LIVRE BLANC

Voyage vers la robustesse

Construire une stratégie d'organisation pour pallier les risques induits sur le numérique face aux enjeux climatiques, géopolitiques, sociaux et technologiques

INFOGREEN FACTORY

CEE Les certificats d'économies d'énergie

PROGRAMME Alt IMPACT se mobiliser pour la sobriété numérique

Co-porté par RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité

ADEME Agence de la transition écologique

Inria

cnrs

Ce document est édité par : Infogreen Factory
https://infogreenfactory.green

Cet ouvrage est disponible en ligne : https://infogreenfactory.green/publications/livre-blanc-robustesse

Coordination générale : Christophe PHAM
christophe@infogreenfactory.fr

Rédaction et conception : Stéphan PECCINI
stephan-pro@peccini.fr
Rédigé avec LyX et LaTeX

Création graphique : Céline VANDERKELEN
celine.vanderkelen@gmail.com

Coordination technique : Carole ALBRESPY
carole.albrespy@infogreenfactory.fr
Cédric GRAVOUIL
cedric.gravouil@infogreenfactory.fr
Charline CORMIER
charline.cormier@infogreenfactory.fr

Remerciements de Christophe Pham
Fondateur Infogreen Factory

En premier lieu, il est essentiel de souligner que ce livre blanc doit beaucoup au travail de recherche exceptionnel et de rédaction menés par Stéphan Peccini, que nous remercions tout particulièrement.

Nos remerciements vont également à l'ADEME (en particulier au programme Alt Impact), cette formidable agence étatique dont les productions sont précieuses et permettent d'ouvrir des voies très prometteuses. L'ADEME nous a fait confiance et nous a surtout fourni des retours réguliers pertinents nous permettant de réorienter parfois nos travaux. Merci à Dylan Marivan et Thomas de Latour de l'ADEME, à Benjamin Ninassi de l'INRIA et au groupement Ecoinfo pour leur relecture.

Nous avons eu la chance de recevoir le soutien appuyé et d'avoir des échanges passionnants et passionnés avec différentes associations comme le CIGREF (merci Flora Fischer et Pierre Skrzypzack), l'Institut du Numérique Responsable (INR — avec merci tout particulier à Vincent Courboulay qui a eu l'extrême bonté de signer la préface et à Guillaume Gallon), l'AGIT (merci à Romuald Ribault et au bureau). Merci également à Digital New Deal (Arno Pons) dont l'initiative conjointe autour de l'IRN (indice de résilience numérique) nous semble porteuse de sens pour le bien commun.

Nous tenons également à remercier chaleureusement nos collègues de l'ambitieux programme Share de l'IRT b<>com qui ont toujours été d'un grand soutien et dont les feedback constructifs nous ont permis d'avancer. Merci en particulier à Martin Ragot, Alexis Nicolas, Christel Fauché, Roger Waldeck et Dominique Poitevin.

Nous avons eu la chance d'obtenir des retours circonstanciés et précieux de la part de nombreuses personnes, dont François Giraudon de Suricats, Ines Genton Garcia de Dirigent, Arnaud Crétot de Neo Loco qui a, aussi, rédigé le chapitre sur la démarche TELED, Nicolas Schmitt (de BNP Paribas), Martin Deron (chercheur canadien autour de la bifurcation du numérique).

Bien entendu, le groupe de travail interne Infogreen Factory a joué un rôle clé. Un grand merci notamment à Charline Cormier, Carole Albrespy, Frédéric Marty, Karine Maj, Axelle Bureau, Stéphanie Chipaux, Frédérik Varlet, France Kaliris, Matthieu Pelard, Anne Himeno, Laurent Devernay et Guillaume Wolff pour leurs contributions.

Merci à toutes les énergies qui ont porté l'équipe lors des 4 mois de rédaction de ce livre blanc. Elles ont permis de rédiger un document qui a une ambition assumée de réinventer le numérique dans un monde dans lequel la « variabilité » devient la norme.

Préface de Vincent Courboulay
Maître de Conférences à La Rochelle Université
Administrateur de l'Institut du Numérique Responsable

Robustesse : quand le numérique change de paradigme

Je dois l'avouer d'emblée : je n'ai jamais été un grand amateur de *livres blancs*. Trop souvent, ils empilent des concepts lisses et rassurants, des promesses bien intentionnées, sans jamais se risquer à l'épreuve du concret. De plus, ils finissent bien souvent dans le cimetière des livres blancs, dans lequel ils sont poussés par une série d'autres livres blancs qui attendent à leur tour d'y entrer.

Et là, j'ai eu une très bonne surprise…

Ce livre blanc sur la robustesse ne se contente pas de définir un énième concept. Il fait quelque chose de plus rare et, à mon sens, plus précieux : il relie la théorie à la pratique, sans simplifier à outrance, sans céder à la facilité du slogan. On y trouve des cadres de réflexion solides, mais aussi des exemples concrets, des choix assumés toujours éclairants. Bref, de la matière vivante.

La robustesse est un thème particulièrement bienvenu. Elle renouvelle le numérique responsable, en le sortant d'une logique défensive. Être robuste, ce n'est pas seulement « réduire son impact » ou « faire mieux avec moins » ; c'est concevoir des systèmes capables d'encaisser les chocs, de durer dans l'incertitude, d'être compréhensibles, réparables, appropriables dans un monde qui l'est de moins en moins. À ce titre, la robustesse élargit utilement la notion de souveraineté, vers un concept d'autonomie stratégique qui permet de ne pas dépendre aveuglément de systèmes opaques ou hors-sol.

Enfin, je tiens à souligner un point essentiel : je connais les équipes qui ont porté ce travail. Leur compétence est réelle, mais c'est surtout leur humanité qui transparaît dans ces pages. On sent une volonté sincère de transmettre, de partager, d'outiller et de ne pas donner des leçons. Cette posture fait la différence.

Je formule donc un vœu en conclusion : que ce document ne reste pas un point d'arrivée, mais devienne un socle. Un socle pour aller plus loin, pour imaginer des MOOC, des serious games, des parcours pédagogiques, des mises en situation concrètes permettant de s'approprier réellement la robustesse. Car si le numérique responsable veut peser face aux crises à venir, il devra non seulement être sobre et éthique, mais devra surtout renforcer la robustesse des organisations.

Et ce livre blanc en est, à l'évidence, une première pierre solide.

Table des matières

Partie I

PRÉAMBULE

Chapitre 1

Avant-propos

Le monde change à une vitesse sans précédent. Crises climatiques, tensions géopolitiques, ruptures technologiques : ces bouleversements ne sont plus des événements isolés, mais des réalités interconnectées qui s'amplifient mutuellement.

Au cœur de cette transformation, une question devient cruciale pour toute organisation : **comment garantir la continuité des activités quand le numérique, devenu indispensable, devient aussi une grande vulnérabilité ?**

Ce livre blanc s'adresse, en particulier, aux directions d'organisations qui se posent ces questions :

- Comment les mutations du monde affectent-elles mon infrastructure numérique ?
- Quels impacts auront ces mutations sur la production de mes services et de mes biens ?
- Quelles stratégies faut-il alors adopter pour renforcer la continuité de mon activité ?

Il s'adresse aussi aux personnes expertes qui accompagneront les organisations dans la mise en œuvre des solutions proposées dans ce livre blanc.

Notre approche combine trois éléments :

- Des exemples concrets inspirants, issus de situations réelles ;
- Des bases scientifiques à l'état de l'art de la recherche internationale(*) ;
- Des outils pratiques pour guider une transformation progressive.

(*) *notamment les analyses convergentes des principales institutions mondiales d'évaluation des risques (AXA Future Risks Report 2024, Allianz Risk Barometer 2025, Swiss Re SONAR 2024-2025, OCDE States of Fragility 2025) et les travaux de recherche récents publiés par l'ONU, l'Union Européenne, Oxford et les réseaux académiques européens (PolyCIVIS, ERC) ou dans Springer, Cambridge University Press, Routledge*

Dans ce monde qui peut sembler anxiogène, il est possible de se protéger en adoptant des stratégies simples à appréhender et nécessaires à mettre en pratique.

Ce livre blanc vous propose un chemin progressif pour renforcer votre capacité à faire face aux futurs possibles du numérique. Non pas en renonçant à la technologie, mais en apprenant à l'utiliser avec discernement, en gérant en douceur le changement à apporter grâce à un accompagnement des personnes de l'organisation et une gouvernance adaptée à cette transformation.

Découvrons ensemble comment y parvenir.

Chapitre 2

Poser les bonnes fondations

Résilience du numérique, robustesse de l'organisation

D'un côté, Hewlett Packard Enterprise (HPE) définit la résilience informatique comme « [la garantie] que [les] systèmes critiques restent opérationnels malgré les perturbations, en protégeant les données et en minimisant les temps d'arrêt » [1].

D'un autre côté, Olivier Hamant théorise depuis des années le terme de « robustesse », qu'il définit comme la capacité à « créer les conditions grâce auxquelles on ne tombe pas » et à « maintenir le système stable malgré les fluctuations, à court terme et à plus long terme » [2].

> **Note :** dans la suite de cet ouvrage, sauf mention contraire, nous emploierons le terme "*résilience*" pour désigner la résilience du numérique et le terme "*robustesse*" pour désigner la robustesse

Est-ce que le numérique peut être robuste ?

Notre conviction est que le numérique ne peut pas être robuste, au sens de la définition d'Olivier Hamant. En effet, il se fonde sur des ressources et des infrastructures indépendantes du secteur, qui sont fragiles et instables.

En revanche, le numérique peut, et doit, être résilient en étant conçu pour résister aux incidents et retrouver son état de fonctionnement après une panne ou une attaque. Toutefois, sur le long terme, certaines causes (manque de ressources cruciales à sa fabrication, conflits géopolitiques…) peuvent rendre problématique son approvisionnement en serveurs et en terminaux et créer des points de rupture.

Notre vision : une stratégie claire fondée sur deux définitions

Définition 1 : la résilience du numérique

Nous considérons la résilience du numérique comme une propriété technique, nécessaire, mais limitée.

Terme	Notre définition
Résilience du numérique	La capacité d'un système numérique à résister aux perturbations (pannes, cyberattaques, crises) et à revenir à un état fonctionnel après l'incident. Cette disposition est limitée par la dépendance du système à des ressources externes (énergie, matériaux, infrastructures) sur lesquelles il n'a pas de contrôle direct et qui pourront manquer dans l'avenir.

- **Nature** : réactive et technique (propriété du système).
- **Objectif** : revenir à un état stable après un choc (élasticité).
- **Limite** : dépendance aux facteurs externes.

Définition 2 : la robustesse de l'organisation par rapport au numérique

La véritable ambition, selon nous, doit se situer au niveau de l'organisation. C'est là que se trouve le véritable levier d'action. Une vision globale de cette notion est indispensable pour intégrer le numérique dans votre stratégie et la déployer. Le numérique est une piste de travail pour assurer la robustesse, mais il n'est pas la seule. Le livre blanc ne traite, toutefois, que cette piste pour vous accompagner dans votre stratégie.

Terme	Notre définition
Robustesse d'une organisation (en relation avec le numérique)	La capacité d'une organisation à maintenir ses fonctions essentielles de manière stable et viable face aux défaillances du numérique, en créant les conditions pour ne pas tomber. Cette robustesse, dimensionnée pour assurer la pérennité souhaitée par l'organisation, repose sur l'hétérogénéité des solutions, la redondance des moyens, l'acceptation d'une lenteur relative et le maintien d'alternatives faiblement technologiques.

- **Nature** : préventive et organisationnelle (propriété de l'organisation).
- **Objectif** : ne pas tomber en cas de défaillance du numérique.
- **Moyen** : créer des marges de manœuvre (redondance, alternatives, etc.).

Pourquoi cette distinction est-elle cruciale ?

Cette distinction n'est pas qu'un simple exercice sémantique, elle est cruciale ! Elle est la clé de voûte d'une stratégie de continuité d'activité lucide et efficace.

Cette distinction permet de reconnaître que la résilience concerne uniquement les systèmes techniques alors que la robustesse relève de l'organisation. Elle évite de chercher une perfection technologique impossible et oriente plutôt les efforts vers la création de marges de manœuvre humaines, structurelles et stratégiques.

En adoptant cette vision, vous ne cherchez plus seulement à vous relever après une crise induite par les vulnérabilités du numérique (la résilience), mais à créer les conditions pour que la plupart des crises n'en soient plus, en apprenant d'elles pour vous renforcer. C'est tout l'enjeu de la robustesse, et le chemin que nous vous proposons d'explorer.

---

[1] HPE. *What is IT resilience ?* URL : https://www.hpe.com/us/en/what-is/it-resilience.html.

[2] Olivier HAMANT. *Pourquoi parler de robustesse et non de résilience ?* larobustesse.org. URL : https://larobustesse.org/?PourquoiParlerDeRobustesseEtNonDeResilie.

Chapitre 3

Structure du document

3.1 Convention

Dans ce document, les liens possibles à l'intérieur ou vers l'extérieur sont les suivants; ils apparaissent sous les formes indiquées ci-après :

Les URL :

- https://infogreenfactory.green
- Les URL apparaissent explicitement avec leur contenu intégral; il n'y a pas de lien vers un site externe qui se fasse en cliquant sur du texte.

Les adresses mail :

- stephan-pro@peccini.fr

Les renvois vers une bibliographie :

- [1]
- En fin de chaque chapitre, la bibliographie des sujets mentionnés dans ce chapitre est insérée. Dans le cas ci-dessus, on verrait dans la bibliographie :
  - [1] HPE. What is IT resilience? url : https://www.hpe.com/us/en/what-is/it-resilience.html.

Les références croisées :

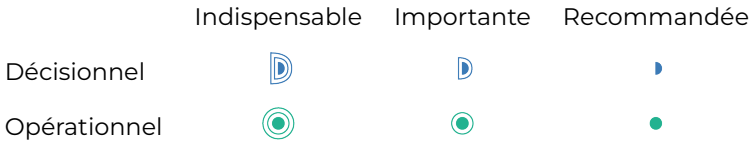
- Structure du document
- Ces références permettent de faire le lien depuis une partie du document vers une autre en affichant le contenu textuel de la destination. En version interactive, cliquer sur le texte pour se rendre vers cette partie et revenir vers la partie d'origine avec le raccourci clavier ou le bouton retour de votre lecteur.

Les termes du glossaire :

- VUCA
- Certains termes peu communs utilisés dans le document sont expliqués en toute fin dans un glossaire général. En version interactive, faire comme pour les références croisées.

3.2 Guide de lecture

Dans les tableaux ci-dessous, le niveau de lecture par rôle pour chaque chapitre du document est défini par les pictogrammes suivants.



Préambule

▷ Bien démarrer.

Livre blanc

▷ Cœur de l'analyse.

Fondations de la démarche

Inspiration principale, enjeux et point de départ.

Outillage

Comment arbitrer, prioriser et dérouler la démarche.

La démarche progressive

Déployer la stratégie afin de renforcer, optimiser et expérimenter.

Conclusion

Le voyage vers la robustesse est maintenant terminé.

Annexes

▷ Compléter et approfondir.

Ressources

Importance du sujet

Outillage détaillé

Comment arbitrer, prioriser et dérouler la démarche.

Compréhension et inspiration

Inspirations pour la compréhension et la déclinaison d'exemples.

Information

Aller plus en détail dans la compréhension des enjeux et des solutions radicales.

La démarche progressive détaillée

Détails et documentions pour déployer la stratégie afin de renforcer, optimiser et expérimenter.

Nous vous préconisons de lire ce document selon les niveaux proposés :

1. Concentrez votre lecture sur les chapitres indispensables; vous aurez alors tous les éléments nécessaires pour comprendre et pour prendre des décisions ou pour déployer la démarche complète (selon votre rôle).

2. En lisant ces premiers chapitres, il est fort probable que vous vous posiez des questions ou que vous ayez envie d'en savoir plus. Les chapitres dont la lecture est importante seront là pour apporter des réponses à ces besoins légitimes.

3. Finalement, vous aurez sûrement envie d'aller plus loin dans la compréhension de ce vaste sujet. Lisez alors les chapitres recommandés, ils vous aideront dans votre progression.

Vous pouvez aussi lire ce document en plusieurs phases,

- Pour le rôle décisionnel :

    1. Lisez dans un premier temps, les fondations de la démarche et l'outillage. Prenez le temps de vous projeter dans votre contexte avec ces nouveaux acquis.

    2. Prenez connaissance des mécanismes de fragilisation qui vous aideront à identifier toutes les situations de risques et à envisager les impacts potentiels sur votre organisation.

    3. Une fois cette imprégnation faite, passez à la démarche progressive, tour par tour, pour bien identifier comment les adapter à votre environnement.

- Pour le rôle opérationnel :

    1. Lisez dans un premier temps, les chapitres consacrés à l'outillage détaillé. Identifiez comment, dans l'activité opérationnelle, ces outils peuvent s'insérer.

    2. Une fois que vous les avez bien intégrés, vous pouvez passer à la lecture de la démarche détaillée afin de la mettre en œuvre, tout par tour.

« L'intelligence, c'est la capacité à s'adapter au changement. »

Stephen Hawking, physicien théoricien et cosmologiste britannique

« La robustesse maintient un système stable, malgré les fluctuations. Le roseau plie mais ne casse jamais. [...]
Les êtres vivants robustes ne sont pas parfaitement adaptés,
ils sont d'abord adaptables. »

Olivier Hamant, chercheur français en biologie et biophysique (La troisième voie du vivant)

Partie II

LIVRE BLANC

Sommaire

Chapitre 4

L’étincelle Oseja

Tout commence dans le chaos.

28 avril 2025, 12 h 33.

La péninsule ibérique s’arrête, brutalement, sans prévenir.

Un phénomène de surtension en cascade sur le réseau électrique paralyse l’Espagne et le Portugal. Cinquante-cinq millions de personnes sont privées d’électricité. Les feux de circulation s’éteignent. Les métros s’immobilisent. Les hôpitaux basculent sur leurs générateurs de secours. Les communications sont coupées.

C’est le chaos ! Illustration parfaite de la fragilité de nos systèmes centralisés et fortement interconnectés. [3]

Pourtant…

Malgré le chaos, un village résiste.

Dans les montagnes du León, au cœur du parc national des Picos de Europa, un petit village de moins de 300 âmes continue de vivre, comme si de rien n’était. Oseja de Sajambre, rarissime point encore alimenté en électricité dans une Espagne paralysée, devient un symbole inattendu de la résilience. [4]

Miracle ?

Non, ce n’en est pas un.

C’est simplement le fruit d’une stratégie délibérée d’adaptabilité aux aléas. Habitués aux coupures de courant hivernales dues aux tempêtes de neige, le maire et tout son village avaient anticipé le problème. Ils ont investi dans un système de micro-réseau électrique capable de fonctionner en autonomie, alimenté par des sources d’énergie locales, distribuées et diversifiées, entre les habitants.

En quelques minutes, le village s’est déconnecté du réseau national défaillant pour s’appuyer sur ses propres ressources. [5]

Leur secret ? Une culture de l’autonomie forgée par l’expérience et un principe simple : ne jamais dépendre entièrement d’un seul système, aussi fiable soit-il en apparence, pour être en capacité de basculer en mode « île » (totale autonomie). [6]

Inspirant, non ?

Cette histoire, parmi tant d’autres, est à l’origine de ce livre blanc.

Le cas d’Oseja de Sajambre propose une leçon universelle qui dépasse la seule question énergétique. Comment l’appliquer, en particulier, pour notre infrastructure numérique, tellement critique et imbriquée dans notre quotidien ?

Nos entreprises, nos administrations, nos services essentiels sont aujourd'hui massivement dépendants d'un « réseau numérique » mondialisé, concentré entre les mains de quelques acteurs, et tout aussi vulnérable à des pannes systémiques ou des défauts d'approvisionnement.

Tout le monde est concerné, **vous aussi !**

La question posée par l'exemple d'Oseja est simple : **comment votre organisation peut-elle devenir l'Oseja du numérique ?** Comment peut-elle développer la capacité à « se déconnecter » des pannes globales pour maintenir ses opérations critiques ? Et ce, quelles que soient les origines des pannes : climatiques, sociales, géopolitiques, concurrentielles…

Ce livre blanc a été pensé et conçu pour répondre à cette question fondamentale. Il propose une approche pour trouver votre propre résilience numérique, non pas en renonçant à la technologie, mais en apprenant à l'utiliser de manière robuste, autonome et pertinente. Pour que la prochaine grande panne numérique ne soit qu'un désagrément passager et, surtout, une opportunité pour progresser.

---

[3] ENTSO-E. *Factual Report : 28 April 2025 Iberian Blackout*. European Network of Transmission System Operators for Electricity, 2025. URL : https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/.

[4] Nicolás BOULLOSA. *The Asterix village in the dark : resilience in a blacked-out world*. Avr. 2025. URL : https://faircompanies.com/articles/the-asterix-village-in-the-dark-resilience-in-a-blacked-out-world/.

[5] ONE MEDIA. *Le village autonome qui a échappé au blackout électrique*. 2025. URL : https://onemedia.fr/actualite/le-village-autonome-qui-a-echappe-au-grand-blackout-electrique/.

[6] James NELSON et al. "Statistical development of microgrid resilience during islanding operations". In : *Applied Energy* 279 (2020), p. 115733. URL : https://www.sciencedirect.com/science/article/pii/S0306261920312150.

Chapitre 5

La polycrise

5.1 Les vulnérabilités convergent et s'amplifient

> *87 % des experts estiment que le monde est plus vulnérable aux risques qu'il ne l'était il y a cinq ans.*
>
> **— AXA - Future Risks Report 2024 (p.4)**

> *Tous les 177 contextes analysés par le cadre multidimensionnel de fragilité de l'OCDE sont exposés à un certain niveau de fragilité.*
>
> **— OCDE - États de fragilité 2025 (p.6)**

> *Les chaînes d'approvisionnement mondiales – la résilience face au risque d'interruption d'activité s'affaiblit.*
>
> **— Swiss Re - SONAR 2024 (p.24)**

Pensez-vous que votre organisation soit prémunie contre les vulnérabilités qui affectent le numérique ? Avant même de répondre à cette question, avez-vous identifié toutes les vulnérabilités qui mettent en danger la filière du numérique, depuis sa fabrication jusqu'à son utilisation ?

Annexe Mécanismes et scénarios
Découvrez six mécanismes de fragilisation qui mettent en danger votre numérique et les six scénarios pour imaginer des chocs sur votre système d'information.

À titre d'exemple, en 2024, la mise à jour de Crowdstrike a entraîné une panne mondiale, lourde de conséquences : vols annulés, interventions chirurgicales reportées, transactions financières arrêtées.

Au lieu d'un bug tel que cela s'est passé, quel aurait été l'impact si cela avait été une cyberattaque contre Crowdstrike, activée plusieurs jours après le déploiement complet ?

Peu relayée dans les médias, l'inondation de la mine de Spruce Pine en 2024 a contraint l'exploitation à s'interrompre pendant deux mois ; l'ouragan Helene était passé par là. Cette mine alimente à 80, voire 90 %, la chaîne de fabrication des semi-conducteurs avec un quartz ultrapur, indispensable et insubstituable. Les stocks stratégiques estimés permettent une interruption de trois mois maximum.

Annexe Vulnérabilités paradoxales
Comprendre l'origine de ces anomalies, comment elles ont ou auraient pu fragiliser de manière très importante le secteur du numérique.

Que serait devenu votre prochain projet en cas de rupture d'approvisionnement plus longue, avec un deuxième ouragan ou un effondrement de la mine ?

Tout au long de ce livre blanc, nous allons trouver ensemble comment identifier les aléas et leurs impacts, découvrir des exemples inspirants qui se déclineront en prenant appui sur vos atouts et en en créant de nouveaux.

Ces incidents, Crowdstrike, Spruce Pine, ne sont pas des anomalies isolées, mais les symptômes d'une transformation systémique que les analystes qualifient désormais de « polycrise ». Ce concept, théorisé par Edgar Morin dès les années 1990 et popularisé récemment par l'historien Adam Tooze, dépasse la simple accumulation de crises pour décrire un phénomène qualitativement différent.

5.2 Le basculement de paradigme : la stabilité n'est plus la norme

Annexe La polycrise
Comprenez les mécanismes qui entrent en jeu, les spécificités pour le numérique et comment arbitrer.

Le nouveau monde que nous connaissons marque la fin d'un paradigme qui a structuré la modernité industrielle : la stabilité comme état normal des systèmes. Pendant plusieurs décennies, l'organisation sociale et économique s'est construite sur l'hypothèse d'un environnement prévisible, climatiquement, géopolitiquement, socialement. Les perturbations constituaient des exceptions temporaires et assez isolées pour se corriger naturellement — avec ou sans intervention humaine — et ainsi permettre de retrouver un équilibre stable, très proche ou identique au précédent.

