu'il ne servait pas la mission, ou parce qu'il échouait au triple filtre de la santé commune ?
3. **Autonomie stratégique. Quelle part** du budget des services vitaux dépend d'un fournisseur unique, et combien de ces fournisseurs relèvent d'une juridiction extra-européenne ? Avons-nous déjà exporté l'intégralité des données d'un service critique, et vérifié qu'elles étaient exploitables hors du fournisseur ?
4. **Résilience technique.** Quand a eu lieu le dernier test réel du plan de reprise d'activité, et sur quel périmètre ? Quel est le taux d'occupation réel des infrastructures que nous maîtrisons, et combien de jours-homme non affectés restent disponibles pour absorber un imprévu ?
5. **Gouvernance et compétences.** Combien de personnes peuvent intervenir en urgence sur l'ERP de l'organisation, et ce chiffre a-t-il été mesuré ou estimé ?

6. **Sobriété et frugalité.** Quel pourcentage des services a fait l'objet d'un arbitrage explicite sur sa pertinence AVANT sa conception, et existe-t-il un plafond de consommation cloud par direction métier ?
7. **Low-technisation.** Quel pourcentage des services vitaux dispose d'un mode dégradé non numérique documenté et testé en conditions réelles ?
8. **Acceptabilité sociale.** Quel est le score RGAA audité, pas auto-déclaré, des services destinés aux publics éloignés du numérique ?
9. **Test de non-régression.** Si l'ERP, le CRM ou l'outil de collaboration disparaissait demain matin, l'organisation pourrait-elle maintenir ses fonctions vitales pendant trois mois ?

Quand six réponses sur huit sont vagues, la priorité est le diagnostic, pas l'investissement. Quand la dernière reçoit un « non » sans alternative documentée, on est face à une dépendance critique qui appelle un investissement immédiat. Quand elle reçoit un « oui » sans hésitation, le service mérite peut-être d'être requalifié : est-il aussi vital qu'on le croit ?

Ce que ces huit questions mesurent, au fond, tient en un mot : l'érosion. Aucune ne demande si le SI fonctionne, toutes demandent ce qu'il en resterait sous contrainte : c'est la différence entre un indicateur de performance, qui dit où on en est aujourd'hui, et un indicateur de niveau de marge, qui dit ce qu'on a déjà consommé sans le voir et qui met le système à risque.

Pour autant, ces huit questions sont un point de départ, et rien de plus. Elles ouvrent la discussion, elles ne la tranchent pas. Aller plus loin suppose un instrument plus fin : une grille par levier, cotée, qui produit un profil plutôt qu'un ressenti, et qui se calibre selon la taille de l'organisation : une TPE n'a pas besoin du même outillage qu'un grand compte, mais elle répond aux mêmes questions.

Ce qu'on cherche à obtenir tient en deux ou trois priorités, tenues pendant 18 mois sans les diluer. Le piège classique est de vouloir traiter les six leviers en parallèle. C'est la meilleure façon de n'en traiter aucun.

Les six premiers mois

Les premiers pas se jouent sur un semestre, en parallèle de l'activité courante, plutôt qu'en grand projet de transformation.

Les trois gestes ouvrent la séquence, avec un partage en COMEX. Il en sort trois ou quatre actions immédiates, qui peuvent être d'une ambition modérée, l'idée est de commencer.

Sauvegarder hors-site les services vitaux qui ne le sont pas. Documenter une procédure de continuité non numérique pour les processus critiques. Mesurer le facteur de bus sur les briques sensibles et constituer au moins un binôme là où il n'y en a pas. Tester pour de vrai un scénario de bascule sur un sous-périmètre représentatif.

Ces actions sont des quick wins. Elles ne transforment pas le SI, mais elles ferment les vulnérabilités les plus béantes : celles qui apparaissent presque toujours en première séance. Elles ont une autre vertu, moins évidente, elles produisent des résultats visibles assez vite pour qu'on obtienne le "droit" d'ouvrir les chantiers qui, eux, ne se verront pas avant deux ans. Elles amorcent le changement culturel qu'on évoque depuis le début.

Un dernier cas, parce qu'il est l'inverse exact du sinistre. En 2021, une municipalité suédoise est frappée par un rançongiciel. Les services sociaux continuent de fonctionner, parce que les équipes disposaient de procédures papier connues, héritées du fonctionnement antérieur, même si elles n'étaient plus exercées en routine. L'incident perturbe quatre semaines durant. Il ne devient pas une rupture de service (Holmström et Große, 2025). Aucun héroïsme là-dedans, juste une réserve de non-régression qui n'avait pas été encore démantelée, et qui a servi.

Ce cas, à l'opposé des exemples de chocs, dit ce qui a tenu : cette municipalité ne l'avait pas construit, elle avait simplement omis de le détruire. C'est toute la différence entre la soutenabilité faible, qui optimise ce qui existe, et la soutenabilité forte, qui protège ce qui ne se rachète ni ne se reconstruit dans le temps que laisse un choc.

D'où la question, plus dérangement que tous les chocs qu'on tire au sort. Qu'avons-nous démantelé, ces dix dernières années, qui ressemblait à ces procédures ? La robustesse commence parfois par un inventaire de ce qu'on a encore, avant la liste de ce qu'il faudrait construire.

Ces gestes tiennent en quelques mois mais ce qui vient après se compte en années, et change le métier de celles et ceux qui dirigent une DSI.

Références et outillage

FluctuIT (Nuageo, Pramotton et Marche), jeu de cartes de fluctuations et de leviers, licence Creative Commons, Framagit, 2026. Atelier Robustesse par Conception, même dépôt. Grille d'auto-diagnostic étendue et base d'actions documentées, accès libre, même dépôt.

Holmström & Große, « Not All Heroes Wear Capes: Cyber Resilience of the Social Administration at a Swedish Municipality », *Risk, Hazards & Crisis in Public Policy*, 2025 (doi.org/10.1002/rhc3.70024).

Alemohammad et al., « Self-Consuming Generative Models Go MAD », ICLR, 2024.

Cigref et INR, *L'approche low-tech au service de la résilience numérique des organisations*, février 2026.

ANSSI, *Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique*, 2022.