Or, les sciences de la complexité révèlent que cette stabilité apparente résultait de conditions historiques exceptionnelles : abondance énergétique fossile, climat stable, croissance démographique et économique continue. Ces conditions s'estompent progressivement, révélant la nature fondamentalement dynamique et imprévisible des systèmes complexes.

Le changement devient la norme, l'incertitude la règle, l'adaptabilité une nécessité permanente.

Cette instabilité structurelle remet en question les fondements de nos stratégies de résilience. Les approches traditionnelles, fondées sur la prédiction et la planification, deviennent insuffisantes, voire inadéquates, face à des systèmes dont les caractéristiques dépendent de l'interaction entre leurs composants. Les neurosciences cognitives, notamment les travaux de Mehdi Khamassi [7] sur la prise de décision dans l'incertitude, révèlent que cette complexité croissante dépasse les capacités cognitives humaines.

Elle génère ce que les informaticiens appellent des « défaillances (bugs) systémiques » : des défaillances qui émergent de l'interaction entre composants fonctionnels pris individuellement. L'incident CrowdStrike illustre parfaitement ce phénomène : un logiciel de sécurité devient lui-même la source d'une panne globale, par effet de cascade.

5.3 Anatomie de la polycrise : interconnexion et amplification

> *À l'ère des polycrises – où les crises interconnectées s'amplifient mutuellement – les dirigeants doivent surmonter les obstacles systémiques pour mettre en œuvre des solutions qui permettent un progrès significatif et durable.*
>
> **— Center for Creative Leadership - Leading Beyond Barriers : Creating Impact in an Age of Polycrisis (p.1)**

Le Cascade Institute de l'Université de Victoria définit la polycrise comme « l'enchevêtrement causal de crises dans plusieurs systèmes globaux de manière à dégrader significativement les perspectives de l'humanité ». Thomas Homer-Dixon, directeur de l'institut, identifie trois caractéristiques fondamentales qui transforment des crises isolées en polycrise systémique :

L'interconnexion structurelle : les systèmes économiques, technologiques, sociaux et environnementaux sont désormais si étroitement imbriqués qu'une perturbation dans l'un se propage inévitablement aux autres.

La synchronisation temporelle : les cycles de crise, autrefois décalés, se synchronisent.

L'amplification non-linéaire : dans un système complexe sous tension, de petites perturbations peuvent déclencher des cascades catastrophiques.

5.4 Polycrise et numérique : vulnérabilités spécifiques du monde connecté

Dans ce contexte de polycrise globale, l'infrastructure numérique présente des vulnérabilités spécifiques qui amplifient les risques systémiques :

- Concentration oligopolistique extrême : cinq entreprises (Amazon, Microsoft, Google, Alibaba, IBM) contrôlent 77 % du marché mondial du cloud, selon Synergy Research.
- Dépendance géopolitique asymétrique : 92 % du marché des semi-conducteurs avancés indispensables à tout notre numérique est concentré entre Taïwan (TSMC – Taïwan Semiconductor Manufacturing Company) et la Corée du Sud (Samsung). 83 % des dépenses IT des entreprises européennes vont vers des entreprises américaines.
- Vulnérabilité des infrastructures physiques : 99 % du trafic internet intercontinental transite par 485 câbles sous-marins. 22 % des datacenters sont déjà menacés climatiquement (Swiss RE, 2024).
- Complexité incontrôlable : la dette technique (coût futur engendré par des choix techniques à court terme) [8] mondiale est estimée à plus de 1500 milliards de dollars.

[7] Mehdi KHAMASSI et al. “Behavioral regulation and the modulation of information coding in the lateral prefrontal and cingulate cortex”. In : *Cerebral Cortex* 25.9 (2015), p. 3197-3218. DOI : 10.1093/cercor/bhu114. URL : https://doi.org/10.1093/cercor/bhu114.

[8] OPTEAMIS. *La dette technique : le passif invisible du numérique*. 2025. URL : https://www.opteamis.com/la-dette-technique-le-passif-invisible-du-numerique/.

Chapitre 6

Votre robustesse face au numérique — Naviguer dans l'ère de la polycrise

6.1 La résilience, vous savez déjà la maîtriser

Nous avons collectivement traversé ces dernières années une succession de crises qui ont fondamentalement transformé nos approches pour les gérer.

- La pandémie de COVID-19 a bouleversé les chaînes d'approvisionnement, imposant une refonte complète des stratégies de sourcing et de stock.
- La guerre en Ukraine a perturbé les approvisionnements énergétiques, contraignant à repenser le mix énergétique et les coûts de production.
- Les événements climatiques extrêmes, inondations, canicules, tempêtes, affectent régulièrement les sites de production et les réseaux logistiques, obligeant à intégrer l'adaptation climatique dans votre planification stratégique.

Face à ces défis, vous avez développé et renforcé une expertise précieuse en résilience opérationnelle. Améliorations des plans de continuité d'activité (PCA) et des plans de reprise d'activité (PRA) associés, diversification des fournisseurs, constitution de stocks stratégiques, cellules de crise, scénarios de stress tests ; ces dispositifs constituent désormais l'arsenal standard de toute organisation consciente de sa vulnérabilité. Selon une étude McKinsey de 2023, 85 % des entreprises européennes ont renforcé leurs dispositifs de gestion de crise depuis 2020 [9].

Cette maturité croissante en matière de résilience témoigne d'une prise de conscience collective : dans un environnement que le Boston Consulting Group qualifie de « permacrise » [10], autre vision de la polycrise, la capacité d'adaptation continue, ou l'adaptabilité, devient plus critique que la seule optimisation de la performance.

Cette expertise en résilience métier constitue un socle solide. Vous savez identifier les processus critiques, évaluer les risques, construire des alternatives, former vos équipes à la gestion de crise. Vous comprenez intuitivement que la redondance, longtemps perçue comme un coût improductif, devient une assurance vitale quand la stabilité n'est plus garantie.

Cette compréhension systémique de la vulnérabilité et de la résilience représente exactement la grille de lecture nécessaire pour aborder un angle mort majeur de votre stratégie : la dépendance au numérique qui sous-tend l'ensemble des opérations, numérique dont la fragilité est souvent sous-estimée, depuis l'extraction des matières premières jusqu'à la livraison des matériels et des services.

6.2 Le test de résilience numérique

Prenons un instant pour cartographier en partie l'infrastructure numérique qui alimente quelques-unes des opérations quotidiennes à titre d'exemple. Cette analyse révèle une réalité souvent occultée par l'habitude et la familiarité technologique.

Les **processus de production** reposent sur des systèmes ERP (Enterprise Resource Planning) hébergés à 67 % dans le cloud selon Gartner [11]. Ces systèmes orchestrent en temps réel l'allocation des ressources, la planification de la production, la gestion des stocks. Une interruption de 24 heures de votre ERP paralyserait littéralement votre capacité de production, comme l'ont expérimenté les 1400 entreprises touchées par la cyberattaque de Kaseya en 2021 [12].

Les **communications internes** transitent massivement par des plateformes collaboratives (Microsoft Teams, Slack, Google Workspace) qui centralisent en même temps les échanges, et la documentation, les processus de validation, la mémoire collective de l'organisation. Une entreprise utilise en moyenne 89 applications SaaS différentes [13], créant une toile de dépendances dont la complexité et les interactions entre composants échappent souvent aux organisations elles-mêmes.

La **relation client** s'appuie sur des CRM (Customer Relationship Management) sophistiqués qui stockent l'historique des interactions, automatisent les campagnes marketing, prédisent les comportements d'achat. Salesforce, leader du marché, traite 100 milliards d'interactions client par jour [14]. Une panne de ces systèmes ne signifie pas seulement une interruption de service, mais une amnésie organisationnelle temporaire.

Les **transactions financières** dépendent entièrement d'infrastructures bancaires numériques interconnectées. SWIFT traite au quotidien 42 millions de messages financiers pour une valeur de 150 000 milliards de dollars [15]. Les systèmes de paiement électronique, les virements automatiques, les prélèvements récurrents — toute cette mécanique financière invisible repose sur des infrastructures dont vous ne maîtrisez ni l'architecture, ni la localisation, ni les vulnérabilités.

Les **services aux citoyens** dépendent massivement de plateformes numériques interconnectées. L'état civil, les inscriptions scolaires, les demandes d'urbanisme, les services sociaux. Une cyberattaque comme celle qui a paralysé la ville d'Angers pendant trois semaines en 2021, ou celle de Lille Métropole en 2022, prive instantanément les citoyens de services essentiels et paralyse l'action publique locale.

Les **missions régaliennes** reposent sur des systèmes d'information critiques. La chaîne pénale numérique, les systèmes de paie (SIRH), les bases de données fiscales, les systèmes de santé publique – ces infrastructures traitent quotidiennement des millions d'opérations vitales. L'hôpital de Corbeil-Essonnes, victime d'un 🕮 Ransomware (Rançongiciel) en août 2022, a dû fonctionner « à l'ancienne » pendant des semaines, reportant des opérations et gérant les urgences sur papier.

Les **capacités d'intervention** dépendent entièrement de systèmes de communication et de coordination numériques. Les centres de régulation (SAMU, SDIS), les systèmes d'alerte et de mobilisation, la géolocalisation des équipes, les bases de données médicales d'urgence – une défaillance de ces systèmes peut coûter des vies. Lors de la panne du système d'appel d'urgence d'Orange en juin 2021, plusieurs régions françaises se sont retrouvées sans accès aux numéros d'urgence pendant quatre heures, révélant la fragilité de ces infrastructures vitales.

Ces dépendances ne sont pas un problème en soi. Elles le deviennent quand elles créent des points de défaillance uniques dont vous pourriez ne pas avoir conscience, ou quand elles reposent sur des infrastructures fragiles que vous ne maîtrisez pas. C'est précisément ce que nous allons identifier et renforcer.

6.3 Commençons doucement

1. Identifiez trois processus métier critiques pour votre organisation.
2. Pour chacun, évaluez sa dépendance au numérique et son impact sur votre pérennité.
3. Posez-vous deux questions simples :
   - Le service peut-il être rendu sans numérique ?
     - Application du premier principe de non-régression.
   - La redondance est-elle suffisante pour pallier les vulnérabilités dans la durée ?
     - Application du deuxième principe de redondance organisée.
4. Imaginez un scénario réaliste de rupture de 24 heures.
5. Ensuite, un plus long, de plusieurs jours, ou plusieurs semaines.

Annexe Mécanismes et scénarios

Voilà, vous venez de débuter la transformation. Pour vous aider, voici les six mécanismes de fragilisation que nous explorerons à travers des scénarios concrets dans tout le livre blanc :

1. Fragilités géopolitiques
   - Rupture géopolitique bloquant l'accès aux composants, minerais ou technologies critiques.
   - Exemple : un embargo sur les puces électroniques ou la fermeture d'un service cloud sans préavis à la suite de tensions internationales.
2. Fragilités physiques/climatiques face à l'incertitude environnementale
   - Événements climatiques extrêmes détruisant les infrastructures numériques.
   - Exemple : une canicule prolongée force l'arrêt des datacenters par manque de refroidissement, comme en 2022 où Google et Oracle ont dû réduire leurs capacités en Europe.
3. Fragilités techniques et complexité systémique
   - Un bug dans une mise à jour critique paralyse une part significative de l'infrastructure numérique mondiale.
   - Exemple : la panne CrowdStrike de juillet 2024 a paralysé 8,5 millions de machines Windows, entraînant des pertes estimées à 5,4 milliards de dollars [16].

4. Mécanismes de contagion et ambiguïté des interdépendances
   - Dépendance à un fournisseur unique dont la défaillance bloque les opérations par effet domino.
   - Exemple : l'ouragan Helene en septembre 2024 a menacé les mines de Spruce Pine, qui fournissent 80 % du quartz de haute pureté mondial, indispensable aux semi-conducteurs [17].
5. Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)
   - Enfermement dans des écosystèmes technologiques dont il est impossible de sortir.
   - Exemple : dépendance à un fournisseur cloud unique dont les coûts de sortie deviennent prohibitifs, éliminant toute alternative.
6. Impacts sociétaux dans un contexte d'incertitude croissante
   - L'accélération de l'IA bouleverse les métiers, provoquant une obsolescence massive des compétences.
   - Exemple : PwC a réduit ses embauches de jeunes diplômés de 13 % en 2025, anticipant les gains de productivité de l'IA [18].

6.4 La fenêtre d'opportunité

Chaque jour qui passe voit s'accroître la complexité et l'interdépendance des systèmes numériques. Les investissements mondiaux en transformation numérique atteindront 3 400 milliards de dollars en 2026 [19]. Cette accélération, sans une très forte intégration des principes de résilience, crée une croissance des vulnérabilités en nombre et en impact.

Toutefois, une fenêtre d'opportunité existe. Les organisations qui agissent maintenant peuvent construire leur robustesse à un coût maîtrisé, en intégrant la résilience dès la conception. Celles qui attendront la prochaine crise majeure devront reconstruire dans l'urgence, à des coûts potentiellement prohibitifs.

Vous avez un avantage : votre expertise en résilience métier. Ce livre blanc aide à la transposer au numérique, pas à pas, sans disruption. Vous ne partez pas de zéro, vous construisez sur vos acquis.

Bienvenue dans ce voyage vers la robustesse. Il commence par une simple question : **connaissez-vous vraiment l'étendue de vos dépendances numériques ?**

Vous venez de faire un premier exercice de pensée. Pour structurer ce parcours de transformation et le rendre systématique, nous proposons trois outils complémentaires :

- Les deux principes fondamentaux qui permettent d'arbitrer le type de décision à prendre pour mettre de l'humain ou renforcer la redondance
- La matrice de criticité, qui aide à identifier les vulnérabilités associées au numérique et à prioriser les actions selon l'impact et la dépendance des processus

- La spirale progressive et intégrative, qui structure la montée en maturité, compétences et connaissances.

Les trois chapitres suivants détaillent ces outils utilisés ensuite dans le parcours pour renforcer progressivement votre résilience numérique.

---

[9] McKinsey and Company. *Building Resilience : The CEO's new imperative*. Rapp. tech. McKinsey et Company, 2023.

[10] Boston Consulting Group. *Leading Through Permacrisis*. Rapp. tech. Boston Consulting Group, 2023.

[11] Gartner. *Cloud Computing Trends and Future Direction*. Rapp. tech. Gartner, 2024.

[12] Reuters. *Kaseya Ransomware Attack : Impact Assessment*. 2021.

[13] Okta. *Business at Work Report*. Rapp. tech. Okta, 2023.

[14] Salesforce. *State of the Connected Customer*. Rapp. tech. Salesforce, 2024.

[15] SWIFT. *Annual Traffic Report*. Rapp. tech. SWIFT, 2023.

[16] Parametrix. *CrowdStrike's Impact on the Fortune 500*. Analyse économique estimant les pertes directes à 5,4 milliards de dollars pour les entreprises du Fortune 500 (hors Microsoft). 24 juill. 2024. URL : https://www.parametrixinsurance.com/reports-white-papers/crowdstrikes-impact-on-the-fortune-500.

[17] Z2Data. *Quartz Mine Disruption in Spruce Pine, NC, Threatens Semiconductor Manufacturing*. Rapp. tech. Z2Data, 2024.

[18] Le Monde. *Aux Etats-Unis, l'IA bouleverse déjà le marché du travail et les prédictions de jobs apocalypse se multiplient*. 2025.

[19] IDC. *Worldwide Digital Transformation Spending Guide*. Rapp. tech. IDC, 2024.

Chapitre 7

Deux principes pour naviguer dans la complexité

Passer du techno-solutionnisme à la robustesse

Annexe Les principes fondamentaux
Comprendre plus en profondeur les deux principes avec des exemples inspirants.

Face à la réalité systémique, le réflexe dominant consiste à rechercher davantage des solutions via les innovations technologiques. Cette approche « techno-solutionniste », théorisée par Evgeny Morozov [20], postule que chaque problème possède une solution technique optimale. L'IA résoudra la complexité. L'informatique quantique sécurisera les communications. La blockchain décentralisera la confiance.

Cette vision n'est pas infondée, bien au contraire. Les avancées technologiques génèrent de réels bénéfices mesurables. Google a réduit de 40 % la consommation énergétique de ses datacenters de Google grâce à l'IA [21]. De même, l'IA a révolutionné la prédiction de la structure des protéines, accélérant la recherche pharmaceutique [22].

Cependant, l'accumulation de solutions technologiques crée paradoxalement de nouvelles vulnérabilités. Chaque couche technologique ajoute de la complexité, et donc de la dépendance. Chaque optimisation réduit ainsi les marges de manœuvre. Chaque automatisation érode les compétences manuelles. C'est ce que David Graeber appelait « l'utopie bureaucratique » de la technologie : la promesse de simplification qui génère une complexification infinie [23].

C'est pour cela que les deux principes suivants doivent s'appliquer afin de pallier l'utilisation systématique de la technologie comme solution à tous les problèmes.

---

[20] Evgeny Morozov. *To Save Everything, Click Here*. PublicAffairs, 2013. URL : https://academic.oup.com/jdh/article-abstract/27/1/111/474220?login=false.

[21] Les Échos. *Comment Google utilise l'intelligence artificielle pour faire baisser sa facture d'électricité*. 2018. URL : https://www.lesechos.fr/2016/07/comment-google-utilise-lintelligence-artificielle-pour-faire-baisser-sa-facture-delectricite-218671.

[22] Nature. "Accurate structure prediction of biomolecular interactions with AlphaFold 3". In : *Nature* (2024). URL : https://www.nature.com/articles/s41586-024-07487-w.

[23] David Graeber. *The Utopia of Rules*. 2015. URL : https://files.libcom.org/files/David_Graeber-The_Utopia_of_Rules_On_Technology_St.pdf.

Premier principe — La non-régression : préserver l'autonomie fondamentale

Le premier principe propose un critère simple, mais puissant pour évaluer toute innovation technologique : **la technologie doit fonctionner comme une aide qui augmente les capacités existantes, non comme un substitut qui les remplace**.

Le test décisif : si la technologie disparaît demain, l'organisation doit rapidement pouvoir se retrouver au minimum dans la situation antérieure à son adoption, jamais dans une situation dégradée.

> *La « résilience »… nourrit essentiellement la capacité individuelle et collective à créer ou à reconstruire de manière créative des vies précieuses dans des contextes changeants.*
>
> **— OPHIR (2025) - Approche par les capacités d'Amartya Sen (p.3)**

Deuxième principe — La résilience contrainte : organiser la résilience quand la substitution est inévitable

Certaines transformations technologiques sont irréversibles et nécessaires à notre société. Les systèmes de paiement électronique, les communications numériques, certains processus industriels automatisés ; revenir en arrière serait très complexe, voire impossible.

Dans ces cas, le deuxième principe s'applique : **organiser systématiquement la résilience par la redondance accrue, la diversification efficace, et la capacité de dégradation contrôlée**, sans oublier de mettre en place une supervision pour détecter les défaillances.

> *Les investissements sont orientés vers la sécurisation des infrastructures critiques, avec une faible exposition à l'innovation de rupture.*
>
> **— Cigref (2025) - Application concrète du principe (p.8)**

Chapitre 8

La matrice de criticité — Boussole de votre résilience numérique

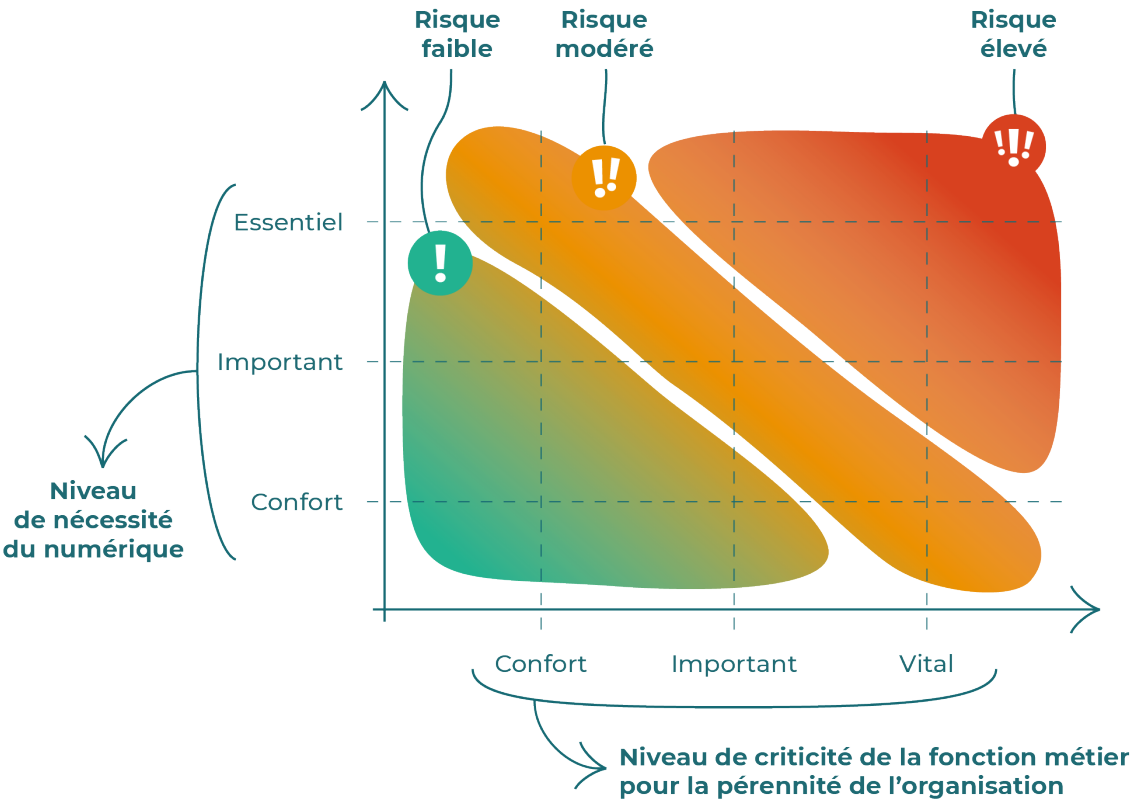


FIG. 8.0.1 : Matrice de criticité

8.1 Identifier vos vulnérabilités : une approche systématique

Annexe La matrice de criticité
Plongez plus en profondeur pour mieux comprendre votre boussole de la pérennité.

Face à la complexité de la polycrise numérique, il peut être tentant de vouloir tout protéger. Cette approche est non seulement coûteuse, mais elle est aussi inefficace. La résilience ne consiste pas à renforcer uniformément tous les systèmes, mais à identifier et prioriser les composants réellement critiques pour votre métier.

C'est précisément l'objectif de la matrice de criticité, outil central de la démarche proposée dans ce livre blanc.

8.2 Comprendre la matrice

La matrice croise deux dimensions essentielles :

Verticalement : le niveau de nécessité du numérique.
Il mesure à quel point votre activité dépend du numérique pour fonctionner. Le numérique peut être de confort (présent, mais non indispensable), important (nécessaire pour l'efficacité et ainsi atteindre les objectifs), ou essentiel (sans lequel l'activité s'arrête).

Horizontalement : le niveau de criticité de la fonction métier pour la pérennité de l'organisation.
Il évalue l'impact d'une défaillance sur votre organisation. Une fonction peut être du confort (impact alors limité, voire anecdotique), importante (perturbation alors notable, mais gérable), ou vitale (paralysie de l'activité).

Le croisement de ces deux axes produit trois zones, du risque faible (zone verte) au risque élevé (zone rouge), en passant par le risque modéré (zone orange).

8.3 Évaluer la criticité : penser aussi en matière de flux métier

Un point essentiel à intégrer dans l'analyse : **la criticité d'un composant numérique ne dépend pas seulement de sa fonction propre, mais également de son rôle dans les flux métier de votre organisation**.

Il ne s'agit pas nécessairement de cartographier exhaustivement toutes les dépendances techniques, mais de tenir compte des flux métier lors de l'évaluation. Posez-vous la question : si ce composant tombe, quels processus métier sont affectés ? Combien de services en dépendent ? Quelle est la cascade potentielle ?

Cette approche systémique permet d'identifier tous les véritables points critiques, souvent invisibles dans une analyse seulement fonctionnelle.

8.4 Prioriser les actions : du risque élevé au risque faible

Une fois vos composants positionnés dans la matrice, la priorisation devient évidente en fonction de la zone :

Rouge (risque maximal) : Ces composants vitaux à criticité forte exigent une attention immédiate. Ils doivent bénéficier de la redondance, numérique ou non, la plus robuste, de plans de continuité éprouvés et testés, et d'une surveillance permanente.