DORA, Règlement (UE) 2022/2554, articles relatifs aux tests de résilience opérationnelle.

Peccini S., *IRON, Guide complet*, mars 2026 (CC BY-NC-ND 4.0). Approche quantitative voisine (axes X/Y/Z agrégés en score) ; divergences : pas de filtre bien commun, pas de sobriété ni de low-technisation, pas d'autonomie stratégique comme levier systémique.

Chapitre 7. Ce que ça change pour le DSI

Pendant six chapitres, j'ai tenu un registre démonstratif : poser le cadre, montrer les cas, articuler les leviers. Je dois ce dernier chapitre à la personne à qui le livre est adressé : celle qui dirige une DSI aujourd'hui, en France ou en Europe. Je veux le faire moins comme un consultant que comme un collègue. Parce que ce qui se joue est un déplacement de la posture du métier.

De gestionnaire de performance à garant de la marge

Pendant vingt ans, le rôle du DSI s'est défini par une promesse simple (sur le papier du moins, le quotidien est autre chose) : « je gère le coût et la performance ». La promesse a tenu tant que le contexte le voulait bien. Optimiser, rationaliser, externaliser, moderniser, à horizon trois à cinq ans. Quatre verbes qui ont structuré une génération de directions des systèmes d'information, et qui ont produit, dans une majorité de cas, ce qu'on en attendait : des SI plus rapides, plus intégrés, moins chers en apparence, plus capables techniquement (souvent de plus en plus complexes aussi pour y parvenir).

Cette promesse n'est plus suffisante : elle était la bonne réponse à un environnement stable, mais l'environnement n'est plus stable. La nouvelle, celle que ce livre propose de prendre au sérieux, ajoute un cinquième verbe aux quatre : tenir. « Je gère aussi la robustesse, et je le fais sur le temps long. »

Le déplacement n'est pas mineur. Il fait passer la fonction de gestionnaire de performance à garant de la marge du SI.

La marge, sous ses cinq formes (capacité, fonctionnement dégradé, diversité, savoir-faire, réversibilité), devient un objet de pilotage en propre, avec ses indicateurs, ses arbitrages, sa place dans les comités.

Le piège le plus courant, pour un DSI, est la pression mimétique. Les organisations adoptent l'IA « pour ne pas paraître dépassées ». Un chiffre situe la profondeur du phénomène : 57 % des salariés qui utilisent l'IA au travail cachent cet usage et présentent le travail généré comme le leur (étude KPMG/Université de Melbourne, 48 000 personnes interrogées dans 47 pays, novembre 2024 – janvier 2025). Le chiffre mesure une dissimulation individuelle, rien de plus. Je le prends comme un symptôme : quand l'usage se cache, la norme a déjà tranché avant toute décision de la DSI. Le DSI qui résiste à cette pression prend un risque réputationnel interne. Celui qui y cède sans cadre prend un risque opérationnel réel. La posture de robustesse consiste à ne pas confondre l'urgence mimétique avec l'urgence stratégique. C'est un exercice solitaire, jusqu'au jour où la crise donne raison au cadrage.

Ce qu'on appelle ici un DSI « robuste » est un repositionnement de la même personne. Quelqu'un qui continue de gérer la performance, mais qui l'utilise comme une composante parmi d'autres pour viser la soutenabilité forte. Quelqu'un qui pose la question « et si c'était indisponible, qu'est-ce qui tomberait dans mes processus ? » avant de signer un contrat. Quelqu'un qui investit du temps et du budget dans l'entretien d'alternatives qui ne

servent pas toujours au quotidien, mais qui changent la donne en cas de choc, et qui défend en COMEX des arbitrages dont les bénéfices ne se voient pas tant que la volatilité et l'incertitude du monde ne se font pas concrètement sentir.

Et a priori, les crises vont survenir.

Tenir : dix-huit mois, puis trois ans

Les six premiers mois du chapitre précédent ferment les vulnérabilités les plus béantes. Ils ne transforment rien. La suite, si, et c'est là que le métier change, parce que c'est là que les bénéfices cessent d'être visibles.

Ce qu'on reconstitue pendant ces années porte un nom. Daly l'avait posé pour les milieux naturels sous la forme de trois règles, transposables au SI presque sans effort : ne pas consommer les compétences internes plus vite qu'on ne les renouvelle, ne pas retirer un composant sans avoir construit son substitut, ne pas accumuler de dette technique au-delà de la capacité de l'équipe à la résorber. Une feuille de route de robustesse n'est rien d'autre que la mise en calendrier de ces trois règles.

Dix-huit mois : la restructuration architecturale. La deuxième phase travaille sur le fond. Elle ouvre les chantiers structurels que le diagnostic a identifiés : diversification des fournisseurs critiques, plan de réversibilité testé pour les briques verrouillées, programme de réinternalisation progressive des compétences cédées au marché, discipline d'écoconception sur les nouveaux services, plafond de consommation cloud par direction métier. Chacun de ces chantiers reconstitue une marge que l'optimisation avait consommée. C'est la phase la plus coûteuse et celle qui produit le moins de résultats visibles à court terme. Donc celle qu'il faut le plus protéger des arbitrages budgétaires.

Un outil aide à tenir le cap : ce qu'on appelle parfois la comptabilité de l'évité, qui consiste à chiffrer les coûts épargnés par un incident qui n'a pas eu lieu grâce aux investissements consentis. C'est une hypothèse d'arbitrage, pas une preuve : elle ne tient devant une direction financière que chiffrée avec ses données à elle, le coût d'une journée d'arrêt de l'organisation, les barèmes des assureurs cyber, la facture des incidents passés. Un test de bascule trimestriel qui évite une panne majeure représente un ordre de grandeur sans mesure avec son propre coût.

Cette phase suppose un sponsoring exécutif explicite et une protection contre les réallocations de budget saisonnières. Aucun arbitrage trimestriel ne doit pouvoir suspendre ces chantiers sans remontée formelle au plus haut niveau, sans quoi la restructuration dérive en urgences perpétuelles et la transformation n'arrive jamais. C'est une bataille interne, et elle se perd en silence.

Trois ans : la transformation systémique. La troisième phase porte sur la culture et la gouvernance. Elle installe la robustesse comme critère d'arbitrage par défaut sur les choix SI. Elle intègre la santé commune dans les comités de pilotage des projets. Elle acculture les directions métiers à un dialogue régulier avec la DSI sur les questions de continuité, de mode dégradé et de dépendance. Elle ouvre un dialogue avec les directions des risques,

qui sont les partenaires naturels de la démarche dans une logique de continuité d'activité. Le résultat est un SI qui se questionne en permanence sur sa propre soutenabilité, et qui sait répondre.

L'enjeu est de tenir sur plusieurs années, en sachant que les premiers résultats opérationnels arrivent vite (souvent dans les six premiers mois) et que les transformations culturelles arrivent lentement, parce qu'elles passent par les têtes et pas par les budgets.

Sobriété, robustesse, autonomie : la convergence

Le repositionnement n'a de sens que parce qu'il fait converger trois conversations que les décennies 2010 et 2020 ont menées séparément : l'efficacité chez les équipes IT, la continuité d'activité chez les équipes risques, la souveraineté dans le débat politique. Chacune tenait un bout du sujet, mais aucune ne sera reprise telle quelle dans la démarche.

L'efficacité devient sobriété le jour où la question du besoin passe avant celle des moyens : faut-il le faire, avant comment faire au minimum. Le PRA, lui, garde sa fonction, revenir après le choc, mais il entre dans un cadre plus large qui travaille aussi le pendant et l'amont : la robustesse. Quant à la souveraineté, elle se mue en autonomie stratégique quand on cesse de vouloir « maîtriser l'ensemble de la chaîne de valeur : matières premières, composants, infrastructures, logiciels, données, normes » pour « chercher à réaliser sa mission sans dépendance critique non maîtrisée envers un fournisseur, une juridiction ou une technologie unique ». Trois déplacements, une même recherche : la soutenabilité forte.

La sobriété renforce la robustesse, on l'a vu au chapitre 3 : elle réduit la surface de dépendance, donc le périmètre à défendre. Et elle la borne : une robustesse sans sobriété multiplie les systèmes de secours et les couches de sécurité jusqu'à déborder les limites planétaires.

La robustesse traduit la sobriété en argument stratégique : c'est la stratégie discursive du chapitre 5, celle du tableau des équivalences entre discours de conviction et discours de risque. Le langage du risque opérationnel parle aux DSI et aux directions générales que la responsabilité environnementale n'atteint pas toujours. La scène se rejoue à chaque COMEX, à peine caricaturée : le dossier ouvert sur « réduire notre empreinte IT » fait plonger les regards dans les téléphones ; le même dossier repris par « éviter un CrowdStrike chez nous » fait lever la tête du directeur financier, qui demande ce que coûterait une journée d'arrêt. C'est un cheval de Troie dans un sens : la même substance, dans un cadre où elle est audible.

**Sobriété perçue
comme...**

**Robustesse perçue
comme...**

Réduction	Opportunité
Frustration	Enthousiasme
Protection (défensive)	Adaptabilité (offensive)
Contrainte subie	Bien commun choisi

Le passage de la première colonne à la seconde relève d'un changement du cadre de pensée : la robustesse rend la sobriété désirable en montrant ce qu'elle produit. D'où la séquence décrite au chapitre 5 : le risque d'abord, la conviction ensuite.

Finalement, reste l'autonomie, à la fois levier et objectif. Un levier d'abord, parce qu'elle rend la robustesse pratiquement possible : sans dépendances cartographiées, sans alternative crédible en face, on ne peut pas être robuste car dépendant de technologies, d'acteurs, de contrats... Un objectif ensuite, parce qu'elle vise à redonner au DSI la cinquième forme de marge, celle de la décision : pouvoir changer de fournisseur, revenir en arrière, dire non, vis-à-vis de tous les acteurs externes.

Au final, la convergence ne met pas les trois au même rang. Dans le cadre de ce livre, la sobriété et l'autonomie stratégique restent des leviers de la robustesse : la sobriété allège ce qu'il y aura à défendre ; l'autonomie stratégique redonne la main pour le défendre, jusque dans les contrats. La robustesse, elle, est le chemin, et la soutenabilité forte la direction commune.

Les appuis du DSI

Le DSI n'est pas tout seul dans ce repositionnement. Deux types d'appuis sont à sa disposition, et il les sous-utilise.

Le premier est réglementaire. DORA (règlement UE 2022/2554) impose au secteur financier des tests de résilience opérationnelle réels : un test exécuté, pas un audit documentaire. C'est l'inscription dans la loi du fait qu'un PRA jamais testé n'est qu'un document. NIS2 élargit le périmètre à des secteurs entiers et met les directions générales en première ligne. Le Cyber Resilience Act, le Data Act, la directive CER, l'AI Act et la CSRD complètent un corpus qui converge vers une exigence commune : prouver, pas déclarer. Le calendrier continue de se durcir : les pouvoirs d'exécution de l'AI Act sur les modèles à usage général s'appliquent au 2 août 2026. Et la Commission a mis sur la table, en juin 2026, un Cloud and AI Development Act qui définit des niveaux de souveraineté pour l'achat public de cloud, les plus exigeants supposant des fournisseurs détenus et

contrôlés depuis l'Union. À ce stade, c'est une proposition : rien n'est voté. La direction, elle, est nette : l'autonomie stratégique entre dans le droit. Le mouvement est dans le bon sens. Il est lent. La conformité réglementaire et la robustesse ne se recouvrent pas exactement, mais le mouvement change ce qu'un DSI peut défendre en COMEX : « on fait ça parce qu'il faut prouver qu'on tient ».

Le second est dans les achats. L'article 58 de la loi AGECE impose que 20 % des achats publics de matériel informatique soient issus du réemploi ou de la réutilisation (décret d'application de 2024). Le Code de la commande publique impose l'allotissement, qui maintient de la diversité fournisseurs dans les marchés. Et le CCAG-TIC prévoit depuis 2021 une clause de réversibilité et de transférabilité, avec un plan de réversibilité annexé au contrat : la sortie se négocie avant signature.