Orange (risque modéré) : Ces composants nécessitent des mesures de protection proportionnées. La redondance peut être modérée, l'utilité de toutes les fonctionnalités évaluées, les plans de continuité exister, et la surveillance être régulière. L'investissement en résilience doit rester proportionné au risque réel.

Verte (risque faible) : Ces composants peuvent se contenter de mesures standard, d'alternatives low-tech, voire de renoncement.

Cette priorisation permet d'arbitrer rationnellement entre les investissements en résilience et les autres priorités stratégiques. Elle évite le double piège de la sous-protection (ignorer les risques) et de la surprotection (dépenser sans discernement).

8.5 Structurer la démarche : de l'analyse à l'action

Cette boussole structure l'ensemble de la démarche proposée dans ce livre blanc :

Identifier les composants applicatifs et techniques et les positionner dans la matrice (exercice de pensée).

Prioriser les actions selon le niveau de risque identifié.

Appliquer les deux principes de résilience (non-régression et renforcement de la redondance) en commençant par les zones à risque maximal.

Décliner opérationnellement à travers une démarche progressive de renforcement.

Cette approche permet de garder une vision stratégique tout en préparant les déclinaisons opérationnelles qui viendront dans les phases suivantes. Elle transforme la complexité de la polycrise numérique en une feuille de route claire et actionnable.

La matrice n'est pas un outil figé : elle doit évoluer avec votre organisation, vos métiers, et l'évolution du contexte numérique. Elle est votre ***boussole*** pour naviguer dans l'incertitude, pas une carte définitive du territoire.

Dans la suite de ce livre blanc, nous détaillerons comment appliquer concrètement cette matrice à travers des exercices de pensée, puis comment décliner les actions de résilience à travers les temps de renforcement progressif.

Chapitre 9

La spirale progressive et intégrative de résilience numérique

Fig. 9.0.1 : La spirale progressive

9.1 Une progression continue vers l'adaptabilité

Annexe La spirale progressive
Découvrir la méthode complète et argumentée pour l'appliquer au quotidien.

La spirale progressive et intégrative structure votre parcours de renforcement de la résilience numérique selon une logique d'accroissement continu. Chaque tour vous place à un niveau supérieur de maturité, de connaissances et de compétences. La progression est continue pendant le parcours de chaque tour, sans saut ni rupture. Vous construisez votre résilience graduellement, en partant des acquis, le point de départ, et en consolidant les apprentissages à chaque étape.

Cette démarche transforme votre organisation en système apprenant : chaque tour devient une opportunité d'apprentissage qui enrichit les tours précédents et suivants. Vous ne répétez pas les mêmes actions, vous les réalisez à un niveau de compréhension et de maîtrise supérieur.

9.2 Trois niveaux de progression

C'est la matrice de criticité qui active cette spirale en structurant le parcours selon une logique de priorité et de progressivité de la zone rouge à la zone verte.

FIG. 9.2.1 : La progressivité

La spirale intègre alors une triple progressivité qui structure votre montée en maturité.

Entre les tours (que nous abordons dans les prochaines sections), vous montez en maturité organisationnelle : vous passez de concepts proches de vos habitudes à des concepts plus radicaux. Cette progression permet d'aborder en douceur des transformations de plus en plus ambitieuses.

Dans chaque tour, vous explorez trois facettes complémentaires de la zone de criticité concernée, liées à des mécanismes différents de fragilisation associés à un ou plusieurs scénarios; elles sont données à titre d'illustration, et sont dépendantes de votre contexte. Ces facettes se renforcent mutuellement et garantissent une vision suffisamment complète des vulnérabilités et des solutions applicables.

Pour chaque facette, vous suivez une progression structurée en six étapes qui guident de l'expérience concrète à l'action opérationnelle :

Exercice de pensée : au travers de quelques questions portant sur des aléas, vous envisagez dans votre contexte comment votre organisation peut réagir.

Mécanisme de fragilisation ou vulnérabilités : pour mieux comprendre le positionnement de l'exercice de pensée, les divers mécanismes concernés sont décrits.

Scénario d'application : afin de contextualiser plus précisément l'exercice de pensée, un ou plusieurs scénarios permettent de se projeter plus aisément.

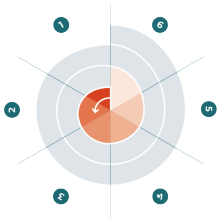
Inspiration : que ce soit dans le numérique ou en dehors, d'autres organisations ont été confrontées à un problème proche ou similaire de celui de l'exercice et ont apporté une solution qui peut être déclinée ou adaptée à votre contexte.

Solutions : des solutions opérationnelles, issues de l'inspiration précédente, sont proposées pour répondre à la problématique induite par l'exercice de pensée.

Bénéfices : l'ensemble des bénéfices sont identifiés de manière collective pour les trois facettes.

9.3 Parcourir la spirale

Tour 1 : Renforcer la zone rouge

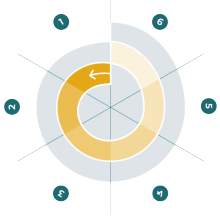


Vous commencez par les processus les plus critiques, ceux dont la défaillance menacerait immédiatement votre pérennité. Les concepts mobilisés que nous vous invitons à déployer restent proches de vos pratiques et de vos habitudes.

Les solutions relèvent de la sécurisation et de la consolidation de l'existant, en ajoutant des couches de protection ou en renforçant les capacités humaines.

Cette approche prudente permet de construire votre confiance méthodologique sur des bases solides avant d'aborder des concepts plus novateurs. Votre zone rouge sera significativement plus résiliente, et vous aurez acquis l'assurance nécessaire pour aborder des transformations plus ambitieuses.

Tour 2 : Optimiser la zone orange



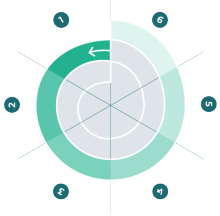
Fort de la maturité acquise au Tour 1, vous explorez maintenant les processus importants, en interrogeant l'utilité réelle de certains outils, en envisageant des alternatives low-tech et en découvrant les blocages qui compliquent les évolutions.

Les concepts mobilisés s'éloignent en partie de vos pratiques et remettent en question certains choix technologiques.

Les solutions relèvent de l'hybridation maîtrisée : conserver le numérique pour l'efficacité, mais construire des alternatives simples pour la résilience.

Ce tour marque un premier tournant dans votre démarche. Vous passez de « Comment mieux protéger mes systèmes ? » à « Ai-je vraiment besoin de ces systèmes sous cette forme ? ».

Tour 3 : Expérimenter dans la zone verte



Les processus les moins critiques deviennent votre laboratoire d'innovation en résilience. Vous pouvez y tester des approches radicales sans risquer la pérennité de votre organisation.

Les concepts mobilisés remettent en question l'impératif technologique en interrogeant la pertinence même de certains choix numériques. Les solutions relèvent de la sobriété numérique délibérée.

Ce tour exige la maturité la plus élevée. C'est aussi le tour le plus libérateur : renoncer au superflu, tout en libérant des ressources pour renforcer l'essentiel.

Poursuivre la spirale : le Tour 4 pour intégrer

La spirale ne s'arrête pas au Tour 3.

Un quatrième tour permet de consolider les apprentissages en appliquant les principes découverts aux tours précédents dans toutes les zones.

Les solutions expérimentées au Tour 3 éclairent d'un jour nouveau votre réflexion sur l'utilité au Tour 2, voire du Tour 1.

Les principes explorés au Tour 2 transforment votre approche de sécurisation de la zone rouge.

Le Tour 4 invite à revisiter les trois zones avec tous les acquis pour passer de la simple compétence à la maîtrise globale.

La matrice évolue avec vous

À chaque tour de la spirale, votre matrice de criticité se transforme. Les processus que vous renforcez deviennent moins dépendants du numérique ou plus résilients face à ses défaillances.

Ce mouvement de progression à travers les quatre tours ne s'arrête jamais. C'est un processus d'amélioration continue qui transforme progressivement votre organisation en système adaptatif. Chaque cycle enrichit le précédent, chaque tour vous place à un niveau supérieur de maturité.

La résilience n'est pas un état à atteindre, c'est une capacité à cultiver. Vous n'êtes jamais « à la fin », mais toujours en progression.

C'est cette capacité d'adaptabilité, bien plus que n'importe quelle technologie, qui fera la différence.

Aller plus loin ?

Après avoir parcouru les quatre tours, vous avez acquis une vision profondément transformée. Les principes que vous avez appliqués au numérique sont universels.

Pourquoi s'arrêter au numérique ?

Chapitre 10

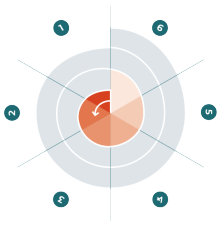
Tour 1 — Renforcer la zone rouge

> *L'interruption d'activité s'est classée au 1er ou au 2e rang de tous les baromètres des risques d'Allianz lors de la dernière décennie… Elle est généralement une conséquence d'événements tels qu'une catastrophe naturelle, une cyberattaque ou une panne.*
>
> **— Allianz Risk Barometer (2025)**

Annexe : Tour 1 détaillé — Sécuriser
Découvrez le Tour 1 dans les détails pour aller plus loin.

Bienvenue dans ce premier tour de la spirale. Il mobilise des concepts proches de vos pratiques actuelles — sécurisation, redondance, simplification — avant d'explorer des approches plus novatrices dans les tours suivants.

Notre fil rouge principal reste l'histoire d'Oseja de Sajambre, ce village espagnol qui a choisi de construire son autonomie énergétique plutôt que de subir les pannes du réseau national. Chaque étape de ce tour rapprochera de cet idéal : devenir votre propre Oseja numérique. Vous allez apprendre à mesurer votre autonomie, à identifier les dépendances critiques, et à construire la résilience progressivement.



Comme nous l'avons établi avec notre boussole, la matrice de criticité, cette première étape est entièrement dédiée à la zone rouge de votre paysage numérique : les services qui sont vitaux pour votre métier et dont la dépendance au numérique est existentielle.

L'objectif de ce tour est d'identifier ces services, et de comprendre les mécanismes profonds qui les rendent fragiles. Pour ce faire, nous allons nous livrer à un exercice de pensée qui évoluera à chaque facette. Pour chacune d'entre elles, nous connecterons cet exercice à des scénarios de crise concrets, nous analyserons les mécanismes de fragilisation sous-jacents. Nous y répondrons par des exemples inspirants, des principes de résilience clairs et des solutions actionnables.

Ce premier tour est votre fondation. Sans lui, tous les efforts d'optimisation et d'expérimentation des tours suivants seraient vains. À quoi bon construire un château de cartes si les fondations s'effondrent ? À quoi bon être une direction visionnaire si votre cœur de métier est à la merci du premier incident technique ?

10.1 Facette 1 : Contre la contagion, la résilience organisée

> *Les disruptions intra-systémiques peuvent se propager d'une partie d'un système à l'ensemble du système via des chaînes causales contagieuses, tandis que les disruptions inter-systémiques débordent des frontières du système vers d'autres systèmes.*
>
> **— Liu & Renn (2025), International Journal of Disaster Risk Science**

Cette première facette explore comment l'interconnexion de nos systèmes crée une fragilité par contagion et comment la résilience organisée permet d'y faire face.

Exercice de pensée : l'interruption de 24 heures

L'exercice consiste à identifier les 5 à 10 services numériques dont l'arrêt pendant 24 heures paralyserait votre activité principale. La méthode est simple : partez de votre processus métier principal (ex. : la production), remontez la chaîne vers les systèmes qui le supportent (ERP, CRM), puis descendez dans le détail des sous-systèmes critiques (base de données, authentification).

Cet exercice simple esquisse la carte de votre zone rouge et force à quantifier concrètement l'impact d'une panne au-delà de la simple remarque « On ne sait pas réellement, mais ce doit être grave ».

Mécanisme de fragilisation : Mécanismes de contagion et ambiguïté des interdépendances

Annexe Mécanismes et scénarios
Toutes les vulnérabilités et les scénarios utilisés pour les tours un à trois sont issus de l'annexe qui les détaille et les argumente.

Nos systèmes sont devenus si complexes et interconnectés que personne ne les maîtrise entièrement. Une défaillance chez un fournisseur de rang 3 peut, par un effet domino, paralyser vos propres opérations.

Le problème n'est plus la panne d'un service, mais la contagion à tout l'écosystème à travers des dépendances invisibles. Cette contagion opère sur trois vecteurs : technique (une base de données corrompue), organisationnel (la panique d'une équipe en cas de crise) et économique (la perte d'un fournisseur critique).

Scénario à envisager : La mégapanne systémique par bug ou cyberattaque

Ce risque n'est pas théorique. En juillet 2024, une mise à jour défectueuse du logiciel de sécurité CrowdStrike a paralysé 8,5 millions de machines dans le monde, clouant au sol des avions et reportant des actes chirurgicaux.

En 2017, le logiciel malveillant NotPetya, initialement ciblé sur l'Ukraine, a coûté plus de 300 millions de dollars au transporteur Maersk en paralysant 76 de ses ports. Dans les deux cas,

une cause semble-t-il mineure dans un système hyperconnecté a entraîné une catastrophe mondiale par contagion.

Inspiration : Wellington et l'anticipation des chocs systémiques

> Annexe Exemples inspirants
> Toutes les inspirations utilisées pour les tours un à trois sont issues de l'annexe qui les détaille et les argumente.

Face à un risque qui affecte tout le système, l'inspiration vient de Wellington. Construite sur une faille sismique, la capitale de la Nouvelle-Zélande ne cherche pas à empêcher l'effondrement, mais à garantir le fonctionnement de la société malgré le chaos.

Le Resilient Cities Network [24] documente leur stratégie de résilience organisée, qui impose de construire une robustesse systémique par la redondance (77 points d'accès communautaires autonomes en eau), la diversification (communications radio et satellite), la modularité (chaque quartier a un plan d'autonomie de 72 h) et des tests réguliers.

Solutions : construire votre autonomie

Pour appliquer cette leçon, il faut commencer à mesurer et à construire son autonomie. Les actions clés incluent :

Cartographier les interdépendances pour visualiser la chaîne de fragilité.

Éliminer chaque Point de défaillance unique (Single Point of Failure / SPOF), comme une dépendance à un seul opérateur, un seul système d'exploitation…

Évoluer de la redondance à la sur-redondance adaptée : pour les services de la zone rouge qui ne peuvent pas être traités par le principe de non-régression, la redondance classique ne suffit plus; face à la polycrise (pannes longues, ruptures d'approvisionnement, événements extrêmes), il faut viser une sur-redondance adaptée au contexte, trois sites au lieu de deux par exemple.

Adopter une architecture hybride, en rapatriant les services les plus vitaux sur des infrastructures maîtrisées (cloud privé ou serveurs locaux).

Définir le seuil d'autonomie (métrique Oseja n°1) : le niveau de service minimum acceptable en cas de crise. C'est le socle sur lequel repose votre continuité d'activité.

Mesurer le temps de bascule (métrique Oseja n°2) : le temps requis pour activer la solution de secours. L'objectif est, par exemple et à adapter selon votre contexte, de le réduire de plusieurs heures à quelques minutes via des exercices trimestriels.

10.2 Facette 2 : Contre le verrouillage, la non-régression

Cette facette explore comment nos choix technologiques passés nous enferment dans des dépendances critiques et comment le principe de non-régression permet de regagner sa liberté.

Exercice de pensée : l'audit de dépendance au fournisseur

Pour chaque service de votre zone rouge, menez un audit de dépendance. Évaluez chaque service sur son fournisseur principal, l'existence d'une alternative réaliste à court terme (moins de six mois), le coût et le délai de migration, et la présence de compétences internes pour opérer sans le fournisseur.

Une autre question importante à se poser est de savoir si ce fournisseur a fait ce même exercice de pensée. Le résultat est un score de verrouillage de 0 (libre) à 10 (prisonnier), qui révèle une vérité inconfortable : pour nos services vitaux, nous sommes souvent devenus des locataires, et non des propriétaires.

Mécanisme de fragilisation : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)

Ce sentiment d'être piégé est le symptôme du verrouillage socio-technique. Les choix technologiques passés, généralement pour des raisons de coût ou de commodité, nous ont enfermés dans des écosystèmes propriétaires.

Ce phénomène de Dépendance au sentier (Path Dependency) se déroule en cinq étapes : Adoption → Intégration → Dépendance → Atrophie des compétences alternatives → Captivité, où changer coûterait trop cher, impliquerait trop de ressources, affecterait trop d'habitudes.

Scénario à envisager : La rupture géopolitique

> *Pour la troisième année consécutive, le changement climatique, l'instabilité géopolitique et la cybersécurité arrivent en tête des préoccupations exprimées par les experts.*
>
> **— AXA Future Risks Report (2024)**

Le verrouillage devient une menace existentielle face à une rupture géopolitique. En 2022, à la suite de l'invasion de l'Ukraine, de nombreuses entreprises russes ont été coupées des services cloud occidentaux (AWS, Azure), paralysant leur activité. Plus subtilement, l'inondation de la mine de Spruce Pine en 2024, quasi unique source mondiale d'un quartz ultra-pur, a mis en péril toute l'industrie des semi-conducteurs ; cela démontre qu'une dépendance invisible à une source unique peut paralyser une chaîne de valeur mondiale.

Inspiration : Les maisons flottantes des Tausug et la conception pour la réparation

Pour lutter contre le verrouillage, cultivez les alternatives. L'inspiration vient des Tausug des Philippines. Comme le documente BBC Future [25], ils construisent des maisons sur pilotis flexibles, avec des matériaux locaux, que tout le monde sait réparer.

Leur principe : concevoir pour la réparation plutôt que pour la perfection. C'est l'incarnation du principe de non-régression : la technologie doit être une aide qui augmente les capacités, non un substitut qui les remplace. Si la technologie disparaît, l'organisation doit pouvoir continuer à fonctionner.

Solutions : augmenter votre indépendance

Appliquer ce principe augmente l'autonomie et réduit le verrouillage. Les actions clés incluent :

Maintenir et exercer les compétences manuelles en organisant des « journées Tausug » où l'on simule une panne et réinvente les processus papier.

Privilégier les solutions ouvertes et interopérables en faisant de la réversibilité un critère de choix aussi important que le prix.

Développer une stratégie multi-fournisseurs ex. : 70 % sur un cloud principal, 20 % sur un cloud de secours, 10 % en local pour le plus sensible, selon la criticité de l'application et sa capacité à être reprise hors numérique

Mesurer le taux d'autonomie (métrique Oseja n°3) : le pourcentage des opérations critiques que vous pouvez maintenir sans services externes. L'objectif est de faire progresser ce taux dans le temps.

10.3 Facette 3 : Contre la complexité, la sobriété intelligente

Cette dernière facette s'attaque à une cause profonde de notre fragilité : notre quête d'efficacité qui, paradoxalement, engendre une complexité dangereuse.

Exercice de pensée : l'audit de complexité

Choisissez le service le plus critique de votre zone rouge et auditez sa complexité sur quatre dimensions. Fonctionnelle : combien de fonctionnalités sont réellement utilisées ? Technique : combien de systèmes externes y sont connectés ? Humaine : combien de personnes comprennent concrètement son fonctionnement ? Économique : quel est le coût de cette complexité (licences, maintenance) ?

Mécanisme de fragilisation : Fragilités techniques et complexité systémique

> *La course au progrès technologique et à l'efficacité affecte la résilience des chaînes d'approvisionnement. De nos jours, une défaillance ou une perturbation dans un maillon quelconque tend à avoir des conséquences plus graves, laissant un temps de réaction minimal.*
>
> **— Michael Bruch, Allianz (2025)**

Les systèmes informatiques qui font tourner votre entreprise sont devenus si complexes que plus personne ne les maîtrise entièrement. Cette complexité exponentielle, ou « dette technique », est une bombe à retardement.

Elle est souvent le résultat du paradoxe de Jevons : les gains d'efficacité nous encouragent à créer des services plus consommateurs, à stocker plus de données et à ajouter plus de fonctionnalités, faisant ainsi exploser la complexité et la fragilité.

Scénario à envisager : L'effondrement climatique en cascade

Cette fragilité se révèle brutalement face à une crise physique. Imaginez une canicule extrême (une des manifestations de l'effondrement climatique en cascade) forçant des restrictions d'électricité ou des défaillances de climatisation : les datacenters, très voraces, sont les premiers touchés.

Les services « efficaces » mais complexes deviennent un passif. L'entreprise qui a simplifié son ERP à peu de fonctionnalités essentielles peut continuer à opérer, tandis que celle qui en a beaucoup trop est à l'arrêt, car son système est trop gourmand pour les ressources disponibles. La question n'est plus simplement « pouvons-nous le faire tourner ? » mais « en avons-nous les moyens en toutes circonstances ? ».

Inspiration : L'Égypte et les barrières de roseaux et les solutions simples pour problèmes complexes

Face à la complexité, l'inspiration vient de solutions frugales. Le PNUD documente comment, face à l'érosion côtière, des communautés égyptiennes ont redécouvert une technique millénaire : les barrières de roseaux [26]. La leçon est claire : les solutions les plus robustes ne sont pas nécessairement les plus sophistiquées.

Un système de sauvegarde sur bandes magnétiques, technologie des années 1960, reste imbattable pour l'archivage. Une documentation papier garantit la continuité en cas de panne totale. C'est le principe de simplicité stratégique.

Solutions : viser la sobriété et la durée

Pour réduire la complexité, il faut viser la sobriété. Les actions clés incluent :

Auditer la valeur par fonctionnalité pour identifier et supprimer les fonctionnalités « zombies » qui ne sont jamais utilisées, mais consomment des ressources et sont source de vulnérabilités.

Créer des « budgets complexité » pour chaque nouveau projet, afin de refuser ou simplifier tout projet qui ajoute trop de dépendances ou de maintenance.

Développer une « architecture de sobriété » en privilégiant les technologies matures et éprouvées et en concevant chaque système pour être facilement remplaçable.

Maximiser la durée d'autonomie (métrique Oseja n° 4) : le temps pendant lequel vous pouvez maintenir votre seuil d'autonomie sans aucune aide extérieure. L'objectif est de l'augmenter pour vous éloigner de la durée maximale d'interruption ou de service dégradé.

10.4 Conclusion du tour 1 : vous êtes un peu plus Oseja

Ce premier tour est terminé. Vous avez identifié votre zone rouge, compris trois mécanismes qui la fragilisent, et vous disposez désormais de quatre métriques claires pour piloter votre résilience :

1. Seuil d'autonomie (métrique Oseja n° 1) : le niveau de service minimum acceptable en cas de crise.
2. Temps de bascule (métrique Oseja n° 2) : le délai pour activer les solutions de secours.
3. Taux d'autonomie (métrique Oseja n° 3) : le pourcentage d'opérations critiques maintenables sans services externes.
4. Durée d'autonomie (métrique Oseja n° 4) : le temps pendant lequel vous pouvez tenir en autonomie complète.

Bénéfices de ce premier tour

Au-delà de l'identification des services vitaux et de la compréhension des mécanismes de fragilisation, ce parcours apporte des bénéfices essentiels. Il crée une prise de conscience collective de la criticité réelle de vos services et favorise un alignement des équipes sur les priorités métier ; c'est un changement important et l'accompagnement des équipes avec une gouvernance adaptée est nécessaire pour obtenir leur adhésion.

Ce processus initie un changement de perspective fondamental, faisant passer de la simple quête d'efficacité à une véritable stratégie de robustesse, ce qui permet de justifier les investissements requis. En vous préparant mentalement aux chocs imprévisibles, il vous dote d'un cadre de décision pour intégrer de nouvelles technologies et se concrétise par un plan d'action mesurable pour les mois à venir.

Indirectement, la mise en place d'une stratégie de diversification des fournisseurs vous renforce par rapport au phénomène du « vendor locking » (verrouillage à un fournisseur) ; un exemple marquant de ce phénomène est le rachat de VMware par Broadcom [27] et la politique tarifaire chamboulée qui s'en est suivie.

Impact des principes sur la matrice de criticité

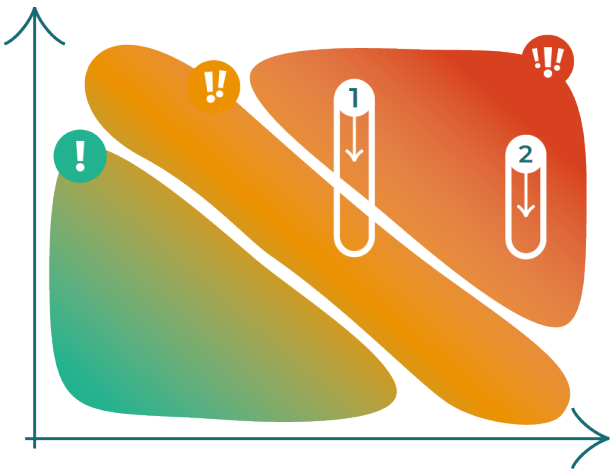


Fig. 10.4.1 : Évolution de la matrice au Tour 1

L'objectif de ce renforcement est de faire évoluer les services de la zone Rouge vers une zone de criticité plus faible (cas n° 1) ou maîtrisée (cas n° 2). Les deux principes directeurs de ce tour y contribuent de manière complémentaire.

Le principe de non-régression agit directement sur la dépendance au numérique. En définissant des processus de secours manuels comme complément ou alternative, un service reste ainsi fonctionnel même en cas de panne, faisant décroître sa dépendance. De plus, en concevant des systèmes réversibles et en privilégiant la sobriété, le risque d'être prisonnier d'une technologie se réduit et la probabilité de défaillances complexes diminue, ce qui abaisse encore la criticité globale.

Le principe de résilience organisée, quant à lui, sécurise les services qui restent dans la zone rouge. Il agit sur la probabilité et la gravité d'une défaillance. En éliminant chaque Point de défaillance unique (Single Point of Failure / SPOF) par la redondance et la diversification, une panne totale devient beaucoup moins probable. En définissant un seuil d'autonomie grâce à la modularité, l'impact d'une panne n'est plus une paralysie, mais une dégradation de service, ce qui en réduit la gravité. Enfin, en testant et en réduisant le temps de bascule, la durée de l'interruption se réduit. Ce principe transforme la zone rouge d'un périmètre de danger imminent à une zone de criticité maîtrisée.

Poursuivons vers le Tour 2

Vous êtes un peu plus comme Oseja. Vous avez appris à mesurer votre autonomie, à identifier les dépendances critiques, et à simplifier les systèmes pour les rendre plus robustes. Comme Oseja a d'abord sécurisé son approvisionnement énergétique avant d'optimiser sa distribution, vous avez sécurisé votre cœur de métier. Ainsi, vous disposez de fondations solides pour continuer à construire.

Le Tour 2 amènera à questionner plus profondément vos choix technologiques, fort de la confiance méthodologique acquise ici.

Le voyage continue. Direction la zone orange et la performance durable.

---

[24] Resilient Cities Network. *Building Wellington's Resilient Community Water Access*. 2020. URL : https://resilientcitiesnetwork.org/wellington-water-security/.

[25] BBC. *Floating bamboo houses keep this indigenous tribe safe*. 2024. URL : https://www.bbc.com/future/article/20240531-the-floating-houses-built-to-withstand-typhoons-and-flooding-in-the-philippines.

[26] United Nations Development Program. *Learning from local ingenuity – how simple reed fencing has unlocked a solution to rising sea levels in Egypt*. 2022. URL : https://www.undp.org/arab-states/blog/learning-local-ingenuity-how-simple-reed-fencing-has-unlocked-solution-rising-sea-levels-egypt/.

[27] LeMagIT. *L'affaire Broadcom VMware : le guide pour comprendre*. 2025. URL : https://www.lemagit.fr/essentialguide/Laffaire-Broadcom-VMware.

Chapitre 11

Tour 2 — Optimiser la zone orange

> *La résilience nourrit essentiellement la capacité individuelle et collective de créer ou de reconstruire de manière créative des vies valables dans des contextes changeants.*
>
> **— OPHIR, Oxford University (2025)**

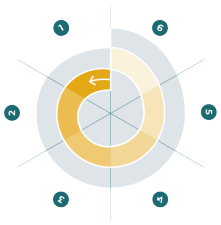
Annexe Tour 2 détaillé — Optimiser
Découvrez le Tour 2 dans les détails pour aller plus loin.

Bienvenue dans le deuxième tour de notre spirale. Dans le Tour 1, nous avons affronté les risques les plus critiques en sécurisant votre zone rouge.

Vous avez appris à protéger le cœur vital de votre organisation et commencé à mesurer votre autonomie avec les métriques Oseja.

Ce tour est dédié à la zone orange : les services qui sont importants pour votre activité, sans être existentiels, et qui ont une forte dépendance au numérique. La notion de dette technique nous a laissé avec une question fondamentale à la fin du Tour 1 : à quoi bon rendre un service robuste s'il est inutile ou trop complexe ?

La quête de simplicité nous incite maintenant à aller plus loin. L'enjeu de ce tour n'est pas seulement d'optimiser, mais de construire une performance durable, en nous assurant que chaque brique de notre système d'information a une réelle pertinence.



Comme Oseja, nous allons apprendre à construire notre autonomie numérique : élaguer le superflu, reconstruire intelligemment et nous inspirer de modèles qui ont déjà prouvé que la robustesse est un avantage concurrentiel.

Pour construire cette performance durable, nous allons explorer trois dimensions complémentaires. D'abord, nous questionnerons l'utilité réelle de nos services numériques : à quoi bon maintenir ce qui ne sert plus ? Ensuite, nous prolongerons la durée de vie de notre matériel pour réduire notre dépendance aux chaînes d'approvisionnement mondiales. Enfin, nous transformerons notre rapport à la panne : au lieu de la craindre, nous apprendrons à nous y entraîner pour devenir plus forts.

Ces trois facettes forment un tout cohérent : la sobriété (éliminer l'inutile), la durabilité (prolonger ce qui est utile) et l'antifragilité (se renforcer par l'épreuve). Pour nous guider, nous nous appuierons sur les concepts des 3U (Utile, Utilisable, Utilisé) [28] et des 5R (Refuser, Réduire, Réemployer, Réparer, Recycler) [29].

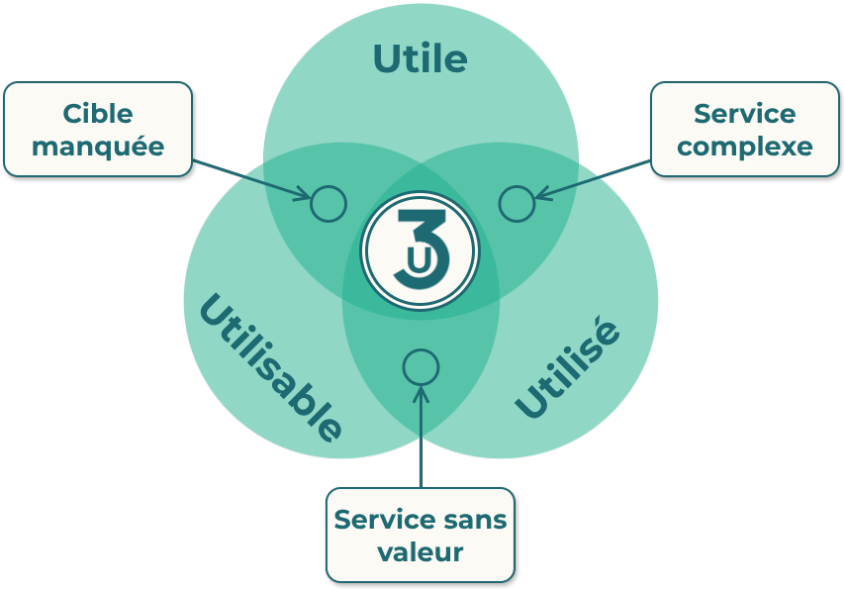


FIG. 11.0.1 : Les 3U

FIG. 11.0.2 : Les 5R

11.1 Facette 4 : Contre l'inutilité, la pertinence

Cette première facette s'attaque à une fragilité coûteuse : la complexité et l'inutilité accumulées au fil du temps.

Exercice de pensée : le test de la justification

Prenez un service important de votre zone orange, idéalement un service qui existe depuis quelques années. Imaginez devoir justifier le budget pour l'année prochaine devant un comité de direction qui ne connaît rien à la technique et répondez à ces questions :

- Quel est le bénéfice métier concret et chiffré de ce service aujourd'hui ?
- Si on arrêtait ce service demain, quel serait l'impact réel sur l'activité ?
- Existe-t-il une alternative plus simple ou moins coûteuse qui pourrait rendre 80 % du même service ?

Cet exercice nous force à sortir de nos habitudes et à nous demander si nous conservons ce service parce qu'il est encore pertinent, ou simplement parce qu'« on a toujours fait ainsi ».

Mécanisme de fragilisation : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)

> *Les géants de la tech – un risque de dépendance.*
>
> **— Swiss Re SONAR 2024 (p.26)**

Annexe Mécanismes et scénarios
Toutes les vulnérabilités et les scénarios utilisés pour les tours un à trois sont issus de l'annexe qui les détaille et les argumente.

Pourquoi est-il si difficile de se défaire d'un service inutile ?

C'est le mécanisme Verrouillages socio-techniques et Dépendance au sentier (Path Dependency) qui entre en jeu.

Les choix technologiques que nous avons faits par le passé, souvent pour des raisons de coût ou de commodité, nous ont enfermés dans des écosystèmes dont il est aujourd'hui extrêmement coûteux, voire impossible, de sortir.

Nous conservons ces outils non pas parce qu'ils sont les meilleurs, mais par simple habitude ou parce que les coûts de migration semblent trop élevés. Ce verrouillage nous empêche d'adopter des solutions plus simples et plus efficaces, et nous fait perdre de vue la question essentielle : ce service est-il encore utile ?

Scénario à envisager : La crise de confiance généralisée

Ce risque est parfaitement illustré par le scénario La crise de confiance généralisée. À force de proposer des services qui ne répondent plus aux besoins réels des personnes utilisatrices, qui sont trop complexes ou perçus comme des outils de surveillance, les organisations créent une rupture de confiance.

En interne, les personnes se détournent des outils officiels au profit du "shadow IT" ; en externe, elles se méfient des services qu'on leur propose, et l'entreprise perd sa Licence sociale d'opérer. La crise de confiance n'est pas seulement externe, elle est donc aussi interne : quand les équipes ne croient plus à la pertinence de leurs propres outils, la performance s'effondre.

Inspiration : L'Égypte et les barrières de roseauxx et la philosophie low-tech

> Annexe Exemples inspirants
> Toutes les inspirations utilisées pour les tours un à trois sont issues de l'annexe qui les détaille et les argumente.

Face au piège de la sur-ingénierie, l'inspiration nous vient d'Égypte [26]. Pour lutter contre l'érosion côtière du delta du Nil, au lieu de construire des digues en béton coûteuses et complexes, les communautés locales ont réutilisé une technique millénaire : des barrières de roseaux plantées le long de la côte. Cette solution, d'un coût dérisoire et utilisant des matériaux locaux, s'est avérée plus efficace et durable que les solutions technologiques modernes. De plus, sa simplicité permet une gestion locale avec des savoirs qui perdurent facilement dans le temps.

> Annexe La low-tech

Cet exemple illustre parfaitement la philosophie low-tech. Il ne s'agit pas d'un retour en arrière, mais d'une démarche d'ingénierie qui vise à répondre à un besoin avec la solution la plus simple, la plus durable et la plus maîtrisable possible. C'est une extension technique du principe de non-régression : ne substituons pas un processus simple qui fonctionne (même s'il est manuel) par une technologie complexe qui ne sera pas adoptée.

La simplicité n'est pas l'ennemie de la performance. C'est la condition de son adoption et donc de sa pertinence. Un outil simple et maîtrisé sera toujours plus performant qu'un outil surpuissant et délaissé.

Solutions : améliorer votre score de pertinence

1. Menez un audit 3U (Utile, Utilisable, Utilisé) : utilisez l'audit 3U comme un outil concret pour mesurer la pertinence de vos services. Créez un comité d'utilisateurs pour évaluer régulièrement votre parc applicatif.

   Utile : le service répond-il à un besoin métier réel et stratégique ?

   Utilisable : le service est-il simple, intuitif et agréable à utiliser ?

   Utilisé : le service est-il réellement adopté par les équipes ou les internautes, serait-il contourné ?

2. Adoptez une politique de « simplification d'abord » (inspirée des 5R) : avant tout projet d'optimisation ou de migration, essayez d'appliquer les deux premiers R :

   Refuser : refusez d'ajouter un nouveau service si le besoin n'est pas explicitement démontré.

   Réduire : éliminez les fonctionnalités peu utiles, voire inutiles, simplifiez les interfaces.

3. Poursuivez cette politique de simplification avec la low-tech : identifiez systématiquement les solutions de type low-tech qui peuvent se mettre en place et établissez une comparaison risques/opportunités entre une solution high-tech et son pendant low-tech.

4. Utilisez des outils d'évaluation complémentaires : pour aller plus loin, vous pouvez vous inspirer de concepts comme erooM [30] (EROOM Optimization Framework) de Boavizta [31], qui propose une grille d'évaluation détaillée de la pertinence et de l'efficacité des services numériques.

5. Mesurez votre « efficacité de pertinence » (métrique Oseja n° 5) ; créez une nouvelle métrique : le ratio entre le coût total de possession d'un service et son score 3U. L'objectif est d'augmenter cette métrique, soit en réduisant les coûts, soit en améliorant la pertinence.

6. Suivez votre « taux de services utiles » (métrique Oseja n° 8) : mesurez le pourcentage de services de la zone orange ayant un score 3U supérieur ou égal à 12. Un taux inférieur à 70 % indique une accumulation de services peu pertinents.

7. Calculez votre « dividende de simplicité » (métrique Oseja n° 9) : mesurez l'économie annuelle réalisée grâce au décommissionnement des services inutiles, exprimée en pourcentage du budget IT. Un dividende de 5 à 10 % est un bon résultat pour une première vague de simplification.

Maintenant que nous avons radicalement diminué l'inutile, il est temps de nous assurer que ce qui reste dure le plus longtemps possible. Car la simplicité sans durabilité n'est qu'une illusion de sobriété.

11.2 Facette 5 : Contre l'obsolescence, la durabilité

Cette facette explore comment notre quête d'efficacité nous a rendus dépendants de chaînes d'approvisionnement fragiles et comment la durabilité permet de regagner notre autonomie matérielle.

Exercice de pensée : le test de la chaîne d'approvisionnement

Prenez un service important de votre zone orange et répondez à ces questions :

- Sur quel type de matériel ce service fonctionne-t-il ?
- Si vous deviez commander 100 nouveaux ordinateurs ou 10 nouveaux serveurs aujourd'hui, quel serait le délai de livraison réaliste ?
- Savez-vous où sont fabriqués les composants clés de ce matériel et quels sont les risques associés à ces lieux ?
- Si un composant essentiel devenait indisponible pendant six mois, quel serait l'impact ?
- Combien d'équipements « dormants » (réformés mais fonctionnels) possédez-vous ?

Cet exercice nous force à voir au-delà du « cloud » et à reconnaître que nos services immatériels reposent sur une infrastructure très matérielle, et donc très vulnérable.

Mécanisme de fragilisation : la double dépendance physique et géopolitique

> *Au-delà des infrastructures défaillantes – les effets en cascade des catastrophes naturelles.*
>
> **— Swiss Re SONAR 2024**

L'illusion d'un numérique infini et toujours disponible masque deux mécanismes de fragilisation critiques :

- Fragilités géopolitiques : la fabrication des composants et la fourniture de services type SaaS sont une carte de tensions mondiales. Un conflit ou un embargo peut instantanément couper votre approvisionnement.
- Fragilités physiques/climatiques face à l'incertitude environnementale : votre matériel dépend de chaînes logistiques longues et de ressources (énergie, eau) qui sont sous pression.

Scénario à envisager : la rupture de la chaîne d'approvisionnement

Ce risque est parfaitement illustré par le scénario La rupture géopolitique. L'incident de la mine de Spruce Pine (Tour 1) nous a montré comment une source unique de matière première peut paralyser une industrie. Pour la zone orange, l'impact peut être plus insidieux : dégradation de la performance, baisse de la sécurité, perte d'innovation.

Inspiration : Infomaniak, Fairphone et la « Mine urbaine »

Comment contrer cette fragilité ? En changeant radicalement de paradigme : passer de la consommation effrénée à la gestion intelligente de nos actifs.

L'inspiration nous vient de deux acteurs qui ont prouvé que la durabilité est une stratégie de résilience. Infomaniak, hébergeur suisse, prolonge la durée de vie de ses serveurs jusqu'à 15 ans en choisissant du matériel évolutif et réparable, et en optimisant ses logiciels. Fairphone a conçu un smartphone modulaire et réparable qui dure deux fois plus longtemps qu'un smartphone classique.

Ces deux exemples incarnent le principe de sobriété intelligente : la durabilité n'est pas l'ennemie de la performance, mais l'alliée de la robustesse. Cette philosophie mène à une solution concrète pour votre organisation : la « Digital Enterprise Mine », fondée sur le principe de la Mine urbaine (urban mine) [32].

Solutions : construire votre autonomie matérielle

Adoptez une stratégie de durabilité matérielle (inspirée des 5R) : appliquez les trois derniers R à votre gestion de parc :

Réemployer : créez un circuit de réemploi des matériels en fonction des besoins cibles.

Réparer : formez vos équipes à la réparation, ayez des fournisseurs locaux, et faites de l'indice de réparabilité un critère d'achat.

Recycler : mettez en place une filière locale de recyclage pour les composants non réutilisables.

Allongez la durée de vie des actifs : remettez en question les cycles de renouvellement systématiques. Un audit technique révélera souvent que de nombreux équipements peuvent fonctionner pendant cinq, voire sept ans, parfois en changeant la destination d'usage.

Construisez votre « Digital Enterprise Mine » : créer votre propre stock tampon, réparti avec vos fournisseurs, avec le matériel existant en créant votre « Digital Enterprise Mine » ; vous pouvez commencer avec le matériel que vous aurez récupéré des fonctions inutiles ou de la mise en œuvre d'alternatives low-tech ou en identifiant les trois composants qui tombent le plus souvent en panne et en mettant en place un premier stock de ces pièces.

Mesurez votre « taux de circularité » (métrique Oseja n° 6) : créez une nouvelle métrique : le pourcentage de vos besoins en composants qui peuvent être satisfaits par votre mine interne.

Suivez la « durée de vie moyenne du matériel » (métrique Oseja n° 10) : mesurez la durée de vie réelle moyenne des équipements, de l'achat à la réforme. Une durée de vie moyenne inférieure à trois ans pour les smartphones, à quatre ans pour les postes de travail ou six ans pour les serveurs indique un renouvellement trop rapide.

Mesurez votre « taux d'autonomie matérielle » (métrique Oseja n° 11) : calculez le pourcentage de vos besoins en remplacement/réparation qui peuvent être satisfaits par votre Digital Enterprise Mine. Un taux de 20 à 30 % est un excellent résultat pour une Mine en phase de démarrage.

Nous avons appris à éliminer l'inutile et à prolonger l'utile. Mais même les systèmes les plus simples et les plus durables finiront par tomber en panne. La question n'est pas de savoir si cela arrivera, mais quand. Surtout : serons-nous prêts ?

11.3 Facette 6 : Contre la fragilité, l'antifragilité

Cette dernière facette s'attaque à une croyance profondément ancrée dans la culture informatique : la quête de la perfection et du « zéro défaut ».

Exercice de pensée : le scénario de la panne inattendue

Reprenez un service de votre zone orange. Imaginez le scénario suivant : demain, à 10 h du matin, ce service tombe en panne. La cause est inconnue et répondez à ces questions :

- En combien de temps la panne sera-t-elle détectée (que dit votre expérience sur le sujet) ? Qui sera alerté, et comment ?
- Quelle est la première personne à appeler ? Est-ce que cette personne est la seule à pouvoir agir ?
- La procédure de diagnostic et de restauration est-elle documentée ?
- Est-ce que cette procédure a déjà été testée « à blanc » ? En conditions réelles ?
- Pensez-vous que l'ensemble de vos fournisseurs de services ou de biens ont aussi réfléchi à ces sujets ? Les accompagnez-vous dans cette démarche ?

Cet exercice révèle parfois, souvent, que nos plans de continuité d'activité sont des documents qui dorment dans un tiroir.

Mécanisme de fragilisation : la complexité systémique et la contagion

La croyance dans la perfection de nos systèmes nous conduit à une fragilité majeure : nous ne nous préparons pas à l'échec. Ce mécanisme combine deux aspects :

- Fragilités techniques et complexité systémique : les systèmes informatiques qui font tourner votre entreprise sont devenus si complexes que plus personne ne les maîtrise entièrement. Cette complexité exponentielle crée un nouveau type de risque : la panne systémique.
- Mécanismes de contagion et ambiguïté des interdépendances : une faille chez un fournisseur de rang 3 peut, par un effet domino, paralyser vos propres opérations. Chaque Point de défaillance unique (Single Point of Failure / SPOF) est souvent masqué dans la complexité des réseaux modernes.

Scénario à envisager : La mégapanne systémique par bug ou cyberattaque

Ce risque est parfaitement illustré par le scénario La mégapanne systémique par bug ou cyberattaque. L'incident CrowdStrike (2024) en est une parfaite illustration : un simple bug dans un logiciel de sécurité a provoqué une panne mondiale massive, affectant des milliers d'entreprises sur toute leur chaîne numérique, impliquant en interne pour la continuité de nombreux acteurs sur un périmètre désiloté.

Inspiration : l'« ingénierie du chaos » et l'antifragilité

Comment se préparer à l'inévitable ? En rendant la panne banale. C'est la philosophie révolutionnaire de l'« ingénierie du chaos » (chaos engineering), popularisée par Netflix avec son outil « Chaos Monkey ». Le principe est simple : un programme parcourt l'infrastructure et éteint délibérément des serveurs au hasard, en pleine journée de production.

Nul besoin d'être Netflix pour appliquer ce principe. Selon votre taille, votre maturité, votre contexte, l'équivalent peut être aussi simple qu'un exercice trimestriel où vous éteignez manuellement et de manière aléatoire un serveur non critique, ou vous simulez la panne d'un service pendant une heure. L'important n'est pas l'automatisation, mais la régularité et l'imprévisibilité de l'exercice.

L'objectif n'est pas de créer le chaos, mais de forcer les équipes à construire des systèmes résilients par conception. C'est une application directe du concept d'antifragilité de Nassim Nicholas Taleb : un système antifragile n'est pas seulement robuste, il se bonifie avec les chocs.

Solutions : de l'incertitude de la panne à l'entraînement à la panne

> *L'approche de stress-testing de la résilience des infrastructures dépasse le stress-testing mono-problème pour un stress-testing systémique tenant compte de l'interconnexion entre systèmes.*
>
> **— Nature Communications (2025)**

Instaurez les « journées de la panne » (Game Days) : une fois par trimestre, réunissez les équipes techniques et métier et simulez un scénario de crise et capitalisez sur les dernières pannes subies ou déclenchées.

Développez une culture de la transparence post-mortem : après chaque incident, organisez une revue « post-mortem » dont l'objectif n'est bien évidemment pas de trouver un coupable, mais de comprendre les causes profondes et d'identifier les solutions, et ainsi se préparer pour la prochaine occurrence.

Automatisez la résilience : votre « chaos monkey » personnel : commencez à automatiser/régulariser les tests de résilience (bascule sur le site de secours, validité des sauvegardes, etc.) et testez des pannes aléatoires sur les services les moins critiques de votre zone orange, puis capitalisez pour inclure tous vos services de la zone orange.

Introduisez le concept d'« hormèse » numérique [33] : de petites pannes contrôlées renforcent progressivement votre résilience globale.

Mesurez votre « temps de récupération moyen » (MTTR) (métrique Oseja n° 7) ; créez une métrique clé : le temps moyen entre la détection d'une panne et le retour à la normale.

11.4 Conclusion du Tour 2 : de la construction à la transformation

Ce deuxième tour est terminé. Nous avons appris à questionner l'utilité de nos services, la durabilité de notre matériel et notre rapport à la panne. Nous avons vu que pour construire une performance durable dans la zone orange, il faut appliquer les principes de simplicité, de durabilité et d'antifragilité.

Synthèse des bénéfices

Au terme de ce tour, votre organisation a non seulement optimisé sa zone orange, mais elle a aussi profondément changé sa culture. Les bénéfices sont quantitatifs et qualitatifs.

Vous avez réalisé des économies substantielles en éliminant les services inutiles et en prolongeant la durée de vie de votre matériel. Vous avez gagné en autonomie matérielle en construisant votre « Digital Enterprise Mine », ce qui vous rend moins vulnérable aux ruptures d'approvisionnement. Mais, surtout, vous avez développé une culture de l'antifragilité : vos équipes ne craignent plus la panne, elles s'entraînent à y faire face, ce qui augmente leur confiance et leur proactivité, et diminue le stress en situation de crise. Le chaos est devenu un allié, et chaque incident est une opportunité d'apprentissage. Comme en Chine, la crise devient naturellement dans l'ordre des choses : les deux idéogrammes utilisés, Wei et Ji, signifient le danger (Wei) et l'opportunité (Ji), car les deux vont ensemble et selon le contexte l'un prime l'autre.