Un mot enfin sur l'achat de logiciel libre, parce qu'il change les réflexes d'achat et de consommation classique d'informatique. La brique logicielle est gratuite ; sa solidité, elle, repose sur la communauté qui la maintient. Une organisation qui en dépend sans jamais y contribuer, en argent, en temps ou en code, se met en position de parasite : elle consomme la maintenance des autres. L'affaire XZ Utils, détaillée au chapitre 5, a rappelé ce que ça coûte quand la communauté s'épuise. Contribuer aux communs dont on dépend relève du même geste que la clause de réversibilité : on sécurise sa chaîne d'approvisionnement logicielle. Et savoir contribuer demande une évolution dans sa culture et son organisation par rapport à un achat classique (avec par exemple, la mise en place d'un Open Source Program Office (OSPO)).

Encadré - La permaentreprise comme exigence de cohérence

Le concept de permaentreprise, formalisé notamment par Sylvain Breuzard et plusieurs entreprises à mission, applique au monde organisationnel les trois principes de la permaculture : prendre soin de la Terre, prendre soin des humains, partager équitablement les ressources et les surplus. Nuageo, fondée en 2014 et reconnue société à mission, s'inscrit dans cette filiation. On ne peut pas tenir un discours sur la robustesse d'autrui si on ne tient pas, dans son propre fonctionnement, une cohérence entre ce qu'on dit et ce qu'on fait. Cette exigence est une condition de crédibilité du propos. Elle est aussi, à l'usage, beaucoup plus exigeante qu'une charte affichée dans un hall d'entrée.

Une dernière chose, qui relève autant du management que de la technique. Ne pas fixer d'objectif explicite, c'est laisser la porte ouverte à des attentes infinies. Je l'ai vu dans de grands cabinets, et je me suis surpris à le reproduire parfois. Un DSI qui ne définit pas explicitement le niveau de robustesse cible (quel mode dégradé est acceptable, pendant combien de temps, pour quels services) installe une logique du toujours plus, où chaque crise révèle une insuffisance qui n'avait jamais été bornée. Google l'a formalisé dans ses pratiques SRE avec ce qu'il appelle l'*error budget* : un volume d'indisponibilité admis d'avance, sur une période donnée, pour un service donné. Tant qu'il n'est pas consommé, les équipes peuvent prendre des risques pour accélérer les évolutions. Dès qu'il approche

de la limite, le curseur bascule sur la fiabilité. C'est un outil de négociation explicite entre vitesse d'évolution et solidité/durabilité. Il dit au passage ce que « préserver la marge » signifie : une marge se dépense pendant le choc et se reconstitue après. La préserver, c'est piloter ce cycle, pas sanctuariser un stock qu'on n'ose plus toucher. La robustesse a besoin du même cadre. Accepter explicitement un niveau de sous-optimalité, c'est fixer le point où l'optimisation s'arrête. Sans ce niveau écrit et partagé, chaque incident relance la demande, plus de redondance, plus de contrôles, plus de budget, et aucun état n'est jamais jugé suffisant.

Quatre cartes postales d'un numérique plus robuste

Quatre images, pour dire où mène la trajectoire. Quatre organisations qui l'ont tenue, quelque part en 2030, et chez qui la démarche se voit dans le quotidien plutôt que dans les indicateurs. Des récits rédigés en ateliers Robustesse par Conception avec des équipes réelles, lissés et consolidés ici - pas des projections technologiques. Chacun montre une marge qu'on a refusé de consommer.

L'opérateur ferroviaire. Dans le 7h12 entre Lyon et Paris, une voyageuse compose son trajet de retour. Une région cloud vient de lâcher en Europe centrale. L'application n'a pas plié : elle a basculé en mode local, sur l'infrastructure de secours hébergée à Saint-Étienne, comme prévu. Les écrans de quai affichent des horaires à jour. L'accessibilité reste réelle pour les personnes en situation de handicap. Le contrôleur valide les billets sur un terminal hors-ligne synchronisé toutes les heures. Un test de bascule trimestriel, appelé en interne « exercice voyageurs » parce qu'il se déroule en conditions réelles sur une ligne régionale, avec de vrais passagers, a institutionnalisé la discipline depuis quatre ans. La non-régression est entrée dans la doctrine d'exploitation : pas de fonctionnalité nouvelle sans procédure manuelle de repli documentée et testée. Le réseau roule. Le service public reste au rendez-vous du pays. Personne, dans le wagon, ne sait qu'une crise vient d'avoir lieu. C'est exactement le résultat recherché.

L'hôpital public régional. Le mode été est activé. Les serveurs principaux basculent sur la zone secondaire, gérée en direct par l'équipe IT du CHU. La messagerie interne, hébergée sur une instance Mattermost autonome, continue de tourner sans interruption. Les classeurs papier des protocoles de soins, mis à jour tous les trimestres et entretenus comme un livrable de continuité à part entière, sont accessibles dans chaque service. Les soignants connaissent les procédures parce qu'ils s'exercent deux fois par an (un exercice « tout numérique coupé » et un exercice de bascule partielle) et que les nouvelles recrues sont formées au mode dégradé en même temps qu'au mode nominal. La doctrine s'est construite à partir du retour d'expérience du CHU de Rouen après la cyberattaque de 2019 et des kits guichet déployés au Centre Hospitalier de Cannes après celle de 2024, consolidés puis partagés via l'ANSSI (le détail des deux cas est au chapitre 5). Pas d'improvisation. Les soins continuent. Le jour où une équipe médicale demande à rebasculer en mode normal parce que « le papier est plus fluide », la DSI sait que le travail de fond a porté.

La banque mutualiste. Un compte client s'ouvre en agence. Le conseiller utilise une application qui fonctionne en local, synchronisée avec le SI central toutes les vingt minutes. La session ne dépend pas d'une connectivité permanente. L'application est légère, accessible, et a été conçue avec la communauté des conseillers terrain plutôt que par un cabinet externe. Principe de co-conception repris du modèle de la MAIF. La banque participe, depuis 2026, à un commun mutualisé entre quatre établissements coopératifs sur les briques d'infrastructure non concurrentielles : annuaire, signature électronique, archivage légal, socle d'authentification. Les compétences sont partagées entre les quatre, les coûts aussi, et aucun des quatre n'est dépendant des trois autres pour continuer à opérer. Les équipes gardent la main sur ce qui compte : la relation client. Le reste est fabriqué en commun, entretenu en commun, et reste en commun.