Impact des principes sur la durabilité

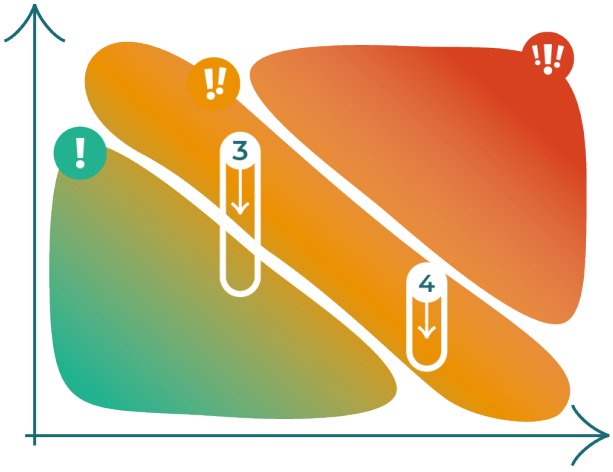


Fig. 11.4.1 : Évolution de la matrice au Tour 2

Les trois principes de ce tour agissent en synergie pour maintenir la performance réellement nécessaire, mais aussi construire la durabilité et la robustesse.

- Le principe de simplicité (facette 4) a un impact direct sur la charge cognitive de vos équipes et sur vos coûts de maintenance.
    - En éliminant le superflu, vous libérez des ressources mentales et financières qui peuvent être réinvesties dans l'innovation. Vous réduisez également votre surface d'attaque en supprimant les applications « zombies » qui sont autant de portes d'entrée potentielles pour des menaces.
    - Vous faites descendre certains services de la zone orange vers la zone verte (cas n°3). Ces services, considérés comme « importants » par habitude, se révèlent finalement moins critiques qu'on ne le pensait. L'audit 3U permet d'identifier ces services et de les traiter avec un niveau d'exigence moindre.
- Le principe de durabilité (facette 5) agit sur votre dépendance aux chaînes d'approvisionnement mondiales.
    - En concevant les systèmes pour qu'ils soient réparables et en gérant les actifs matériels comme une ressource stratégique, vous transformez une contrainte en une opportunité. Votre organisation devient moins fragile face aux chocs géopolitiques et environnementaux.
    - En prolongeant la durée de vie de votre matériel et en construisant votre Digital Enterprise Mine, vous ne faites pas sortir les services de la zone orange, mais vous réduisez leur vulnérabilité face aux ruptures d'approvisionnement (cas n° 4). Sur la matrice, cela se traduit par une réduction de la gravité de l'impact en cas de crise géopolitique ou climatique.
- Le principe d'antifragilité (facette 6) transforme radicalement votre rapport à l'échec.
    - Au lieu de viser une perfection illusoire, vous acceptez l'inévitabilité de la panne et vous y préparez. En rendant la panne banale et contrôlée, vous renforcez la résilience des systèmes et la compétence des équipes. Votre organisation ne se contente pas de résister aux chocs, elle s'en nourrit pour devenir plus forte.
    - Avec un entraînement régulier à la panne, vous ne changez pas la position des services dans la matrice, mais réduisez la durée et la gravité des interruptions. Un service de la zone orange qui tombe en panne ne paralyse plus votre organisation pendant des jours, mais seulement quelques heures.

Résultat global : après le Tour 2, votre zone orange est plus petite (certains services sont descendus vers la zone verte), plus autonome (moins dépendante des chaînes d'approvisionnement) et plus résiliente (mieux préparée aux pannes).

Transition vers le Tour 3 : de la résilience individuelle à la résilience collective

Vous êtes un peu plus comme Oseja : vous avez appris à construire votre autonomie, à tester votre résilience et à vous renforcer par l'épreuve.

Mais, en construisant cette résilience interne, nous avons ouvert une nouvelle perspective. La « Digital Enterprise Mine » nous a montré que nos déchets peuvent devenir une ressource pour soi-même, mais également l'être pour d'autres. Le Chaos Engineering nous a appris l'importance du partage et de la transparence. Nous avons commencé à comprendre que la résilience la plus forte n'est pas individuelle, mais collective.

Et, si la prochaine étape de votre montée en maturité était de passer de la construction de votre propre forteresse à celle d'un écosystème résilient ? C'est tout l'enjeu du Tour 3, où nous aborderons la zone verte non plus comme un coût à optimiser, mais comme une opportunité de leadership et de transformation systémique.

---

[26] United Nations Development Program. *Learning from local ingenuity – how simple reed fencing has unlocked a solution to rising sea levels in Egypt*. 2022. URL : https://www.undp.org/arab-states/blog/learning-local-ingenuity-how-simple-reed-fencing-has-unlocked-solution-rising-sea-levels-egypt/.

[28] Institute for Sustainable IT. *La règle des 3U*. URL : https://fr.wiki.isit-europe.org/nr/Utile_Utilisable_Utilis%C3%A9.

[29] Race for Water. *La règle des 5R*. 2024. URL : https://www.raceforwater.org/fr/nous-soutenir/eco-gestes/.

[30] Le Web Vert. *La loi d'erooM, de Tristan Nitot*. 2024. URL : https://www.lewebvert.fr/blog/2024-06-20-interview-tristan-nitot/.

[31] Boavizta. *Le diagnostic rapide EROOM*. 2024. URL : https://www.boavizta.org/eroom/diagnostic-rapide.

[32] International Copper Association. *Mines urbaines*. URL : https://internationalcopper.org/fr/policy-focus/climate-environment/urban-mining/.

[33] Centre de l'hormèse. *Qu'est-ce que l'Hormèse ?* 2024. URL : https://www.hormese.com/a-propos/hormese.

Chapitre 12

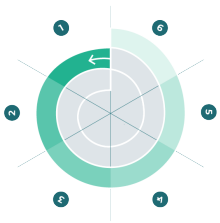
Tour 3 — Expérimenter dans la zone verte

> *L'économie du 21e siècle doit permettre à l'humanité de prospérer dans un espace juste et sûr, entre un plancher social et un plafond écologique.*
>
> **— Kate Raworth (2017)**

Annexe Tour 3 détaillé — Expérimenter
Découvrez le Tour 3 dans les détails pour aller plus loin.

Au sommet, vous avez sécurisé la zone rouge (cœur vital) au Tour 1, optimisé la zone orange (performance durable) au Tour 2, maîtrisé les métriques Oseja, créé votre « Digital Enterprise Mine » et développé l'antifragilité.

Vous pouvez maintenant inspirer les autres.



Le Tour 3 dépasse l'optimisation de la zone verte (services de confort) : il s'agit de choisir où concentrer vos ressources limitées (financières, énergétiques, humaines, cognitives).

Comme Oseja, qui a limité sa consommation pour garantir son autonomie et partager son électricité lors d'un blackout, vous verrez que la vraie force vient du partage de la résilience.

Sans fournisseurs, sans clients ou sans compétences pérennes, vous ne l'êtes pas.

Le paradoxe : abandonner le superflu augmente votre force. Partager vos ressources inutilisées crée plus de valeur. Reconnaître vos vulnérabilités vous renforce.

Pour bâtir ce leadership, explorez trois dimensions complémentaires :

Questionner le gaspillage de la zone verte : éliminer ce qui manque de valeur réelle.

Transformer les déchets en ressources via l'extension de votre « Digital Urban Mine » au bénéfice de l'écosystème.

Adopter le modèle du donut pour prospérer dans un espace juste et sûr, entre plancher social et plafond écologique.

Ces facettes forment un tout cohérent : sobriété stratégique (éliminer le superflu), circularité (recycler), préservation/régénération (créer de la valeur pour l'écosystème).

12.1 Facette 7 : Contre le gaspillage, la sobriété stratégique

Cette facette cible une fragilité coûteuse : le gaspillage de ressources dans des services à faible valeur.

Exercice de pensée : l'audit du dividende de sobriété

Listez les services en zone verte. Pour chacun, vous pouvez alors calculer les éléments suivants :

- Coût total annuel (licences, infrastructure, support, énergie, temps IT)
- Valeur métier réelle
- Taux d'utilisation réel
- Dividende de sobriété potentiel en cas de suppression

Ce dividende représente les ressources — matérielles, électriques, financières, cognitives — que vous pouvez libérer pour renforcer les zones critique et importante.

Mécanisme de fragilisation : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)

> **Annexe Mécanismes et scénarios**
> Toutes les vulnérabilités et les scénarios utilisés pour les tours un à trois sont issus de l'annexe qui les détaille et les argumente.

Pourquoi est-il si difficile de quitter un service inutile de la zone verte ? Les choix technologiques passés, souvent pour coût ou commodité, enferment dans des écosystèmes coûteux à quitter. Ces services sont conservés par habitude, coûts de sortie élevés, ou incapacité des équipes à faire autrement.

Le cycle de ce verrouillage est insidieux car progressif et difficilement détectable : adoption (« Cette solution est parfaite »), intégration (« Connectons-la à nos systèmes »), dépendance (« On ne peut plus s'en passer »), atrophie (« Les équipes ne savent plus faire autrement »), captivité (« Changer coûterait trop cher »).

Ce mécanisme crée un coût d'opportunité : chaque euro dépensé pour un service verrouillé n'est pas investi dans la résilience des zones critique et importante. Libérez-vous de ce verrouillage et vous récupérez ainsi des capacités pour les zones orange et rouge.

Scénario à envisager : La crise de confiance généralisée

Vos services sont souvent trop complexes, trop déconnectés des besoins réels ou perçus comme intrusifs ; ils brisent la confiance nécessaire à une utilisation sereine.

En interne, les utilisateurs fuient les outils officiels vers le « shadow IT » ; en externe, ils doutent des services, et l'entreprise perd sa Licence sociale d'opérer. Les « déconnexions volontaires » augmentent, creusant la fracture générationnelle, sociale…

L'entreprise gardant trop de services inutiles ou mal perçus gaspille ses ressources et alimente la méfiance. À l'inverse, celle qui rationalise sa zone verte en conservant seulement les services à valeur claire maintient cette confiance.

Inspiration : 37signals et l'Estonie

Annexe Exemples inspirants

Comment contrer cette fragilité ? En changeant radicalement de paradigme : passer de l'accumulation à la sobriété stratégique.

L'inspiration vient de deux acteurs montrant que la sobriété bien intégrée est un avantage concurrentiel :

37signals (Basecamp) [34] génère 100M$/an avec 60 personnes et 6 outils (contre 89 en moyenne). Leur règle : « Si ça ne sert pas directement le client, on ne le fait pas ».

L'EstonieautociteeEstonia gère 1,3 million de citoyens avec une identité numérique unique, un portail pour tous les services, 13 employés IT et un coût de 50M€/an (vs 1 milliard pour pays similaires). Résultat : 99 % des services publics en ligne, 98 % de satisfaction.

Annexe La low-tech

Ces précurseurs appliquent la philosophie low-tech : des solutions simples, durables et maîtrisables. Pour votre zone verte, il devient important de privilégier des alternatives low-tech aux services complexes, quand ceux-ci sont nécessaires.

La sobriété stratégique n'est pas de la décroissance. C'est l'allocation intelligente des ressources, en arbitrant entre un confort fragile et une robustesse durable.

Solutions : maximiser votre dividende de sobriété

Instaurez la « matrice d'arbitrage » : chaque année, listez les services en zone verte et le dividende lié à leur suppression. Proposez un plan : « Si on coupe ce service, on finance cela ».

Adoptez des « politiques de désengagement » (Sunset Policies) : toute application peu utilisée est listée pour suppression. Le propriétaire a trois mois pour justifier, sinon suppression.

Adaptez votre production selon les ressources : l'inspiration vient de la démarche TELED (Annexe La démarche TELED) qui priorise les tâches consommatrices, passant d'un flux tendu à une gestion par stocks stratégiques.

Communiquez le réinvestissement : annoncez le décommissionnement de l'ancienne application et les économies financeront un second site de secours. Vous ne supprimez pas, mais renforcez.

Mesurez votre « ratio de sobriété » (métrique Oseja n° 12) : calculez le pourcentage du budget IT en zones rouge et orange. « Aujourd'hui 60 % est affecté aux zones critiques, 40 % au confort. Objectif 80/20 en 2 ans. » Plus ce ratio est haut, meilleur est votre alignement.

Pratiquez la « sobriété offensive » : ne coupez pas que vos services inutiles, aidez vos partenaires. Partagez votre liste de services supprimés et de critères. Créez un « GitHub de la sobriété » pour documenter les décisions. Lancez un challenge territorial : « Qui libérera le plus de ressources ? » La sobriété devient contagieuse.

Adoptez la règle du « 1 pour 1 » : pour chaque nouveau service en zone verte, il faut en supprimer un existant. Si la démarche est trop radicale pour votre contexte, vous pouvez commencer par « 3 pour 1 » ou « 2 pour 1 », puis vous progresserez dans le temps avec la maîtrise acquise.

Après avoir libéré des ressources, pérennisez et étendez la gestion des déchets en ressources. La sobriété sans circularité est une illusion.

12.2 Facette 8 : De la mine d'entreprise à la mine urbaine

Vos déchets numériques deviennent une ressource collective ; la circularité partagée construit une résilience écosystémique.

Exercice de pensée : l'audit des actifs dormants

Repensez aux services décommissionnés en facette 7. Qu'en est-il du matériel associé ? Des dizaines, voire des centaines d'ordinateurs, écrans, serveurs mis au « rebut » chaque année : matériels fonctionnels rendus dans le cadre de contrats trop courts, matériels réparables et jetés…

Comme pour la facette 5, listez les matériels remplacés et posez-vous les questions suivantes :

1. Pourquoi ce remplacement ? (Obsolescence, fin de garantie, politique)
2. Que deviennent ces équipements ? (Recyclage, stockage, destruction)
3. Quelle valeur représente ce matériel dormant ?
4. Quels obstacles à leur réutilisation ? (Données, garanties, certifications)
5. Est-ce que votre chaîne de fournisseurs se pose aussi ces questions ? Vos clients ? Comment les accompagnez-vous pour qu'ils en aient aussi plus conscience ?
6. Est-ce que vos matériels ne pourraient pas rendre votre écosystème plus indépendant, plus résilient ?

Cet exercice révèle une mine d'or traitée comme un déchet.

Mécanisme de fragilisation : la dépendance géopolitique et physique

Cette gestion du matériel comme déchet crée deux fragilités :

- Fragilités géopolitiques : la fabrication des composants critiques, comme les semi-conducteurs, est concentrée dans des zones à risque (Taïwan), et les matières premières clés sont quasi-exclusivement contrôlées par la Chine. Chaque maillon est une vulnérabilité. En jetant des équipements fonctionnels, vous renforcez votre dépendance à ces chaînes fragiles.
- Fragilités physiques/climatiques face à l'incertitude environnementale : jeter des équipements réparables augmente la pression sur les ressources (terres rares, eau, énergie) et aggrave les fragilités physiques et climatiques. Vous contribuez au problème mondial alors que vous détenez une part de la solution.

Scénario à envisager : la pénurie paradoxale

Ce risque illustre le scénario La rupture géopolitique. Une crise bloque l'importation de puces mémoire ou rend leur tarif rédhibitoire. Vous avez un besoin urgent de RAM pour un serveur critique en zone orange, mais le fournisseur annonce neuf mois de délai.

Dans l'entrepôt d'une partie prenante, 20 serveurs mis au rebut il y a six mois contiennent ces barrettes. Faute de processus pour les récupérer et certifier, ce stock reste inaccessible. La pénurie est là, malgré une abondance potentielle.

Inspiration : la « Digital Urban Mine » et la résilience collective

Transformez votre vision du déchet : la « Digital Enterprise Mine » devient un levier de résilience collective.

Une direction éclairée voit les actifs dormants de son écosystème comme ressource collective. Elle crée une « Digital Urban Mine » : plateforme locale avec entreprises, reconditionneurs, associations, pour collecter, démanteler, certifier, redistribuer composants et équipements.

Cette mine, alimentée par la zone verte, utilise les ordinateurs décommissionnés des services de confort pour prolonger des postes essentiels et des serveurs critiques.

Comme Oseja a créé un micro-réseau énergétique, vous créez un micro-réseau de ressources matérielles.

La Digital Urban Mine est un bien commun numérique. Elle nécessite gouvernance collective, règles partagées, responsabilité mutuelle. Vous devenez source d'inspiration et de savoir-faire.

Solutions : créer un bien commun numérique

L'approche devient novatrice : inversez la logique et commencez par le collectif.

Au Tour 2, vous avez créé votre mine interne (Digital Enterprise Mine). La vraie valeur est dans le partage en développant une Digital Urban Mine collective avec d'autres organisations, fondée sur votre mine, sur ses principes.

Continuer avec le collectif : transformez votre mine en plateforme collective avec quelques partenaires. Partagez vos déchets numériques.

Adopter une gouvernance de bien commun (inspirée d'Elinor Ostrom [35]) : la Digital Urban Mine est un bien commun numérique. Appliquez les principes d'Ostrom : cocréation des règles, rotation des responsabilités, transparence des usages… Personne n'est propriétaire exclusif, tout le monde est bénéficiaire, assurant la garantie d'un bon fonctionnement.

Viser l'impact sociétal, en même temps que l'économique : don de composants à des associations, écoles, structures d'insertion, formations gratuites à la réparation, publication en open source de vos protocoles… La mine devient un projet social, renforçant votre Licence sociale d'opérer.

Mesurer l'« impact commun » (métrique Oseja n° 13) : mesurez « pourcentage de composants donnés par rapport à reçus ». Ratio > 1 = contributeur net, < 1 = bénéficiaire net (acceptable en démarrage). Cette métrique évalue l'impact collectif, pas l'efficacité individuelle.

Utiliser la mine comme levier de sobriété : en décommissionnant un service, vous économisez et alimentez la mine collective avec des équipements profitant à l'écosystème.

Intégrer une approche progressive (pour des organisations moins matures) : si l'approche est trop radicale, commencez par maîtriser votre Enterprise Mine interne (Tour 2), mutualisez avec 2-3 entreprises, élargissez au secteur, puis au territoire.

Lancer des défis pratiques à adresser (quelle que soit l'approche) : création d'un protocole standardisé pour certifier les composants, investissement dans des outils de formatage sécurisé, démarrage par éléments standardisés (RAM, disques durs, alimentations).

Après avoir libéré des ressources (facette 7) et transformé des déchets en ressources (facette 8), adoptez une vision vers un espace juste et sûr. Sobriété et circularité sans vision restent une optimisation locale.

12.3 Facette 9 : Le donut de Raworth et le courage du « Non »

Le modèle du donut guide la prospérité entre plancher social et plafond écologique.

Exercice de pensée : votre position dans le donut

Le donut de Kate Raworth [36] définit un espace sûr entre un plancher social (les besoins fondamentaux) et un plafond écologique (les limites planétaires).

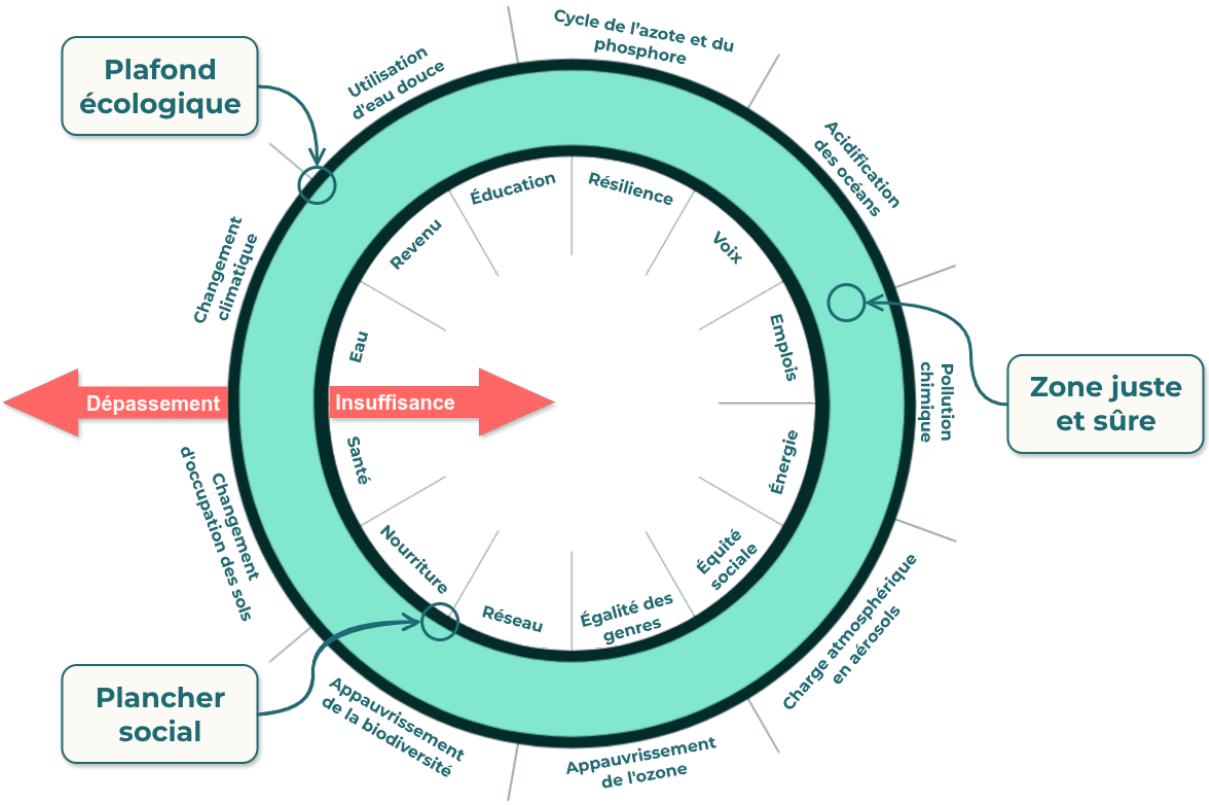


FIG. 12.3.1 : Le donut de Kate Raworth

Évaluez un service de la zone verte selon les axes suivants :

Plancher social : Est-ce que le service satisfait des besoins clés (santé, éducation, emploi) ou participe à l'insuffisance ?

Plafond écologique : Est-ce que le service impacte fortement des limites (CO_2, eau, ressources) ou contribue à réduire les dépassements ?

Position dans le donut : Est-ce que le service se positionne dans l'espace juste, sous le plancher, au-dessus du plafond, ou les deux ?

Beaucoup de services verts sont au-dessus du plafond sans rester au-dessus du plancher (sans valeur sociale), ce qui est le pire des cas.

Mécanisme de fragilisation : Impacts sociétaux dans un contexte d'incertitude croissante

Pourquoi maintenir des services numériques sans valeur sociale ni durabilité ?

Le numérique peut créer de la surcharge informationnelle, de la surveillance, de la dépendance aux algorithmes, de la fracture numérique. Il génère ainsi de la méfiance et de l'incertitude qui nuisent à votre entreprise.

Cette perte de confiance peut provoquer de la pression réglementaire, des difficultés à recruter des talents en quête de sens, et du rejet de produits nuisibles ou sans valeur réelle.

Scénario à envisager : La crise de confiance généralisée

Des scandales liés au numérique (fuites de données sensibles ou critiques, manipulations grâce à des biais cognitifs, surveillance de masse, désinformation) provoquent un rejet massif du numérique.

Votre organisation investit dans des services qui sont énergivores, complexes à appréhender et à utiliser, intrusifs par les données demandées ou collectées sans consentement, hors des attentes sociales… Les personnes, déçues par des promesses non tenues et des atteintes à la vie privée, se détournent, multipliant les « déconnexions volontaires ».

Ignorer ces impacts, c'est perdre une partie de la clientèle, du personnel, de la population et votre Licence sociale d'opérer est dévalorisée. Vous devenez obsolète stratégiquement.

Inspiration : Amsterdam, ville donut

Pour contrer la fragilité, adoptez le donut de Kate Raworth comme boussole stratégique. Amsterdam, première ville donut au monde [37] est une source majeure d'inspiration. Depuis 2020, Amsterdam a adopté le modèle du Donut comme cadre stratégique pour guider ses politiques publiques, devenant ainsi la première grande ville à intégrer cette vision dans sa gouvernance. Elle a inspiré d'autres villes ou organisations à faire de même.

Le donut n'est pas un simple outil de sensibilisation, mais également de navigation. Il aide à arbitrer entre les projets hors de l'espace juste et sûr, et ceux qui y restent ou aident à y entrer. C'est un acte de courage et de lucidité.

Le donut transforme votre zone verte : au lieu de maintenir des services dépassant le plafond écologique sans satisfaire le plancher social, concentrez vos ressources sur des services créant de la valeur sociale tout en respectant les limites planétaires.