La ville moyenne. Au guichet de l'état civil, une habitante vient déclarer une naissance. L'agente ouvre un portail simplifié qui tourne sur un poste reconditionné sous OS allégé. Le portail fonctionne en mode 2G dégradé pour les démarches qui n'exigent pas de pièce jointe lourde. Quand tout tombe, ce qui est arrivé deux fois en trois ans (une coupure réseau, une attaque sur le datacenter de la métropole), le kit guichet papier prend le relais sur les actes urgents et la remontée vers l'état civil se fait par téléphone. Le kit a été monté en 2026 sur le modèle des procédures de France Services : dossiers pré-imprimés, registres numérotés, tampons dateurs, grille de contrôle, reçus. La continuité du service public dépend de la formation des agents, qui n'ont jamais désappris à faire autrement, et du fait qu'une personne au moins dans chaque service sait traiter un acte à la main. Pas de la disponibilité du datacenter de la métropole.

Ces récits sont des images vers lesquelles plusieurs organisations marchent déjà, pas des prophéties. Ils rendent visible ce qu'on essaie de construire : un numérique qui tient, qui sert, et qui n'oblige personne à improviser son métier le matin d'une panne.

Questions non résolues

Plusieurs questions restent ouvertes au moment où ce manifeste est finalisé. À défaut de les traiter, je vais les nommer.

L'autonomie stratégique reste-t-elle un levier de la robustesse, comme nous l'avons traitée dans le cadre des six leviers, ou devient-elle un pilier à part entière, au même rang que la robustesse elle-même ? Plusieurs retours terrain me poussent vers la deuxième option : c'est souvent un point d'entrée dans la robustesse, un point d'entrée opérationnel, pragmatique, comme peut l'être la sobriété dans des cas plus rares. L'articulation théorique reste à clarifier.

Comment opérationnaliser l'articulation entre le filtre du bien commun et les méthodes de scoring de risques numériques qui se mettent en place dans les directions des risques ? Le bien commun appelle un jugement. Les méthodes de scoring appellent une métrique. Les deux registres ne se réduisent pas l'un à l'autre, et personne n'a encore proposé de méthode satisfaisante pour les faire dialoguer.

Comment opérer le passage de consommateur à contributeur de communs à l'échelle d'une DSI moyenne, sans budget dédié et sans tradition de contribution amont ? Les outils existent. La culture interne, elle, est rarement prête.

Comment articuler soutenabilité faible et soutenabilité forte dans les démarches existantes ? Les démarches de numérique responsable installées depuis dix ans travaillent dans le cadre de la soutenabilité faible, par optimisation ; le passage à la soutenabilité forte suppose de questionner ce cadre sans casser la dynamique. À quel rythme, avec quelles équipes, sous quelles conditions politiques cette bascule est-elle possible sans perdre ce qui a été construit ? La question n'a pas de réponse générique : elle se joue organisation par organisation.

La démarche serait-elle plus simple à adopter dans le service public que dans l'entreprise ? Mon expérience penche du côté des entreprises, et c'est peut-être un biais de ce livre. Pour autant, une collectivité valide le filtre du bien commun par nature : sa mission est de servir tout le monde, y compris les plus éloignés du numérique. Par exemple, la stratégie de numérique responsable de Villejuif, intitulée « Le numérique, c'est pas automatique », en donne un indice : le besoin questionné avant l'outil (son intitulé le dit), des logiciels libres jusque dans les écoles, un accompagnement humain de proximité pour les démarches en ligne. Plusieurs des limites du NR pointées au chapitre 1 y sont traitées de front. Un cas ne fait pas une règle ; mais il est intéressant de le noter.

Une dernière question, la plus inconfortable, m'est adressée autant qu'au lecteur. Tant que le client est un DSI et que la finalité est la continuité du SI, ce livre reste un discours de l'intérieur : il consolide le système qu'il critique. Je ne prétends pas résoudre cette contradiction, je préfère la nommer. On ne descend pas d'un train en marche, et je ne crois pas qu'on aide qui que ce soit en sautant. Une robustesse intègre ralentit le wagon, allège ce qu'il transporte, et garde une porte ouverte. Léa, au début de ce livre, n'avait pas besoin qu'on supprime le train. Elle avait besoin qu'il tienne.

Ces questions n'ont pas de réponse arrêtée. Elles dessinent les chantiers de ce qui suivra ce livre.

La trajectoire

On n'évite pas les chocs. On ne les encaisse pas non plus, au sens où la résilience le suppose. On apprend à fonctionner dans un monde où les chocs sont devenus la norme. C'est ce que la robustesse veut dire, en quelques mots.

Cette démarche suppose un changement de regard : accepter une part de sous-optimalité (des marges, du jeu, des redondances) parce que c'est elle qui absorbe les chocs. C'est, formulé autrement, ce que la soutenabilité forte demande : garder intacte la marge qui ne se rachète pas dans l'urgence, même quand rien ne l'exige encore.

Elle suppose aussi un changement de finalité. La robustesse n'a de sens que si elle sert quelque chose qui vaut la peine d'être protégé. Un système d'information qui dégrade la santé humaine, sociale ou des milieux naturels mérite d'être transformé, pas d'être rendu

robuste. Et cette transformation dépasse le sujet informatique : elle touche la raison d'être de l'organisation qui l'héberge.

Cette posture est contre-culturelle dans un milieu qui valorise la disponibilité maximale et le 100 % de tout. Elle est contre-culturelle, et elle est nécessaire.

Pour autant, rien de tout cela ne se joue dans un plan quinquennal. Le DSI qui se reconnaîtra dans ce livre est celui qui, lundi matin, posera à son équipe une nouvelle question : celle qu'il ne posait pas vendredi. Une seule. Puis une autre la semaine suivante. Pas besoin d'avoir tout compris ni tout mis en œuvre d'un coup. Le mouvement fait le reste.

La robustesse du SI, c'est d'abord une trajectoire à tenir.

Références

Règlement (UE) 2022/2554 (DORA), Résilience opérationnelle numérique du secteur financier.