Solutions : intégrer le donut dans votre stratégie

Créez votre « tableau de bord du donut » : évaluez (faible, moyen, élevé) chaque service de la zone verte sur sa contribution sociale et son impact écologique sur les impacts négatifs et positifs. Priorisez le décommissionnement des services à faible contribution et fort impact.

Instaurez le « test du donut » : avant tout projet, demandez : « Ce projet satisfait-il ou impacte-t-il un besoin humain fondamental ou les limites planétaires ? ». Refusez s'il échoue à avoir des impacts positifs qui compensent les impacts négatifs.

Communiquez votre vision donut : publiez un « Manifeste donut » exposant votre engagement à prospérer dans l'espace juste et sûr. Partagez métriques, arbitrages, échecs et succès pour inspirer.

Évaluez votre « Position donut » : calculez la moyenne des scores sociaux et écologiques de vos services.

Réinvestissez le dividende de sobriété dans le donut : utilisez les ressources libérées pour financer des projets ramenant dans l'espace juste et sûr, par exemple formation à la réparation ou migration vers des datacenters bas carbone.

Publiez votre « déclaration d'interdépendance numérique » : inspirée de l'Agile Manifesto pour le bien commun. Exemples : « Notre résilience dépend de notre écosystème », « Nous ne sacrifions jamais le collectif à notre organisation », « Notre succès se mesure à notre contribution au bien commun ». Cette déclaration guide votre stratégie.

Pour les pionniers : instaurez le « veto donut citoyen » ; les organisations avancées peuvent donner à un panel citoyen le pouvoir de bloquer tout projet hors de l'espace juste et sûr. Si la démarche est trop radicale, commencez par un « Conseil donut consultatif » sans veto, puis progressez.

12.4 Conclusion du Tour 3 : de la résilience individuelle à l'inspiration de la collectivité

Ce tour est terminé. Vous avez appris à questionner le gaspillage des services de confort, transformer vos déchets en ressources collectives avec la Digital Urban Mine, et adopter le modèle du donut pour prospérer dans un espace juste et sûr. Pour un leadership dans la zone verte, appliquez sobriété stratégique, circularité et prévention, réparation, régénération.

Synthèse des bénéfices

Votre organisation a rationalisé sa zone verte, transformant sa posture avec des bénéfices organisationnels, stratégiques et écosystémiques.

Vous avez réalisé des économies substantielles en décommissionnant les services inutiles (dividende de sobriété). Vous avez gagné en autonomie matérielle via une « Digital Urban Mine » collective, réduisant la vulnérabilité et créant de la valeur pour l'écosystème. Surtout, vous avez développé une culture du leadership : vos équipes transforment les contraintes en opportunités. Vous avez passé une étape de la résilience individuelle à collective, de la forteresse à l'écosystème, devenant votre propre Oseja numérique.

Impact des principes sur la performance durable

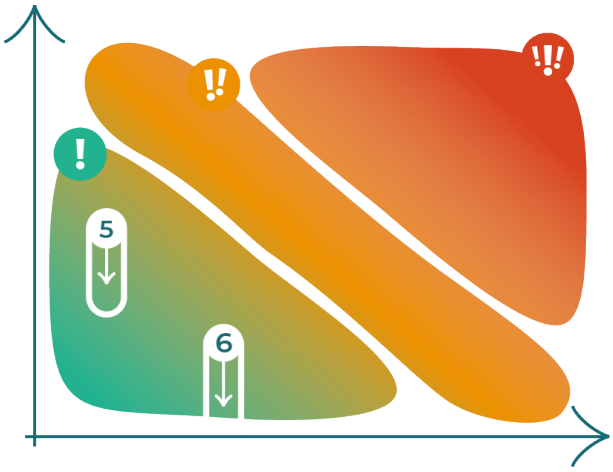


Fig. 12.4.1 : Évolution de la matrice au Tour 3

Les trois principes agissent en synergie pour un leadership performant et durable.

- La sobriété stratégique (facette 7) réduit le coût d'opportunité et la charge cognitive.
    - En éliminant le superflu, vous libérez des ressources financières, énergétiques et cognitives à réinvestir dans les zones critiques.
    - La zone verte diminue : seuls les services à valeur claire sont conservés.

- La circularité (facette 8) lutte contre le gaspillage systémique et l'interdépendance subie.
    - Transformer les déchets numériques en ressources via la Digital Urban Mine crée une boucle vertueuse, anticipant les pénuries à venir.
    - La récupération libère des ressources matérielles réinvesties dans les zones rouge et orange, réduisant les vulnérabilités et prolongeant la durée de vie des équipements.
- La régénération (facette 9) change le rapport au sens et à la 🕮 Licence sociale d'opérer.
    - Avec le donut comme boussole, vous créez de la valeur sociale en respectant les limites planétaires, et en devenant un modèle inspirant.
    - Le dividende de sobriété réinvesti renforce les zones rouge et orange ou votre potentiel de la Digital Mine, en améliorant votre ratio de sobriété (80/20 au lieu de 60/40) et l'alignement stratégique.

Résultat global : après le Tour 3, la zone verte est rationalisée (cas n° 5), les ressources libérées (cas n° 6) réinvesties dans les zones critiques et importantes. Vous passez de la résilience individuelle au leadership collectif, de la forteresse à l'écosystème, devenant votre Oseja numérique.

Votre organisation n'est plus celle qui sécurise (Tour 1), ni optimise (Tour 2). Elle TRANSFORME :

- Les déchets deviennent des biens communs (Digital Urban Mine collective),
- La compétition cède la place à la coopération (gouvernance d'Ostrom, partage sobriété),
- La fragilité individuelle évolue en antifragilité collective (résilience écosystémique).

12.5 Et maintenant ? Le chemin vers la maîtrise

Vous avez fini le Tour 3. Prenez le temps et mesurez votre progrès : vous avez transformé votre zone verte en levier de leadership, choisi l'essentiel, converti vos déchets en ressources collectives, prospéré dans un espace sûr. Comme Oseja de Sajambre, qui partage son électricité lors des blackouts, vous avez compris que la vraie force vient du partage de la résilience.

Vous êtes maintenant votre propre Oseja numérique.

Votre transformation après trois tours

Avant les trois tours, votre organisation était fragile, dépendante, dispendieuse :

- Zone rouge : vulnérable et dépendante des chaînes mondiales.
- Zone orange : complexe et inefficace, avec des services inutiles et du matériel gâché.
- Zone verte : gaspillage de ressources pour des services sans valeur.

Après les trois tours, votre organisation est résiliente, autonome, sobre, inspirante :

- Zone rouge : sécurisée, autonome, avec une redondance adaptée et organisée, et une résilience accrue.
- Zone orange : optimisée, durable, avec une performance utile et pérenne.
- Zone verte : rationalisée, impact positif sur l'écosystème et la collectivité.

Votre matrice de criticité devient votre matrice de résilience et de leadership. Vous ne subissez plus, ne résistez plus, n'optimisez plus. Vous transformez et inspirez.

De la compétence à la maîtrise : un quatrième tour vous attend

Le voyage ne s'achève pas ici, la maîtrise commence.

Les trois premiers tours vous ont donné la compétence :

- Tour 1 : Protéger (sécuriser le critique avec les métriques Oseja n°1-4)
- Tour 2 : Optimiser (construire durablement avec les concepts des 3U, des 5R, de l'antifragilité, et les métriques n°5-11)
- Tour 3 : Transformer (inspirer l'écosystème via la sobriété, la circularité collective, le donut, avec les métriques n°12-14)

Vous maîtrisez les outils, vous avez de belles convictions et une forte capacité de transformation.

Il ne reste plus qu'à intégrer ces acquis fluidement, savoir quand et où les appliquer, les transposer et les orchestrer selon contexte.

Le Tour 4 offre cette maîtrise. En effet, la spirale est une hélice ascendante : chaque tour accroît votre maturité et votre robustesse. Le Tour 4 marque le passage de la compétence technique à la maîtrise stratégique en maximisant l'impact de tous les acquis sur l'ensemble des zones.

Le Tour 4 vous attend, maintenant.

[34] 37SIGNALS. *Getting Real : The smarter, faster, easier way to build a successful web application*. URL : https://basecamp.com/gettingreal.
[35] Elinor OSTROM. *Governing the Commons*. Cambridge University Press, 1990.
[36] Kate RAWORTH. *Doughnut Economics : Seven Ways to Think Like a 21st-Century Economist*. Chelsea Green, 2017.
[37] *Amsterdam, ville donut*. URL : https://amsterdamdonutcoalitie.nl/.
[115] E-ESTONIA. *We have built a digital society and so can you*. URL : https://e-estonia.com/.

Chapitre 13

Tour 4 — Intégrer et approfondir

13.1 Introduction : le passage de la compétence à la maîtrise et l'approfondissement

> **Annexe** Tour 2 détaillé — Optimiser
> Découvrez le Tour 4 dans les détails pour aller plus loin.

Vous avez parcouru trois tours de la spirale. Vous avez sécurisé votre zone rouge avec le principe de non-régression et la résilience organisée (Tour 1), optimisé votre zone orange avec la durabilité et l'antifragilité (Tour 2), et choisi l'essentiel dans votre zone verte avec la sobriété et le Donut (Tour 3). Vous avez acquis des outils puissants et des convictions profondes.

Il reste toutefois une étape importante, celle qui transforme la simple compétence en maîtrise globale : apprendre à appliquer les bons outils au bon moment, même hors de leur contexte originel. Maîtriser ne signifie pas connaître le plus d'outils, mais choisir le bon outil pour chaque situation, transposer un apprentissage d'une zone à une autre.

Ce quatrième tour n'enseigne pas de nouveaux concepts. Il invite à revisiter les trois zones avec un regard neuf et aguerri, armé de tous les acquis des tours précédents.

Vous allez découvrir que les outils appris dans une zone peuvent transformer les autres zones, vérifier, approfondir et intégrer. Ce tour n'est donc pas une révision, c'est l'acquisition d'une compétence supérieure : la capacité d'orchestration et de contextualisation.

Important : ce tour est obligatoire pour atteindre la maîtrise, mais ses parties sont flexibles. Chaque organisation choisit son niveau d'ambition selon sa maturité. Certaines actions sont pragmatiques et accessibles à tous, d'autres sont radicales et réservées aux pionniers. À vous de choisir jusqu'où vous voulez aller.

13.2 Zone verte : le contrôle de conformité

L'objectif : s'assurer que les fondamentaux ont bien été appliqués

Lors du Tour 3, vous avez rationalisé votre zone verte avec des notions ambitieuses et novatrices : la sobriété stratégique, la Digital Urban Mine collective, le Donut de Raworth. Mais, avez-vous bien intégré les outils fondamentaux du Tour 2 qui pouvaient être appliqués dès le départ ? Les 3U (Utile, Utilisable, Utilisé) et les 5R (Refuser, Réduire, Réemployer, Réparer, Recycler) sont des outils pragmatiques et puissants. Si vous les avez appliqués dans le Tour 3, cette étape sera rapide. Si vous ne l'avez pas fait, c'est le moment d'améliorer et d'aller plus loin.

Comment aborder cette zone

État d'esprit : ne considérez pas cette étape comme une remise en question de votre travail, mais comme un contrôle qualité. Vous allez vérifier que les fondamentaux sont bien en place avant de passer aux zones plus complexes.

Approche : reprenez la liste des services de confort (zone verte) et posez-vous cette question simple : avez-vous mis en œuvre les notions suivantes comme expliqué dans le Tour 2 ?

1. Les 3U ?
2. Les 5R ?
3. Le dividende de sobriété ?

Résultat attendu : si vous avez bien fait le Tour 3, les outils ont déjà été appliqués et cette étape sera une simple confirmation. Si ce n'est pas le cas, vous aurez identifié des axes de progrès avant de passer à la zone orange.

Enjeu : une zone verte bien rationalisée libère des ressources (financières, matérielles, cognitives) qui peuvent être réinvesties dans les zones rouge et orange. Cette étape ne doit pas être négligée.

13.3 Zone orange : l'approfondissement vers la radicalité

L'objectif : aller au-delà de l'optimisation, vers la transformation

Lors du Tour 2, vous avez optimisé votre zone orange avec les 3U, les 5R, la Digital Enterprise Mine et l'antifragilité. C'était déjà un travail considérable et précieux. Mais, le Tour 3 a apporté des notions encore plus puissantes et radicales : le Donut, la sobriété offensive, la gouvernance des biens communs (Ostrom), et la déclaration d'interdépendance numérique. Ces notions ont été introduites dans le Tour 3 pour certaines, et d'autres, issues du Tour 2, ont aussi été renforcées, poussées et expérimentées dans des contextes plus larges.

Il est maintenant temps de les appliquer à votre zone orange. En effet, ces notions peuvent transformer vos projets d'optimisation en projets de transformation sociétale et écologique.

Comment aborder cette zone

État d'esprit : ne considérez pas cette étape comme une simple application mécanique d'outils, mais comme un questionnement profond de vos projets. Vous allez passer de « Comment optimiser ? » à « Pourquoi optimiser ? Pour qui ? À quel prix écologique et social ? »

Approche : vous allez appliquer trois notions radicales du Tour 3 aux projets de la zone orange :

1. La sobriété offensive : vos optimisations ne doivent plus bénéficier seulement à votre organisation, mais à tout votre écosystème. Partagez publiquement vos meilleures pratiques, créez un « GitHub de l'optimisation », lancez des challenges territoriaux. Rendez la sobriété désirable.

2. La gouvernance des biens communs (Ostrom) : certains de vos projets d'optimisation pourraient devenir des biens communs numériques. Au lieu de les garder pour vous, proposez-les en open source avec une gouvernance collective. Vous renforcez ainsi la résilience de toute votre chaîne de valeur, et la vôtre par voie de conséquence.

3. Le Donut de Raworth : chaque projet d'optimisation doit être questionné à travers le prisme du Donut. Contribue-t-il au plancher social (besoins humains fondamentaux) ? Respecte-t-il le plafond écologique (limites planétaires) ? Les projets qui optimisent au prix d'une dégradation sociale ou écologique doivent faire l'objet d'un arbitrage pour être repensés ou abandonnés.

Résultat attendu : après cet approfondissement, votre zone orange n'est plus seulement optimisée (Tour 2), elle est aussi alignée sur vos convictions profondes (Tour 3). Vos projets d'optimisation deviennent des projets de transformation sociétale. Vous ne cherchez plus uniquement la performance, mais la préservation, la restauration, voire la régénération.

Enjeu : c'est ici que se fait le passage du statut de gestionnaire efficace à celui de source d'inspiration, au-delà du simple confort de votre zone verte. Performance et responsabilité ne sont pas contradictoires, mais complémentaires.

13.4 Zone rouge : la simplification pragmatique et l'aspiration radicale

L'objectif : simplifier le critique sans le fragiliser, puis oser le questionner

Votre zone rouge est votre cœur de métier, vos services critiques. Lors du Tour 1, vous l'avez sécurisée avec la résilience organisée, la redondance géographique et la non-régression. C'était nécessaire et précieux. Mais, maintenant que vous avez acquis les outils du Tour 2 (3U, 5R, antifragilité) et les convictions du Tour 3 (Donut, sobriété), il est possible d'aller plus loin.

Cette zone se divise en deux approches complémentaires :

1. Approche pragmatique (obligatoire) : simplifier la zone rouge avec les outils du Tour 2.

2. Approche radicale (optionnelle) : questionner la zone rouge avec les convictions du Tour 3.

Comment aborder cette zone

État d'esprit : la zone rouge est sacrée, mais elle ne devrait pas être intouchable. Même le critique peut être simplifié, et cette simplification renforce la robustesse au lieu de la fragiliser. Toutefois, si vous ne vous sentez pas suffisamment mature pour la revisiter, patientez, la maturité viendra plus tard.

Approche pragmatique (obligatoire) : simplifier avec les outils du Tour 2

Vous allez appliquer trois tests aux services critiques :

1. Le test de l'utilité (3U) : même dans un ERP (progiciel de gestion intégré ou enterprise resource planning) critique, toutes les fonctionnalités ne sont pas vitales.

2. Le test de la circularité (5R) : vous allez appliquer les 5R à votre zone rouge. Refuser les mises à jour non critiques qui ajoutent de la complexité. Réduire le nombre de serveurs par consolidation sans perdre votre redondance. Réutiliser des composants de la mine. Réparer plutôt que remplacer. Recycler les équipements obsolètes.

3. Le test de l'antifragilité : vous allez rendre la panne si banale que vos équipes n'en ont plus peur. Intégrez le Chaos Monkey sur les services critiques, faites des post-mortems sans concession ni culpabilisation.

Résultat attendu : votre zone rouge devient plus simple, plus sobre, plus autonome et plus entraînée. La robustesse n'est plus passive (protéger), elle est active (entraîner).

Approche radicale (optionnelle, pour les pionniers) : questionner avec le Donut

Pour les organisations les plus avancées, il est possible d'aller encore plus loin en questionnant la zone rouge avec le Donut. Votre zone rouge contribue-t-elle, au moins en partie, au plancher social (besoins humains fondamentaux) ou le respecte-t-elle ? Respecte-t-elle le plafond écologique (limites planétaires) ou contribue-t-elle à réduire les impacts ?

Avertissement : ces questions sont radicales et peuvent remettre en question des choix critiques. Si c'est trop tôt pour le faire, concentrez-vous sur l'approche pragmatique.

Exemple : votre datacenter critique consomme l'équivalent énergétique de centaines de foyers. Est-ce justifié ? Pourriez-vous migrer vers une infrastructure plus sobre (low-tech, énergies renouvelables, refroidissement passif) sans compromettre la criticité ?

Résultat attendu : si vous allez jusque-là, vous transformez votre zone rouge en un modèle de sobriété et de responsabilité. Vous prouvez que même le critique peut être sobre et entraîner tout votre secteur.

Enjeu : c'est ici que vous montrez que vos convictions ne sont pas réservées au confort (zone verte) ou à l'important (zone orange), mais qu'elles irriguent même le critique (zone rouge). Vous obtenez de la cohérence de bout en bout.

13.5 Conclusion : la spirale intégrée pour atteindre la maîtrise

Vous avez terminé le quatrième tour. Vous avez vérifié que les fondamentaux du Tour 2 ont bien été appliqués dans votre zone verte. Vous avez approfondi votre zone orange avec les notions radicales du Tour 3. Vous avez simplifié votre zone rouge avec les outils pragmatiques du Tour 2, et peut-être même questionné avec les convictions du Tour 3.

Vous avez terminé l'étape d'apprentissage des outils. Vous les appliquez à bon escient dans leur contexte d'origine. Vous avez, en plus, acquis la maîtrise : vous savez quand et où appliquer les bons outils, même hors de leur contexte. Vous savez choisir entre pragmatisme et radicalité selon votre maturité et votre ambition.

La spirale n'est plus un guide externe, elle est devenue votre gouvernail intérieur

Face à toute nouvelle technologie, à toute nouvelle crise, à toute nouvelle opportunité, les réflexes sont acquis pour l'analyser à travers trois filtres complémentaires :

Le filtre du critique (zone rouge) : Est-ce que cela touche à mon cœur de métier ? Comment le sécuriser et le simplifier sans le fragiliser ?

Le filtre de l'important (zone orange) : Est-ce que cela améliore ma performance de manière durable et responsable ?

Le filtre du confort (zone verte) : Est-ce que cela en vaut vraiment le coût ? Quelles ressources puis-je libérer en y renonçant ?

Ces trois filtres ne sont pas séquentiels, ils sont simultanés. Vous les appliquez en parallèle, vous les faites dialoguer. C'est cela, la maîtrise.

Votre direction est devenue mature, pragmatique et inspirante

Vous avez parcouru les quatre tours de la spirale. Vous avez acquis la compétence (Tours 1-3) et la maîtrise (Tour 4). Vous êtes maintenant capable de :

Protéger ce qui est vital (Tour 1)

Optimiser ce qui est important (Tour 2)

Transformer ce qui procure du confort (Tour 3)

Intégrer tous ces acquis de manière fluide et contextuelle (Tour 4)

Subir simplement les contraintes et résister aux chocs sont maintenant derrière. Les contraintes deviennent des opportunités, en inspirant l'écosystème, et prouvant par la réussite que performance et responsabilité ne sont pas contradictoires.

La spirale ne s'arrête jamais. Elle est le moteur de l'amélioration continue et de la pertinence dans un monde en perpétuel changement. L'objectif initial de devenir un Oseja numérique est atteint : un modèle de résilience, de sobriété et de leadership pour votre secteur.

Félicitations. Vous avez la maitrise de la résilience numérique pour aller vers plus de robustesse de votre organisation.

13.6 Et maintenant ?

Les quatre tours de la spirale sont terminés. Vous avez acquis les outils, les convictions et la maîtrise. Mais, la spirale ne s'arrête pas là. Elle est une hélice ascendante : chaque tour fait monter en maturité, en compétences, en robustesse.

La prochaine fois qu'une nouvelle technologie émergera (IA générative, informatique quantique, edge computing, etc.), vous ne la subirez pas. Vous l'analyserez à travers les trois filtres (critique, important, confort). Vous saurez où la placer dans votre matrice de criticité. Vous saurez quels outils appliquer (3U, 5R, Donut, sobriété offensive…). Vous saurez quand être pragmatique et quand faire preuve de radicalité. Vous saurez comment capitaliser sur les nouveaux acquis que cette technologie vous aura permis d'intégrer.

La spirale est devenue votre ADN numérique. Les défis à venir sont à votre portée.

Chapitre 14

Le basculement de paradigme

14.1 Le monde change, l'organisation doit aussi évoluer

Au début de ce livre blanc, nous avons posé un diagnostic : le monde a changé et continue d'évoluer. La stabilité n'est plus la norme. L'incertitude est devenue la règle. La polycrise est devenue structurelle.

Face à ce basculement du monde, les organisations doivent opérer leur propre transition pour être en capacité de s'adapter aux fluctuations. En ajustant leurs pratiques et en transformant leur paradigme : repenser le rapport au numérique, à la performance, à la gouvernance, et à toutes les parties prenantes. Un numérique stable et sans limites n'est plus envisageable ; il en est de même pour le métier porté par ce numérique.

L'expérience récente révèle que cette apparente stabilité résultait de conditions historiques exceptionnelles qui s'estompent progressivement, révélant la nature fondamentalement fragile et imprévisible des systèmes numériques complexes face aux chocs de la polycrise.

Il s'agit alors de résister à ces chocs, tout en se bonifiant grâce à eux. Devenir antifragile est une évidence : transformer chaque crise en opportunité d'apprentissage, chaque panne en test de résistance. Concrètement, cela signifie pratiquer le Chaos Engineering, à savoir le fait d'instaurer une culture de l'apprentissage, et traiter la redondance comme un investissement stratégique là où elle est réellement nécessaire. L'organisation antifragile n'est pas celle qui ne tombe jamais, mais celle qui se relève plus forte à chaque fois, moins vulnérable.

Cette capacité à se bonifier demande cependant de concentrer les ressources sur l'essentiel, ressources limitées à court terme. Il ne s'agit pas de renoncer en partie au numérique par ascétisme, mais au superflu pour sanctuariser l'essentiel. En effet, le dividende de sobriété libère des ressources pour construire la résilience là où elle compte vraiment.

Toutefois, la sobriété n'est pas un absolu ; elle reste relative à un contexte : on peut avoir une forte redondance sur les services critiques, tout en éliminant leurs fonctionnalités inutiles. Elle devient ainsi une stratégie : choisir l'essentiel pour concentrer les ressources sur la robustesse du réel cœur de métier.

Une gouvernance adaptée est alors nécessaire pour gérer ce recentrage des ressources. Il convient d'élever la robustesse au rang de pilier stratégique, au même titre que la finance. Cela implique de disposer d'indicateurs de robustesse au tableau de bord de direction, d'un comité de robustesse au même niveau que le comité d'audit, d'un budget pérenne, d'une gestion adaptée au changement profond qui se met en place et d'un engagement fort de la direction. Élever la robustesse au rang stratégique, c'est transformer la vulnérabilité en avantage compétitif durable.

Cependant, cette robustesse ne peut pas se construire seule dans un système d'interactions fortes entre toutes les parties prenantes. Elle se bâtit avec les autres par la mutualisation des ressources critiques, le partage des connaissances, la création de communs numériques. Cette coopération ouvre une perspective plus ambitieuse : celle d'une performance régénérative.

Le modèle du Donut propose un cadre de réalisme pour naviguer dans un monde contraint. Au minimum, il permet d'anticiper et de s'adapter. À son plein potentiel, il devient un idéal de performance régénérative. Chaque organisation choisit où elle se situe sur ce spectre, selon sa maturité et son ambition. Le leadership du vingt-et-unième siècle consiste à gagner et à le faire avec les autres parties prenantes, toutes ensemble.