Directive (UE) 2022/2555 (NIS2), Niveau commun élevé de cybersécurité dans l'Union.

Loi n° 2020-105 du 10 février 2020 (AGEC), article 58 sur les achats publics issus du réemploi.

Daly, *Beyond Growth*, Beacon Press, 1996 (les trois règles, transposées au SI).

Cigref/INR, *L'approche low-tech au service de la résilience numérique des organisations*, février 2026.

OCTO Technology, *Repenser la souveraineté numérique*, 2025.

Breuzard, *La permaentreprise : un modèle viable*, Eyrolles, 2022.

Beyer et al. (Google), *Site Reliability Engineering*, O'Reilly, 2016.

Conclusion

Pendant que ce manifeste s'écrivait, le réel n'a pas cessé de fournir des arguments. Daejeon a brûlé. Cloudflare est tombé. La péninsule ibérique a tenu plusieurs heures sans électricité. À chaque événement, je me suis demandé s'il fallait rouvrir un chapitre. À chaque fois, la réponse a été non : le mécanisme y était déjà, seul le nom de l'acteur changeait. Un livre sur les fluctuations s'expose à être rattrapé par elles, et c'est exactement ce qui s'est produit. Si vous lisez ces pages dans cinq ans, d'autres noms auront remplacé ceux-là. La liste des cas vieillira vite. La grille de lecture, je crois, tiendra.

Ce livre s'interrompt plus qu'il ne se termine. Les six questions laissées ouvertes au chapitre 7 sont les chantiers de la suite, pas des précautions d'auteur. La place de l'autonomie stratégique : levier ou pilier ? Le dialogue entre le jugement du bien commun et les métriques des directions des risques. Le passage de consommateur à contributeur de communs. L'articulation entre les démarches de numérique responsable installées depuis dix ans et la soutenabilité forte qui les déborde. La part du service public, peut-être mieux disposé que l'entreprise à accueillir la démarche. Et la position du livre lui-même : on ne descend pas du train en marche. Aucune ne se résoudra dans un bureau d'études. Elles se résoudront en mission, en atelier, dans les allers-retours entre ce cadre et les organisations qui s'en saisiront, le contesteront, le tordront pour le faire entrer dans leur réalité. Le cadre sortira transformé de l'exercice. Tant mieux : un cadre qui ne bouge pas est un cadre que personne n'utilise.

C'est pour cette raison que les outils présentés dans ce manifeste sont des communs. La démarche ne nous appartient déjà plus, et c'est voulu : une méthode de robustesse qui dépendrait d'un seul cabinet aurait, encore une fois, un facteur de bus à un.

Corinne Morel Darleux appelle ça « archipéliser » les résistances : des îlots qui agissent chacun à leur façon, reliés sans être alignés, chacun à son poste d'un plan plus vaste. C'est une définition de la robustesse qui s'ignore : l'hétérogénéité, les redondances, les erreurs et les incohérences locales d'un archipel sont ce qui empêche un choc de tout emporter, là où le continent optimisé le propage d'un seul tenant. Son livre porte un titre en forme d'alternative : *Plutôt couler en beauté que flotter sans grâce*. Ce manifeste parie sur une troisième voie : tenir la mer - « *parce qu'on est heureux en mer, et peut-être aussi pour sauver nos âmes* ».

Il faut le dire sans détour : la soutenabilité est une démarche de société, et elle déborde de toutes parts le périmètre de ce livre, celui des SI comme celui des entreprises. Une partie des actions proposées ici jouent à la marge, d'autres sont hors de portée d'une DSI seule. Ce constat ne fait que préciser l'ambition : éveiller, montrer que c'est possible, multiplier les îlots de résistance face à la performance insoutenable.

Pour résumer la thèse de ce manifeste : le numérique responsable, tel qu'il se pratique, mesure, optimise, compense, dans un cadre qu'il ne remet pas en cause et comme si toute perte pouvait être remplacée : c'est de la soutenabilité faible. Or le monde qui vient est incertain, traversé de crises multiples et imprévisibles, et une logique d'optimisation n'est pas taillée pour y faire face. C'est la soutenabilité forte qu'il faut viser : des SI qui maintiennent leurs fonctions essentielles à travers les chocs, au service de la santé commune, celle des personnes, de la société et des milieux naturels. Le chemin pour y parvenir : une démarche de robustesse. Elle garde intacte la marge qui ne se rachète pas dans l'urgence, sous ses cinq formes : la capacité, le fonctionnement dégradé, la diversité, le savoir-faire, la réversibilité.

Reste la question du moral. On pourrait fermer ce livre avec le sentiment d'une liste de menaces, et ce serait un contresens. La robustesse, au sens où Olivier Hamant l'emploie, est joyeuse : elle n'attend pas la catastrophe, elle cesse d'en avoir peur. Une équipe qui a testé son mode dégradé dort mieux qu'une équipe qui empile les assurances sans jamais les ouvrir. Un DSI qui sait ce qu'il accepterait de perdre négocie autrement avec ses fournisseurs, avec sa direction, avec lui-même. C'est peut-être naïf, mais je tiens cette sérénité-là pour le premier bénéfice de la démarche : avant les économies, avant la conformité, avant même la continuité. On travaille mieux quand on a regardé la panne en face.

Et puis il y a Léa, sur son quai de Marseille. Son train est parti à l'heure parce que des gens qu'elle ne connaîtra jamais ont défendu des budgets sans gloire, entretenu des compétences qui ne servaient presque jamais, testé des bascules dont aucun communiqué n'a parlé. Quand la robustesse fonctionne, il ne se passe rien. Pas de récit, pas de héros. Un train qui part, un guichet qui reste ouvert. C'est une drôle de promesse pour finir un livre : si nous réussissons, personne ne le remarquera. Je signe pour ça.

Quelque part en 2030. Au guichet de l'état civil d'une ville moyenne, une habitante vient déclarer une naissance. L'agente ouvre un portail simplifié qui tourne sur un poste reconditionné, en mode 2G dégradé. Si tout tombe (ce qui est arrivé deux fois en trois ans), le kit guichet papier prend le relais. La continuité du service public dépend de la formation des agents et du fait qu'ils n'ont jamais désappris à faire autrement, pas du datacenter de la métropole.