Ces concepts forment un tout cohérent, mais leur intégration demande du temps. Comme la spirale de maturité proposée dans ce livre blanc, ce dernier invite à descendre pour comprendre, puis à remonter pour transformer. À chaque cycle, l'organisation renforce sa conscience, affine ses priorités et ancre la robustesse dans sa culture.

14.2 Le nouveau contrat organisationnel

Toutes ces dimensions se renforcent mutuellement. La robustesse antifragile comme priorité équilibre la gouvernance et permet la coopération. La sobriété stratégique concentre les ressources et finance pleinement la robustesse. La gouvernance stratégique de la robustesse transforme l'intention en moyens concrets. La coopération démultiplie la robustesse individuelle face aux chocs systémiques.

Ensemble, elles dessinent un nouveau contrat : celui d'une organisation qui cherche une nouvelle performance dans la durée et la sérénité. Qui cherche à croître et à se régénérer, voire à régénérer. Qui cherche à gagner avec les autres, en les inspirant.

Ce n'est pas une utopie. Des organisations ont déjà fait ces choix. Elles ont assez facilement traversé les crises récentes quand d'autres le faisaient avec difficulté ou s'effondraient. Elles ont su basculer, transformer les chocs en opportunités d'apprentissage. Elles ont compris que la robustesse est un avantage pour perdurer. Que la sobriété est une stratégie gagnante d'architecture. Que la gouvernance de la robustesse est un investissement majeur et rentable. Que la coopération, au-delà de l'altruisme, est le réalisme nécessaire à un système sain et pérenne.

Ce paradigme n'est pas réservé aux grandes organisations. Comme Oseja face à la panne, chaque organisation peut choisir d'être autonome sans être isolée : cultiver la sobriété, la coopération et la lucidité pour continuer à fonctionner, même lorsque le monde vacille.

La question finale n'est donc plus de savoir si, mais comment votre organisation choisira d'opérer ce changement.

« Quand le vent du changement souffle, certains construisent des murs, d'autres des moulins. »

Proverbe chinois

« Le vent éteint la bougie et attise le feu. Il en va de même avec le hasard, l'incertitude et le chaos : vous voulez les utiliser, pas vous en protéger. Vous voulez être le feu et souhaiter le vent. »

Nassim Taleb, Antifragile : les bienfaits du désordre (2013)

Partie III

ANNEXES

Sommaire

Annexe A

Ressources majeures

Les réflexions développées dans ce livre blanc s'appuient sur un ensemble de travaux récents qui, chacun à leur manière, explorent les défis systémiques auxquels font face les organisations contemporaines. Les sources mobilisées proviennent d'horizons complémentaires : institutions de recherche européennes et internationales, organismes de prospective des risques, centres de leadership et réseaux professionnels.

Cette diversité de perspectives permet d'ancrer les concepts proposés dans un dialogue entre analyse académique, observation empirique et expertise de terrain.

Sans prétendre à l'exhaustivité, ces ressources convergent sur plusieurs constats structurants : la nature interconnectée des crises actuelles, la nécessité d'approches multidimensionnelles pour y répondre, et l'importance d'une gouvernance anticipative capable de transformer la gestion des risques en levier de performance durable.

Les travaux cités ont été publiés entre 2024 et 2025, reflétant ainsi l'actualité des enjeux traités et la dynamique de recherche en cours sur ces questions. Leur mobilisation dans ce livre blanc vise à nourrir une réflexion opérationnelle tout en maintenant un ancrage dans les débats théoriques et institutionnels contemporains.

[38] Allianz. *Risk Barometer 2025*. Allianz Global Corporate and Specialty, division assurance des grandes entreprises. Enquête annuelle auprès de 3 778 experts en gestion des risques dans 106 pays identifiant les principaux risques commerciaux mondiaux (cyber-incidents, interruptions d'activité, catastrophes naturelles). 2025. URL : https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf.

[39] AXA. *Future Risks Report 2024*. AXA, groupe d'assurance mondial, en partenariat avec Ipsos. Enquête auprès de 3 000 experts et 20 000 citoyens explorant les risques émergents et leur interconnexion dans un contexte de polycrisis (pollution, cybersécurité, changement climatique, éthique technologique). 2024. URL : https://www-axa-com.cdn.axa-contento-118412.eu/www-axa-com/dad8b74b-e921-4b2d-bea8-2f7dabe369aa_axa_futurerisksreport_2024_va.pdf.

[40] Center for Creative Leadership. *Leading Beyond Barriers : Creating Impact in an Age of Polycrisis*. Center for Creative Leadership, organisation à but non lucratif leader mondial du développement du leadership depuis 50+ ans. Identifie les capacités de leadership critiques pour naviguer dans les crises interconnectées et les barrières psychologiques bloquant le progrès sur les défis globaux. 2025. URL : https://cclinnovation.org/wp-content/uploads/2025/02/leadingbeyondbarriers.pdf.

[41] Cigref. *4 Archétypes de la fonction numérique pour 2040*. Cigref, réseau de 150 grandes entreprises et administrations publiques françaises créé en 1970. Rapport d'orientation stratégique proposant 4 archétypes prospectifs de la fonction numérique à l'horizon 2040 (innovation, résilience, responsabilité, transversalité). 2025. URL : https://www.cigref.fr/rapport-dorientation-strategique-2025-du-cigref-4-archetypes-de-la-fonction-numerique-pour-2040.

[42] European Research Council. *Transformative change for a sustainable future*. European Research Council, organisme de financement de la recherche d'excellence de l'UE créé en 2007. Synthèse de 300+ projets explorant les stratégies innovantes pour un changement transformatif vers la durabilité et l'équité. 2024. URL : https://erc.europa.eu/sites/default/files/2024-12/Transformative-change-for-a-sustainable-future.pdf.

[43] Huan Liu et Ortwin Renn. "Polycrisis and Systemic Risk : Assessment, Governance, and Communication". In : *International Journal of Disaster Risk Science* (2025). Huan Liu (Kyoto University) et Ortwin Renn (Research Institute for Sustainability, expert mondial de la gouvernance des risques). Article de synthèse examinant polycrisis et risque systémique, leurs différences et implications pour la gouvernance et la communication des crises. URL : https://link.springer.com/article/10.1007/s13753-025-00636-3.

[44] Nature. "A systemic risk assessment methodological framework for the global polycrisis". In : *Nature Communications* (2025). Ajay Gambhir (ASRA) et 27 co-auteurs (Stockholm Resilience Centre, Oxford, Edinburgh, PIK). Cadre méthodologique d'évaluation des risques systémiques pour la polycrisis, appliqué aux crises alimentaire et énergétique. Méthodologie disponible via STEER (outil open-access). URL : https://www.nature.com/articles/s41467-025-62029-w.pdf.

[45] OCDE. *États de fragilité 2025*. OCDE, organisation internationale de 38 pays membres. Rapport analysant la fragilité dans 61 pays via un cadre multidimensionnel de 56 indicateurs couvrant 6 dimensions (politique, sociétale, sécuritaire, environnementale, économique, humaine). 25 ans d'expertise sur la fragilité. 2025. URL : https://www.oecd.org/content/dam/oecd/fr/publications/reports/2025/02/states-of-fragility-2025_c9080496/3797ea0f-fr.pdf.

[46] Oxford Poverty and Human Development Initiative. *Resilient Human Development*. Oxford Poverty and Human Development Initiative (OPHI), centre de recherche de l'Université d'Oxford dirigé par Sabina Alkire. Cadre conceptuel sur le développement humain résilient face aux chocs et crises, appliquant une approche multidimensionnelle de la pauvreté et du bien-être. 2025. URL : https://ophi.org.uk/sites/default/files/2025-09/OPHIRP_68a_2025_Resilient_%28Alkire%29.pdf.

[47] PolyCIVIS. *From Polycrisis to Polysolutions*. PolyCIVIS, réseau Jean Monnet de l'alliance universitaire CIVIS (11 universités euro-africaines). Approche interdisciplinaire explorant la polycrisis et proposant des solutions durables via une compréhension systémique de la gouvernance, des systèmes économiques et de la dimension humaine. 2025. URL : https://civis.eu/storage/files/1foundational-brief-polycrisis-and-policy-series-formatted-version2-schreiber-etal-mar-2025.pdf.

[48] Jürgen Scheffran. "Systemic risks and governance of the global polycrisis in the Anthropocene". In : *Global Sustainability* (2025). Jürgen Scheffran (Université de Hambourg, IFSH), expert en sécurité climatique et conflits environnementaux (500+ citations). Analyse la stabilité du nexus climat-conflit-migration-pandémie et les cascades de basculement dans la polycrisis de l'Anthropocène. Intègre recherche sur climat-conflit et risques systémiques. URL : https://www.cambridge.org/core/services/aop-cambridge-core/content/view/95EF7C378D08AD2806659BBACFABBAF5/S2059479825100264a.pdf/systemic_risks_and_governance_of_the_global_polycrisis_in_the_anthropocene_stability_of_the_climateconflictmigrationpandemic_nexus.pdf.

[49] Swiss Re. *SONAR 2024*. Swiss Re Institute, centre de recherche du réassureur mondial. Rapport annuel SONAR identifiant 16 risques émergents via crowdsourcing interne (résilience des chaînes d'approvisionnement, climat, cyber, isolement social, chaleur extrême). Outil de dialogue avec le secteur pour la gestion proactive des risques. 2024. URL : https://www.swissre.com/institute/research/sonar/sonar2024.html.

[50] Bishoy L. Zaki, Valérie Pattyn et Ellen Wayenberg. "Policymaking in an age of polycrises : emerging perspectives". In : *Policy Design and Practice* (2024). Bishoy L. Zaki, Valérie Pattyn et Ellen Wayenberg (Université de Gand). Collection spéciale développant

l'utilité analytique du concept de polycrisis pour la conception des politiques publiques et l'apprentissage politique en temps de crises interconnectées. DOI : 10.1080/25741292.2024.2432048. URL : https://doi.org/10.1080/25741292.2024.2432048.

A.1 Des références aux concepts du livre blanc

Les ressources majeures apportent des éléments validant ou confortant les concepts du livre blanc. Les citations suivantes associées à ces concepts ont été extraites des documents correspondants avec la page de l'information.

Concepts fondateurs

La polycrise

Rôle dans le livre blanc : Concept central qui décrit l'interconnexion des crises contemporaines affectant les systèmes numériques.

- **AXA (2024)** - Un leader mondial de l'assurance :
  - « *L'édition 2024 fournit une mine d'informations. Une fois de plus, elle souligne la polycrise qui saisit maintenant le monde* » (Thomas Buberl, CEO AXA, p.4)
- **CCL (2025)** - Institution de référence mondiale en leadership :
  - « *À une époque de polycrise — où les crises interconnectées s'amplifient mutuellement — les dirigeants doivent surmonter les barrières systémiques pour mettre en œuvre des solutions qui apportent un progrès significatif et durable* » (p.1)
- **Liu & Renn (2025)** - Publication Springer :
  - « *L'émergence du risque systémique mondial [...] a été étroitement liée à ce qui a été qualifié de polycrise actuelle d'enchevêtrement causal de crises dans de multiples systèmes mondiaux* » (p.1)
- **Nature Communications (2025)** - Revue prestigieuse :
  - « *L'émergence du risque systémique mondial dans un monde de plus en plus dégradé sur le plan environnemental, technologiquement avancé et interconnecté, a été étroitement liée à ce qui a été qualifié de polycrise actuelle* »(Gambhir et al., p.1)
- **PolyCIVIS (2025)** - Réseau de 21 universités européennes :
  - « *La polycrise est un réseau complexe de crises interconnectées, parfois avec des effets en cascade, qui transcendent les frontières politiques traditionnelles* » (p.2)
- **Scheffran (2025)** - Cambridge University Press :
  - « *Une polycrise mondiale a été définie comme l'enchevêtrement causal de crises dans de multiples systèmes mondiaux d'une manière qui dégrade considérablement les perspectives de l'humanité* » (p.2)

- **Cigref (2025)** - Club informatique des grandes entreprises françaises :
  - « *Le Système (D)SI évolue dans un environnement global instable, marqué par des tensions géopolitiques, des risques cyber croissants et des contraintes budgétaires persistantes.* » (p.107)

La robustesse numérique comme réponse systémique

Rôle dans le livre blanc : Approche alternative à l'optimisation pure, privilégiant la résilience et la continuité.

- **Cigref (2025)** - Validation de l'approche :
  - « *Son positionnement stratégique est le fruit d'une optimisation des contraintes, en particulier financières et sécuritaires. Le Système (D)SI assume pleinement le rôle de fonction support sur laquelle les métiers peuvent s'appuyer avec confiance et fiabilité.*" (p.107)
  - « *Il privilégie la robustesse, la résilience opérationnelle et la continuité des activités.* » (p.107)
- **Swiss Re (2024)** - Mission de construction de résilience :
  - « *Chaque année, Swiss Re SONAR informe et inspire des conversations sur les risques émergents, aidant l'industrie de l'assurance et ses clients à continuer à construire la résilience* » (p.2)
- **Nature Communications (2025)** - Stress-testing systémique :
  - « *Approche de test de résistance de la résilience des infrastructures : va au-delà des problèmes isolés [...] vers des tests de résistance systémiques tenant compte de l'interconnexion entre les systèmes* » (p.3)

La fragilité systémique

Rôle dans le livre blanc : Diagnostic de base qui justifie l'urgence de l'approche de robustesse.

- **OCDE (2025)** - Organisation internationale de référence :
  - « *Tous les 177 contextes analysés par le cadre multidimensionnel de fragilité de l'OCDE sont exposés à un certain niveau de fragilité* » (p.6)
  - « *C'est une époque définie par de multiples crises, chocs et incertitudes* » (p.6)
- **AXA (2024)** - Données statistiques massives :
  - « *87 % des experts estiment que le monde est plus vulnérable aux risques qu'il ne l'était il y a cinq ans* » (p.4)
  - « *92 % des experts ont répondu oui [concernant l'augmentation du nombre de crises], tout comme 90 % de la population générale* » (p.4)

- **Scheffran (2025)** - Analyse scientifique :
  - « *La polycrise actuelle est sans précédent, en partie parce que l'interconnectivité et l'intensité des interactions ont considérablement augmenté avec la mondialisation* » (p.3)
- **Allianz (2025)** - Validation empirique massive :
  - « *La poussée vers le progrès technologique et l'efficacité affecte la résilience des chaînes d'approvisionnement. De nos jours, une défaillance ou une perturbation dans n'importe quel segment d'une chaîne d'approvisionnement tend à être plus grave, laissant un temps de réponse minimal* » (Michael Bruch, p.15)
  - *« L'automatisation et la numérisation ont considérablement accéléré les processus, ce qui peut parfois submerger les individus en raison du rythme rapide et de la complexité des [systèmes] modernes* » (p.15)
- **Swiss Re (2024)** - Autorité mondiale en risques émergents : « *Chaînes d'approvisionnement mondiales – la résilience contre le risque d'interruption d'activité s'affaiblit* » (p.24) :
  - *« Comme l'expérience de la pandémie de COVID-19 l'a montré, les chaînes d'approvisionnement peuvent être fortement perturbées, entraînant des implications durables" »* (p.24)
- **Cigref (2025)** - Perspective des directions numériques :
  - « *Dans ce contexte, il adopte une posture centrée sur la robustesse, la résilience opérationnelle et la continuité des activités." (p.107)*

Principes de robustesse

Non-régression capacitaire

Rôle dans le livre blanc : Premier principe fondamental préservant les compétences critiques.

- **Cigref (2025)** - Validation institutionnelle directe :
  - *« Son modèle repose sur une centralisation forte, une valorisation du facteur humain et une expertise technique doublée d'une fine connaissance des incidents passés. »* (p.8)
  - *« "Le Système (D)SI fait de la gestion des risques un moyen essentiel de sa performance. »* (p.108)
- **OPHIR (2025)** - Approche par les capacités d'Amartya Sen :
  - *« La résilience [...] nourrit essentiellement la capacité individuelle et collective de créer ou de reconstruire de manière créative des vies de valeur dans des contextes changeants »* (p.3)
- **CCL (2025)** - Critique du scientisme — autre nom du techno-solutionnisme :
  - *« Scientisme : dépendance excessive à la science et à la technologie comme solution universelle » ("Scientism : Overreliance on science and technology as universal solution").* (p.4-5)

Résilience organisée

Rôle dans le livre blanc : Second principe structurant l'organisation pour la robustesse.

- **Cigref (2025)** - Application concrète du principe :
  - *« Les investissements sont orientés vers la sécurisation des infrastructures critiques, avec une faible exposition à l'innovation de rupture. »* (p.8)
  - *« L'IA est utilisée avec parcimonie, le cloud est sélectif, et les enjeux environnementaux sont intégrés de manière pragmatique. »* (p.8)
- **Nature Communications (2025)** - Cadre des capacités de résilience :
  - *« Application de techniques de cartographie causale pour saisir les implications des risques et des crises se propageant entre les systèmes »* (p.3)
- **OPHIR (2025)** - Investissement préventif :
  - *« Certains types de résilience doivent être construits à l'avance [...] les scénarios d'urgence doivent être répétés »* (p.15)

Archétypes et stratégies

Typologie des approches (Cigref 2025)

Rôle dans le livre blanc : Validation de la diversité des stratégies de robustesse (polysolutions).

Les 4 archétypes identifiés :

- **Archétype 1 « Le Labo »** : Innovation de rupture comme réponse aux crises
- **Archétype 2 « Le Caméléon »** : Agilité et adaptabilité permanente
- **Archétype 3 « L'Équipe Responsable »** : Durabilité comme facteur de résilience
- **Archétype 4 « Le Système (D)SI »** : Robustesse et continuité opérationnelle

Convergence avec le livre blanc : L'Archétype 4 valide directement l'approche de robustesse numérique *: « Son objectif principal est d'assurer la continuité des activités par la robustesse, en sécurisant architectures, produits et services numériques. "* » (p.108)

Évolution vers la robustesse

Rôle dans le livre blanc : Transition des organisations vers des approches plus robustes.

- **Cigref (2025)** - Émergence de l'archétype robuste :
  - *« Le Système (D)SI évolue dans un environnement dont il réussit à optimiser les contraintes. Il privilégie la robustesse, la résilience opérationnelle et la continuité des activités. »* (p.8)
- **Allianz (2025)** - Prise de conscience des limites de l'optimisation :
  - *« La poussée vers le progrès technologique et l'efficacité affecte la résilience des chaînes d'approvisionnement »* (p.15)

Mécanismes de fragilisation

Mécanismes de contagion et cascade

Rôle dans le livre blanc : Explication de la propagation des crises entre systèmes.

- **Liu & Renn (2025)** - Typologie des disruptions :
  - *« Les perturbations intra-systémiques peuvent se propager d'une partie d'un système à l'ensemble du système via des chaînes de cause à effet contagieuses dans le réseau du système, tandis que les perturbations inter-systémiques débordent des limites du système vers d'autres systèmes »* (p.2)
- **Scheffran (2025)** - Mécanisme de réaction en chaîne :
  - *« Lorsque le nombre ou la densité d'événements interconnectés dépasse un seuil et devient 'surcritique', la dynamique dévastatrice se déclenche et se propage d'elle-même comme une réaction en chaîne incontrôlée »* (p.3)
- **PolyCIVIS (2025)** - Effets trans-frontières :
  - *« Les effets trans-frontières font référence à la capacité de la polycrise à transcender des domaines spécifiques et à impacter divers aspects de la société »* (p.3)
- **Nature Communications (2025)** - Framework Cascade Institute :
  - *« Application de techniques de cartographie causale pour saisir les implications des risques et des crises se propageant entre les systèmes, en distinguant entre les stress à évolution lente et les événements déclencheurs imprévisibles à évolution rapide »* (p.3)
- **Allianz (2025)** - Business interruption comme conséquence systémique :
  - *« L'interruption d'activité (BI) s'est classée soit n°1 soit n°2 dans chaque Baromètre des risques d'Allianz au cours de la dernière décennie… L'interruption d'activité est généralement une conséquence d'événements comme une catastrophe naturelle, une cyber-attaque ou une panne, une insolvabilité ou des risques politiques comme un conflit ou des troubles civils »* (p.15)
- **Swiss Re (2024)** - Effets en cascade systémiques :
  - *« Au-delà des infrastructures brisées – les effets en cascade des catastrophes naturelles »* (p.34)
- **Cigref (2025)** - Gestion des risques systémiques :
  - *« La gestion des risques est au cœur de la performance du Système (D)SI, qui intègre des dispositifs de surveillance et de veille, de traçabilité et de remédiation. »* (p.108)

Mécanismes de verrouillage technologique

Rôle dans le livre blanc : Analyse des dépendances et 📖 Point de défaillance unique (Single Point of Failure / SPOF).

- **AXA (2024)** - Dépendances critiques :
  - *« L'inquiétude concernant ce risque est probablement étroitement liée à [...] la dépendance croissante vis-à-vis des grands fournisseurs »* (p.10)
- **CCL (2025)** - Scientisme technologique :
  - *« Scientisme : dépendance excessive à la science et à la technologie comme solution universelle »* (p.4-5)
- **PolyCIVIS (2025)** - Techno-solutionnisme :
  - *« Le techno-solutionnisme climatique [...] pose une menace significative. Cette croyance peut conduire à la complaisance et à des angles morts »* (p.5)
- **Swiss Re (2024)** - Big Tech comme risque de dépendance :
  - *« Big Tech – un risque de dépendance » ("Big Tech – a dependency risk")* (p.26)
  - *« IA – impacts assurantiels non intentionnels et leçons du cyber silencieux »* (p.46)
- **Cigref (2025)** - Approche de réduction des dépendances :
  - *« Une part significative est co-développée avec un nombre restreint d'éditeurs logiciels de confiance, dans une logique partenariale de long terme. Les investissements ciblent les étapes critiques des différentes chaînes de valeur et visent à réduire les dépendances extérieures. »* (p.108)

Approches transformationnelles

Polysolutions

Rôle dans le livre blanc : Vision intégrée de la réponse aux crises multiples.

- **PolyCIVIS (2025)** - Concept novateur :
  - *« Pour répondre aux complexités de la polycrise, ce document fondateur préconise des 'polysolutions' – des approches intégrées et multiformes qui s'attaquent aux causes profondes des crises interconnectées" »*p.2)

Coopération et biens communs

Rôle dans le livre blanc : Vision collaborative de mutualisation des ressources.

- **AXA (2024)** - Collaboration public-privé :
  - *« Atténuer l'impact [...] exige une collaboration et un partenariat accrus entre les secteurs privé et public »* (p.25)
- **CCL (2025)** - Exemple historique :
  - *« L'Initiative mondiale pour l'éradication de la poliomyélite illustre cela, réunissant l'OMS, l'UNICEF, Rotary International, les CDC, et les gouvernements nationaux »* (p.2)
- **OCDE (2025)** - Coopération comme catalyseur :
  - *« La coopération au développement [...] peut agir comme catalyseur pour stimuler le développement, prévenir les conflits et construire de meilleurs avenirs »* (p.4)
- **Cigref (2025)** - Mutualisation des actifs :
  - *« Le Système (D)SI optimise les coûts et mutualise le plus possible ses actifs numériques. »* (p.108)

A.2 Matrice de correspondance — Concepts du livre blanc × Références majeures

Le tableau ci-dessous permet d'identifier les sources avec leur niveau de pertinence pour chacun des concepts et principes utilisés dans ce livre blanc.