C'était trop long ? Un résumé en une page.

Un SI ultra-optimisé est un SI ultra-fragile. Dans un monde stable, optimiser était rationnel. Dans un monde fluctuant, ce qui est optimisé pour un état particulier casse dès qu'on en sort.

Le numérique responsable, tel qu'il se pratique, mesure et optimise l'empreinte : le premier tiers du travail. Les choix de numérisation et la solidité de ce qu'on construit restent hors champ.

Optimiser dans un cadre qu'on ne questionne pas, c'est la soutenabilité faible. Elle consomme en silence la marge qui ne se rachète pas dans l'urgence, sous cinq formes : capacité, fonctionnement dégradé, diversité, savoir-faire, réversibilité. L'optimisation prend cette marge pour du gaspillage ; le choc la révèle pour ce qu'elle est : l'actif qui fait tenir tout le reste.

La robustesse maintient la fonction pendant et en amont du choc. La résilience attend de tomber pour se relever. La robustesse est le chemin vers la soutenabilité forte.

Elle se paie en sous-optimalité assumée : un taux d'occupation de 70 %, des redondances, du temps non alloué. Ce que la performance compte comme une dépense, la soutenabilité l'inscrit comme un actif. Les 30 % restants font partie du cahier des charges.

On ne rend pas tout robuste. Le filtre du bien commun - santé humaine, santé sociale, santé des milieux - décide de ce qui mérite l'effort. Le reste se simplifie, se réduit ou s'arrête.

Sobriété d'abord : questionner le besoin avant d'optimiser la réponse. Un service qui n'existe pas n'exige aucune marge : pas de mode dégradé à concevoir, pas de fournisseur dont dépendre, pas de compétence à entretenir.

Le test qui change tout : si cet outil disparaissait demain matin, saurait-on encore rendre le service ? Tant que la réponse est oui, on protège cette capacité. Quand elle devient non, on conçoit le mode dégradé, et on le teste.

Quand la robustesse fonctionne, il ne se passe rien. Un train qui part, un guichet qui reste ouvert. Si nous réussissons, personne ne le remarquera.

=> Remarque à intégrer :

On a conscience que la démarche de soutenabilité devrait être une démarche sociétale qui dépasse le cadre des SI et celui des entreprises.

L'expérience que j'aie est plus proche des entreprises que celle des organisations publiques et collectivité, peut-être que la démarche de robustesse serait plus simple à adoptée là bas, simplement du fait de la validation du filtre bien commun inhérente aux missions de service public. L'exemple de la démarche NR de villejuif, un contre exemple criant aux limites du NR identifiées dans le ce livre, en est une illustration parfaite.

On sait qu'on a des actions à la marge, et que d'autres sont hors de portées de la DSI. Le but est d'éveiller, de montrer que c'est possible, de créer ilots de résistance face à la performance insoutenable.

Une envie de cette démarche serait d'éviter les problème ou les conséquences de chaque problemes. Parfois c'est normal de tomber. On ne veut pas faire de tout le monde des champions du monde de ski hors piste. Tant que les conséquences de la chuttes sont acceptable, il suffit de se relever et de repartir. Si la chute mets en danger une organisation, il faut des parades. = loi des incident (itil ?)

Question ouverte : faire plus de comparaison que de chiffre ou compraison et chiffres pour que ça marque (ex 11% de la conso d'électricité, = consommation d'une ville etc)

•

Ça tient.

Brèves du futur - huit lieux, une journée de 2030

Gare de Marseille, Le TGV 6h54 pour Paris partira à l'heure, avec Léa dedans. Ca vous le savez. Mais la journée de mardi ne s'arrête pas là. *CE mardi 17 septembre 2030, Une région cloud lâche en Europe centrale, un effacement électrique est programmé en Normandie, un orage de grêle traverse le Sud-Ouest, un éditeur de logiciel dépose le bilan, un préfet limite l'eau d'un datacenter, une licence américaine est suspendue du jour au lendemain, une grève interprofessionnelle immobilise les transports. Rien d'exceptionnel : c'est un mardi de 2030 dans un monde en polycrise. Huit lieux, huit heures de la même journée, voici quelques exemples de comment cette situation a été vécue par les personnes sur place :*

8h15 - Centre hospitalier de Trévières

L'effacement électrique commence à 8h30. Deux heures, comme prévu, comme annoncé la veille par le gestionnaire de réseau. Dehors, il fait déjà 27 degrés, canicule de septembre, la troisième de l'année. Nadia, cadre de santé aux urgences, termine son café debout devant le tableau d'affichage. Elle n'est pas inquiète. Elle vérifie.

À 8h30 précises, les serveurs cloud "s'endorment" et les équipements locaux prennent le relais. Les dossiers patients passent en mode texte : diagnostic, traitements, allergies, le noyau clinique, rien d'autre. Les écrans des salles d'attente s'éteignent, remplacés par un tableau blanc et un feutre. Un interne de première année saisit ses observations sans ralentir. Pour lui, c'est un mardi normal, il n'a jamais connu d'hôpital qui panique quand l'électricité se retire.

Nadia, si. Elle se souvient de la réunion de 2026 où elle avait demandé qu'on maintienne les prescriptions manuscrites en doublon pour les patients critiques. « Le papier, sérieusement ? » avait souri le consultant venu présenter le tout-numérique. Elle se souvient d'avoir insisté pour que chaque service garde une check-list de continuité plastifiée au mur, pour que l'exercice papier-crayon reste trimestriel même quand plus personne n'y croyait, pour que les nouveaux internes apprennent à travailler débranché avant d'apprendre les raccourcis clavier. On l'avait trouvée rétrograde. Le mot exact, dans un couloir, avait été « folklorique ».

À 9h10, une arrivée d'une patiente en urgence vitale. Le tri se fait en quatre-vingt-dix secondes, le bloc est prévenu par le téléphone filaire interne, la prescription part sur papier pendant que le mode texte enregistre en parallèle. À 10h30, l'électricité revient, les systèmes se resynchronisent, les classeurs retournent sur leurs étagères.

Dans le vestiaire, l'interne lui demande pourquoi on garde tout ce papier alors que « ça marche, en fait, leur truc de bascule ». Nadia range sa blouse. Ça marche parce qu'on a gardé le papier, dit-elle. Le jour où l'outil tombe pour de bon, le savoir faire sans deviendra juste le savoir faire.

9h02 - Lycée Rosa-Bonheur

Ce matin-là, les élèves de terminale composent - Quatre heures d'évaluation commune, pour bien commencer l'année. À 9h02, Inès retourne son sujet et commence à lire.

Elle ignore, comme tout le monde dans la salle, que pendant la nuit, la plateforme éducative d'un grand éditeur américain a été suspendue pour toute l'Europe. Un différend entre gouvernements, une décision de justice de l'autre côté de l'Atlantique, et au final un accès global coupé à distance. Des millions de comptes scolaires étaient inaccessibles au lever du jour, même les serveurs eux fonctionnent parfaitement. Ici c'est l'extraterritorialité du droit Américain qui a débranché la prise.

Personne ne l'a remarqué parmi les lycéens, justement parce que les sujets étaient dupliqués sur les serveurs de l'académie, chiffrés, répliqués dans deux rectorats. Personne ne l'a remarqué aussi, parce que le cahier de textes, les notes et les copies existent sur l'espace numérique de la région, opéré par un groupement d'intérêt public, sur des briques libres que trente académies maintiennent ensemble. Personne ne l'a remarqué encore, parce que les convocations étaient imprimées et que l'évaluation se fait sur papier, comme toujours : un examen doit pouvoir se tenir dans un gymnase sans réseau, à égalité pour toutes et tous. Quant aux postes de la salle informatique, reconditionnés, ils tournent sur des systèmes Linux que le lycée maîtrise : aucune mise à jour venue d'ailleurs ne peut les éteindre.

Dans la salle des professeurs, la proviseure adjointe lit la dépêche sur son téléphone. Ailleurs en Europe, des établissements ferment pour la journée, des examens sont reportés, des parents cherchent des solutions. Elle repense aux années de débats : les enseignants qui trouvaient l'outil américain « quand même plus pratique », les réunions interminables sur le groupement public... Tout cela avait semblé lent, austère, un peu têtue.

À 13h02, Inès rend sa copie. Elle ne saura jamais qu'à mille kilomètres, des élèves de son âge n'ont pas composé ce matin. L'égalité devant l'examen a tenu à des choix d'architecture faits avant qu'elle n'entre au collège.

11h40 - Mairie de Coudray-les-Eaux

Après les deux dernières canicules, la sécheresse persistante : l'arrêté préfectoral, tombé lundi, rationne l'eau du datacenter régional à 30 % de son quota. Depuis ce matin, le portail citoyen tourne en mode léger, pages en texte, sans images, soixante kilo-octets chacune. Le réseau est passé en 2G sur une partie du territoire. À l'accueil de la mairie, Théo, vingt-quatre ans, agent d'état-civil depuis six mois, délivre un acte de naissance à une dame qui n'a pas de smartphone. Un tampon, un sourire, le tour est joué.

Vers 11h40, un homme d'un certain âge dépose un dossier d'urbanisme. Il regarde l'écran de Théo, terminal noir, écriture blanche, et sourit. « Le mode 60 Ko... Il marche toujours, alors. » Théo lève la tête. L'homme se présente : Gilbert, l'ancien responsable informatique du syndicat intercommunal, à la retraite depuis trois ans.

« C'est vous qui avez mis en place le "mode léger" ? »

— C'est nous, oui. On l'a écrit dans le cahier des charges en 2026 : toute page du portail doit rester utilisable sur un téléphone de dix ans d'âge et un réseau 3G. Le prestataire avait ri à l'époque mais on a été au bout, vous savez pourquoi ?

— La sécheresse ?

— Pas seulement. Regardez la dame de tout à l'heure. Le portail le plus léger du monde ne lui sert à rien. Alors on a fait voter une règle en conseil : jamais cent pour cent dématérialisé. Chaque démarche garde son alternative non numérique. Le mode léger et le guichet, c'est le même combat : un service qui demande peu : Peu d'eau, peu de réseau, peu d'équipement, peu d'aisance numérique. Ce qui demande peu tient longtemps, et tient pour tout le monde.
»

Théo repense à sa formation : une matinée en ligne, une matinée tout au papier. Il avait trouvé ça étrange, ce soin mis à travailler "déconnecté". À midi, il ferme le guichet du matin. Quatorze demande traitée, pour quatorze personnes reçues, dont cinq sans écran, deux sans français courant, une sans domicile. Le datacenter, lui, a économisé son eau. Personne n'a eu à choisir entre les deux.

20h15 - Régie des eaux du Val-de-Serre

Au siège de la régie des eaux du Val-de-Serre, il n'y a que 3 présentes sur 7. Deux se sont déclaré en grève, deux bloqués à quarante kilomètres par la grève interprofessionnelle. Personne n'a paniqué en l'apprenant. Le tableau de service de ce mardi ressemble à un exercice qu'on a déjà fait.

À 20h15, l'alarme sonne : défaut sur la pompe de reprise de la station des Crêtes, pression en baisse sur le réseau haut. Marina est d'astreinte. Les Crêtes ne sont pas son secteur, et ça n'a aucune importance : à la régie, personne ne travaille à temps plein sur son périmètre. Quatre jours sur cinq chez soi, le cinquième chez les autres. La procédure de bascule, elle l'a jouée en double avec Karim au printemps, une fois en conditions réelles, une fois tout au manuel. Trente-cinq minutes plus tard, la pompe de secours a pris le relais, la pression remonte, le réservoir de tête n'a jamais entamé sa réserve.

La grève s'est réglée la semaine suivante, et l'eau, elle, n'a manqué à personne. On ne conçoit pas un service public en espérant que les gens renoncent à leurs droits.

Note de lecture

7 lieux, une journée. Aucun de ces récits ne décrit une prouesse, et c'est le propos : la robustesse ne se voit pas. Elle se compte en catastrophes qui n'ont pas eu lieu, en journées restées ordinaires.

Un système d'information robuste, inscrit dans une soutenabilité forte, promet peu de choses si ce n'est que le jour où quelque chose arrive, ce soit un mardi comme les autres.