Sources

ALZ : Allianz Risk Barometer 2025

AXA : AXA Future Risks Report 2024

CCL : Center for Creative Leadership - Leading Beyond Barriers (2025)

CIG : Cigref - 4 Archétypes de la fonction numérique pour 2040 (2025)

ERC : European Research Council - Transformative change for a sustainable future (2024)

L&R : Liu & Renn - Polycrisis and Systemic Risk (2025)

NCO : Nature Communications - Systemic risk assessment framework (2025)

OCD : States of Fragility 2025

OPH : Oxford - Resilient Human Development (2025)

PCI : PolyCIVIS - From Polycrisis to Polysolutions (2025)

SCH : Scheffran - Systemic risks and governance (2025)

SRE : Swiss Re SONAR 2024

ZPW : Zaki, Pattyn & Wayenberg - Policymaking in polycrises (2024)

Légende

A : Validation forte et détaillée

B : Validation substantielle

C : Mention ou validation partielle

- : Non mentionné

	ALZ	AXA	CCL	CIG	ERC	L&R	NCO	OCD	OPH	PCI	SCH	SRE	ZPW
1. CONCEPTS													
Polycrise	–	A	A	A	C	A	A	C	C	A	A	–	A
Fragilité systémique	A	A	C	A	C	B	B	A	B	B	B	A	C
Risques systémiques	A	A	C	A	C	A	A	B	C	B	A	B	B
Interconnexion/Interdépendance	A	A	B	B	B	A	A	C	C	A	A	A	B
2. PRINCIPES													
Non-régression capacitaire	C	–	A	A	–	–	–	–	A	B	–	–	–
Résilience organisée	B	C	B	A	B	B	A	B	A	B	B	A	C
Optimisation des contraintes	C	–	C	A	–	C	C	C	C	C	C	C	C
3. STRATÉGIES													
Diversité des approches	–	–	–	A	–	–	–	–	–	A	–	–	–
Robustesse vs Agilité	B	–	C	A	C	B	A	C	B	C	B	C	C
Innovation mesurée	C	C	C	A	C	–	–	–	C	C	C	C	–
4. MÉCANISMES													
Contagion/Cascade	A	B	C	B	–	A	A	C	–	A	A	A	B
Mécanismes géopolitiques	B	A	C	A	–	C	C	B	–	C	A	C	C
Verrouillage technologique	B	A	B	B	C	C	C	–	–	A	C	A	–
Dépendances critiques	B	A	C	A	–	C	C	C	–	B	C	A	–
Biais cognitifs	C	A	A	–	–	C	–	–	C	A	–	C	–
5. CONSTRUCTION													
Approche multidimensionnelle	B	B	A	B	A	A	B	A	B	A	B	B	A
Gouvernance anticipative	C	C	C	B	C	A	A	B	B	B	A	B	B
Gestion des risques	B	C	C	A	–	C	C	C	C	C	C	B	C
Investissements préventifs	C	–	C	A	C	C	C	C	A	C	C	C	C
6. TRANSFORMATIONS													
Coopération/Biens communs	C	A	A	B	B	B	C	B	C	A	B	C	C
Leadership transformationnel	C	B	A	C	B	C	C	C	A	B	C	C	B
Sobriété/Post-croissance	C	–	A	C	B	–	–	–	C	A	B	B	–
7. SCÉNARIOS													
Mégapanne (CrowdStrike)	–	A	–	–	–	–	–	–	–	–	–	–	–
Business interruption	A	–	–	C	–	–	–	–	–	–	–	A	–
Crise de confiance	C	B	C	C	–	C	–	–	C	A	C	C	C
Désinformation/IA	C	A	–	C	–	–	–	–	–	B	–	B	–
8. OUTILS													
Matrice de criticité	–	–	–	–	–	B	C	B	C	–	C	–	–
Chaos Engineering	–	–	–	–	–	–	B	–	B	–	–	–	–
Métriques d’autonomie	–	–	B	B	–	–	–	–	B	–	–	–	–

Annexe B

Les principes fondamentaux de la robustesse

Face à la dépendance croissante aux technologies numériques, deux principes guident une approche résiliente et durable. Ces principes ne visent pas à rejeter la technologie, mais à établir un cadre de réflexion permettant d'éviter le piège du techno-solutionnisme.

Ce concept, critiqué par des réseaux académiques comme PolyCIVIS, décrit la croyance selon laquelle l'innovation technologique seule peut résoudre des problèmes complexes, créant ainsi un « faux sentiment de sécurité » et retardant les changements structurels nécessaires [76].

L'objectif : construire des organisations qui tirent parti du numérique sans en devenir les otages.

B.1 La non-régression : préserver l'autonomie fondamentale

Le premier principe propose un critère simple mais puissant pour évaluer toute innovation technologique. Il s'inspire de l'approche par les capacités (Capability Approach), développée par l'économiste et philosophe Amartya Sen (Prix Nobel d'économie 1998) et au cœur des travaux d'institutions comme l'Oxford Poverty & Human Development Initiative (OPHIR) [46].

L'idée centrale est que le développement ne doit pas être mesuré par les ressources (la technologie), mais par la capacité réelle des individus et des organisations à accomplir ce qui a de la valeur pour eux (leur agence ou pouvoir d'agir) [94].

Appliqué au numérique, ce principe de non-régression capacitaire signifie que la technologie doit augmenter les capacités et l'autonomie, non les remplacer.

Le test décisif : si la technologie disparaît, l'organisation ne doit pas se retrouver dans une situation où ses capacités fondamentales sont dégradées par rapport à la situation antérieure. Selon ce principe, l'adoption technologique ne doit pas entraîner une perte de compétence ou d'agence.

Applications concrètes du principe de non-régression

La navigation maritime illustre parfaitement ce principe. Le GPS a révolutionné la navigation, mais l'Organisation Maritime Internationale impose aux officiers de maintenir leurs compétences en navigation astronomique [96].

Résultat : lors des brouillages GPS en mer Noire (2017-2022), les navires ont pu continuer à naviguer.

De même, en agriculture de précision, une étude de l'INRAE montre que les fermes « augmentées » (technologie + savoirs traditionnels) ont une productivité 23 % supérieure aux fermes « substituées » (technologie seule) en cas de défaillance technique [97].

Le secteur médical offre un contre-exemple instructif. Le système Watson d'IBM, retiré après avoir recommandé des traitements dangereux, illustre les risques de la substitution pure [98]. À l'inverse, les hôpitaux qui maintiennent les compétences cliniques parallèlement aux outils d'IA évitent ces erreurs catastrophiques.

La crise de la dématérialisation des services publics français (2019-2024) constitue un exemple à grande échelle de violation du principe de non-régression. Treize millions de Français se trouvent en difficulté avec les démarches exclusivement numériques, ce que le Défenseur des droits a dénoncé comme une « dématérialisation à marche forcée » [104].

B.2 La résilience organisée : construire des capacités face à la polycrise

Lorsque la technologie devient indispensable pour des services critiques, car les capacités humaines ne sont plus suffisantes pour les assurer, le principe de non-régression atteint ses limites. Il faut alors passer à une logique de résilience organisée.

Ce second principe ne se contente pas de préserver les capacités existantes, mais vise à en construire de nouvelles, voire remplacer les existantes qui sont insuffisantes, pour naviguer dans un contexte de polycrise.

La recherche sur le développement humain et la gestion des catastrophes, notamment les travaux de l'OCHA (Bureau de la coordination des affaires humanitaires des Nations unies) repris par OPHIR, offre un cadre puissant pour structurer cette résilience en trois niveaux de capacités [94].

Capacités d'absorption (Absorptive Capacities)

Il s'agit de la capacité à encaisser les chocs immédiats sans altérer la structure fondamentale du service. C'est la résilience au sens classique, qui repose sur la redondance.

Cependant, face à la polycrise, où les pannes peuvent être longues, les chaînes d'approvisionnement rompues, les événements extrêmes destructeurs, les décisions politiques bloquantes, une simple redondance devient insuffisante. Il faut évoluer vers une sur-redondance adaptée (multi-sites, stocks stratégiques) et la capacité de dégradation gracieuse (maintenir les fonctions essentielles en sacrifiant le reste), comme l'a fait WhatsApp lors de la panne de Facebook en 2021 [102].

Capacités d'adaptation (Adaptive Capacities)

Ce niveau va au-delà de la simple absorption des chocs. Il s'agit de la capacité à ajuster ses stratégies et à diversifier ses options lorsque le contexte change durablement. Cela implique une diversification radicale des dépendances, non seulement technologique (multi-cloud, on-premise) mais aussi géopolitique (fournisseurs de différents blocs économiques).

C'est la leçon apprise par Toyota qui, malgré sa stratégie multi-fournisseurs, a dû augmenter ses stocks tampons pour faire face aux ruptures d'approvisionnement prolongées [110]. Le Chaos Engineering, popularisé par Netflix, est une méthode pour développer cette capacité d'adaptation en testant continuellement la réponse du système à des pannes délibérées [103].

Capacités de transformation (Transformative Capacities)

C'est le niveau de résilience le plus élevé. Il ne s'agit plus seulement de s'adapter, mais de transformer les structures et les logiques profondes qui créent la vulnérabilité. Comme le souligne une étude de Nature Communications, il faut envisager des « réponses transformationnelles » qui s'attaquent aux racines du risque systémique [82].

Cela peut se traduire par une dégradation volontaire et planifiée, comme la réduction de la qualité vidéo par Netflix et YouTube en 2020 pour préserver la bande passante européenne [107], ou l'utilisation de files d'attente virtuelles par Roland Garros pour maîtriser les pics de charge [106]. C'est un changement de paradigme : la performance n'est plus l'unique objectif et devient même secondaire ; la stabilité et la soutenabilité deviennent les critères de conception essentiels.

B.3 Articulation des principes : une grille de décision

Pour déterminer quel principe appliquer à un service donné, quatre questions clés structurent la réflexion :

1. Le service est-il critique ou important pour l'activité ?
   (a) Si non, le principe 2 ne s'applique pas systématiquement.
   (b) Si oui, continuer l'évaluation.
2. La fonction existait-elle avant la technologie ?
   (a) Si oui, le principe 1 (non-régression) s'applique : la technologie doit augmenter, pas remplacer.
   (b) Si non, le principe 2 (résilience organisée) devient central.
3. Un retour arrière est-il envisageable ?
   (a) Si oui, il faut maintenir impérativement les compétences traditionnelles.

(b) Si non, il faut investir pertinemment dans la sur-redondance et les alternatives.

4. Quelle durée de panne est supportable ?

(a) Mois : la redondance classique peut suffire.

(b) Semaines : il faut envisager de la sur-redondance et des stocks tampons.

(c) Jours : il faut repenser entièrement l'architecture.

Exemples d'application

Un hôpital évaluant son système de dossiers patients électroniques illustre la complexité de cette grille. Le service est critique (continuité des soins vitale), la fonction existait (dossiers papier), mais le volume actuel rend le retour total impossible. La durée de panne tolérable étant de quelques heures seulement, une solution maximale s'impose : système électronique principal sur trois sites minimum, procédures papier d'urgence maintenues, personnel formé mensuellement aux deux méthodes, et stocks de consommables pour trois mois.

La crise énergétique européenne (2022-2024) a validé ces principes à grande échelle. Les entreprises ayant maintenu des contrats énergétiques diversifiés ont survécu, tandis que celles dépendant d'une seule source (gaz russe) ont subi des arrêts prolongés. Les datacenters nordiques valorisant le refroidissement naturel ont gagné en résilience [113].

---

[76] F. Schreiber et al. *From Polycrisis to Polysolutions : An Interdisciplinary Approach to Complex Global Challenges*. Foundational Brief. PolyCIVIS, mars 2025. URL : https://civis.eu/storage/files/1foundational-brief-polycrisis-and-policy-series-formatted-version2-schreiber-etal-mar-2025.pdf.

[82] A. Gambhir et al. "A Systemic Risk Assessment Methodological Framework for the Global Polycrisis". In : *Nature Communications* (2024). URL : https://www.nature.com/articles/s41467-025-62029-w.

[94] S. Alkire. *Resilient Human Development*. Rapp. tech. OPHIRP_68a_2025. Oxford Poverty et Human Development Initiative, 2025. URL : https://ophi.org.uk/sites/default/files/2025-09/OPHIRP_68a_2025_Resilient_%28Alkire%29.pdf.

[95] ICJ. *Principle of Non-Regression in Environmental Law*. 2018. URL : https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/an-international-law-principle-of-nonregression-from-environmental-protections/DFB6236C0504491E00B4174EE6D13186.

[96] IMO. *STCW Convention Requirements*. Rapp. tech. International Maritime Organization, 2023. URL : https://www.imo.org/en/ourwork/humanelement/pages/stcw-conv-link.aspx.

[97] INRAE. *Agriculture Numérique et Résilience*. Rapp. tech. 2024. URL : https://hal.inrae.fr/hal-05290456v1/file/LActu-newsletter-2024.pdf.

[98] IEEE Spectrum. "How IBM Watson Overpromised and Underdelivered on AI Health Care". In : *IEEE Spectrum* (2019). URL : https://spectrum.ieee.org/how-ibm-watson-overpromised-and-underdelivered-on-ai-health-care.

[99] EASA. *Certification Specifications for Large Aeroplanes*. Rapp. tech. European Union Aviation Safety Agency, 2023. URL : https://www.easa.europa.eu/en/document-library/certification-specifications.

[100] Netflix Tech Blog. *Multi-Region Resilience*. 2023. URL : https://netflixtechblog.com/.
[101] Basel Committee. *Principles for Operational Resilience*. Rapp. tech. Bank for International Settlements, 2023. URL : https://www.bis.org/bcbs/publ/d516.htm.
[102] Facebook Engineering. *More details about the October 4 outage*. 2021. URL : https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/.
[103] Netflix. *Chaos Engineering Principles*. 2023. URL : https://www.gremlin.com/community/tutorials/chaos-engineering-the-history-principles-and-practice.
[104] Défenseur des droits. *Rapport sur la dématérialisation des services publics*. Rapp. tech. 2024. URL : https://www.defenseurdesdroits.fr/rapport-dematerialisation-et-inegalites-dacces-aux-services-publics-266.
[105] Signal Blog. *Maintaining Service During the Facebook Outage*. 2021. URL : https://signal.org/blog/.
[106] Queue-it. *Roland Garros Virtual Queue Case Study*. 2024. URL : https://queue-it.com/.
[107] EU Commission. *Streaming Platforms Bandwidth Reduction Agreement*. Rapp. tech. European Commission, 2020. URL : https://commission.europa.eu/strategy-and-policy/coronavirus-response/digital-solutions-during-pandemic_en.
[108] SEC. *Market Circuit Breakers Rules*. Rapp. tech. U.S. Securities et Exchange Commission, 2023. URL : https://www.sec.gov/rules-regulations.
[109] CrowdStrike. *Post-Incident Analysis Report*. Rapp. tech. Rapport officiel post-incident détaillant la mise à jour défectueuse du 19 juillet 2024 qui a affecté 8,5 millions de machines Windows. 2024. URL : https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.
[110] Toyota. *Supply Chain Resilience Strategy*. Integrated Report 2023. 2023. URL : https://global.toyota/pages/global_toyota/ir/library/annual/2023_001_integrated_en.pdf.
[111] ERCOT. *Texas Grid Failure Analysis*. Rapp. tech. 2021. URL : https://energy.utexas.edu/research/ercot-blackout-2021.
[112] ANSSI. *Panorama de la cybermenace 2024*. Rapp. tech. Agence nationale de la sécurité des systèmes d'information, 2024. URL : https://cyber.gouv.fr/publications/panorama-de-la-cybermenace-2024.
[113] European Energy Agency. *Datacenter Energy Resilience Report*. Rapp. tech. 2024. URL : https://www.eea.europa.eu/.

Annexe C

La matrice de criticité

C.1 Introduction

Face à la polycrise décrite dans ce livre blanc avec ses impacts sur le numérique, une tentation naturelle émerge : vouloir tout protéger — niveau de redondance, fréquence et conservation des sauvegardes et des archives, durée de vie illimitée. Cette approche maximaliste est non seulement coûteuse, elle est aussi contre-productive. Elle dilue les ressources sur des composants secondaires au détriment des éléments réellement critiques, et génère une complexité qui devient elle-même une source de fragilité.

La matrice de criticité propose une alternative rationnelle : identifier et prioriser ce qui est réellement critique pour la pérennité de votre organisation. Elle commence par une question fondamentale : « Qu'est-ce qui fait tourner mon organisation, et qu'est-ce qui la mettrait en péril si cela s'arrêtait ? »

Cette approche s'inscrit dans une démarche de sobriété numérique et d'ataraxie numérique, concepts développés par Stéphane Crozat [67] qui invitent à se questionner sur ce qui est nécessaire, utile, voire agréable, plutôt que de céder à l'accumulation technologique. Elle s'appuie également sur les travaux du NIST [118] sur l'analyse de criticité et sur les recherches de Rinaldi et ses collègues sur les interdépendances des infrastructures critiques [56].

Cette annexe détaille la méthodologie complète d'utilisation de la matrice, depuis l'identification des processus métier critiques jusqu'au positionnement des composants numériques qui les supportent.

C.2 Comprendre la matrice : deux axes, neuf intersections, trois zones de risque

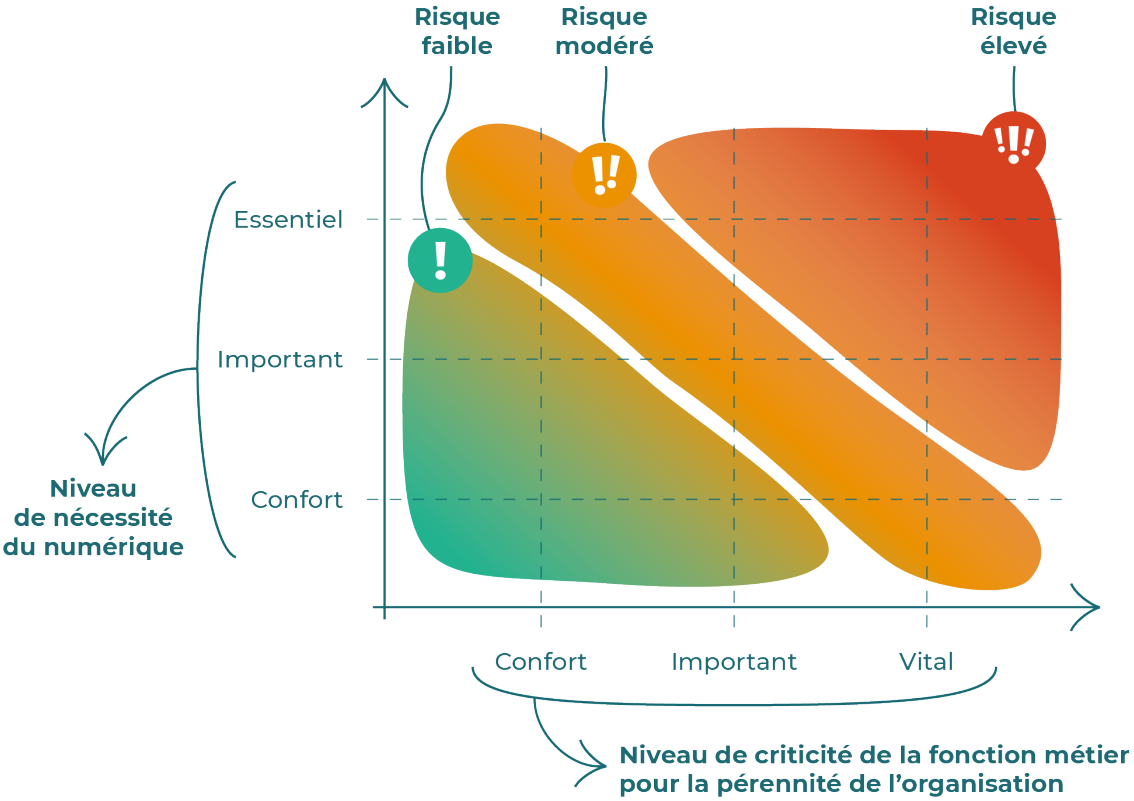


FIG. C.2.1 : Matrice de criticité

Les deux axes d'évaluation

La matrice croise deux dimensions complémentaires qui, ensemble, déterminent le niveau de risque.

L'axe vertical : le degré de dépendance au numérique.

- Cet axe mesure à quel point votre processus métier dépend du numérique pour fonctionner. Il distingue trois niveaux :

  Confort : des alternatives non numériques existent et permettent de continuer l'activité ;

  Important : le numérique est nécessaire pour l'efficacité, mais des solutions dégradées temporaires sont possibles ;

  Essentiel : sans numérique, le processus s'arrête immédiatement.

L'axe horizontal : l'impact de l'arrêt de l'activité portée par le numérique sur la pérennité de l'organisation.

- Cet axe évalue les conséquences d'un arrêt du processus métier sur votre organisation. Il distingue également trois niveaux :

  Confort : impact limité, récupération rapide sans conséquence durable

  Important : perturbation notable mais gérable, l'organisation peut absorber le choc

  Vital : menace la pérennité (financière, réputationnelle ou réglementaire) et la capacité à continuer à produire

Le croisement : neuf intersections, trois zones de risque

Le croisement de ces deux axes produit une matrice de neuf cellules, regroupées en trois zones de risque selon un code couleur :

Zone verte (risque faible) : l'impact d'un arrêt du numérique reste limité. Ces processus et les composants qui les supportent peuvent se contenter de mesures de protection standard, d'alternatives low-tech, voire de renoncement.

Zone orange (risque modéré) : le risque est intermédiaire. Ces processus nécessitent des mesures de protection proportionnées.

Zone rouge (risque élevé) : le risque est fort. Ces processus exigent une attention maximale et de fortes mesures de résilience.

C.3 Méthodologie d'évaluation : quatre étapes, du métier vers le numérique

Étape 1 : Identifier les processus métier critiques

Commencez par lister les processus métier essentiels au fonctionnement de votre organisation. Un processus métier est une activité ou un ensemble d'activités qui créent de la valeur pour vos clients, vos usagers, ou votre mission.

Exemples de processus métier :

Production : Fabrication de produits, transformation de matières. premières, assemblage

Vente et relation client : Prospection, devis, prise de commandes, facturation, service après-vente.

Logistique : Approvisionnement, gestion des stocks, expédition, livraison.

Ressources humaines : Recrutement, gestion administrative du personnel, paie, formation.

Finance et comptabilité : Trésorerie, comptabilité générale, reporting financier.

R&D : Conception, prototypage, tests, validation

Services aux usagers (secteur public) : Délivrance d'actes administratifs, accueil du public, instruction de dossiers.

Dix à quinze processus métier suffisent pour une première itération. Concentrez-vous sur ceux qui ont un impact direct sur votre pérennité. Cette approche rejoint la méthodologie du NIST qui recommande de partir des objectifs organisationnels avant de descendre vers les systèmes techniques.

Étape 2 : Évaluer la dépendance au numérique de chaque processus

Pour chaque processus métier identifié, posez-vous la question : « Ce processus peut-il fonctionner sans numérique ? »

Grille d'évaluation :

Confort : Le numérique facilite le processus, mais des alternatives non numériques existent (papier, téléphone, processus manuels) et permettent de continuer sans impact majeur. Vous pouvez basculer sur ces alternatives pendant plusieurs jours ou semaines.

Important : le numérique est nécessaire pour l'efficacité opérationnelle. Des alternatives existent mais entraînent une perte de performance significative. Vous pouvez tenir quelques jours en mode dégradé, mais pas indéfiniment.

Essentiel : sans numérique, le processus s'arrête immédiatement ou dans les heures qui suivent. Aucune alternative viable n'existe à court terme. L'activité est paralysée.

Exemple fictif :

Processus métier	Dépendance	Justification
Production automatisée	Essentiel	Sans système de pilotage numérique, les machines ne fonctionnent pas. Aucun mode manuel.
Facturation	Important	Possible manuellement (calculatrice, papier), mais très lent et source d'erreurs. Intenable au-delà de quelques jours.
Paie	Important	Calculs manuels possibles en théorie, mais complexité réglementaire rend cela très difficile en pratique.
Communication RH	Important	Les communications peuvent se faire par échange de messages papier sans dégrader le service.
Accueil du public	Important	Peut se faire sans numérique (guichet physique, formulaires papier), mais difficilement par manque de personnel.

Étape 3 : Évaluer l'impact d'un arrêt du processus sur la pérennité

Pour chaque processus métier, posez-vous la question : « Si ce processus s'arrêtait pendant plusieurs jours, quel serait l'impact sur la pérennité de mon organisation ? »

Grille d'évaluation :

Confort : Impact limité sur le chiffre d'affaires, la réputation ou les obligations réglementaires. Récupération rapide sans conséquence durable. Désagrément temporaire pour certains collaborateurs ou usagers, mais pas de menace pour l'organisation.

Important : Impact notable mais gérable. Perte financière modérée, dégradation temporaire de la réputation, ou perturbation de certaines activités non critiques. Votre organisation peut absorber le choc et récupérer sans séquelles majeures.

Vital : Impact majeur menaçant la pérennité. Perte financière significative (arrêt du chiffre d'affaires, pénalités contractuelles), atteinte grave à la réputation, non-respect d'obligations réglementaires critiques, ou paralysie des activités essentielles. Risque de faillite, de crise majeure, ou de mise en cause de la responsabilité.

Exemple fictif :

Processus métier	Impact	Justification
Production automatisée	Vital	Arrêt rapide du CA, voire immédiat, risque majeur de perte de clients, pénalités de retard.
Facturation	Vital	Trésorerie en danger.
Paie	Vital	Obligations sociales non respectées, crise sociale interne, risque de poursuites.
Communication RH	Confort	Ralentissement de la coordination, mais pas d'impact majeur à court terme.
Accueil du public	Important	Mécontentement des usagers, dégradation de l'image.

La matrice correspondante à cet exemple fictif devient :

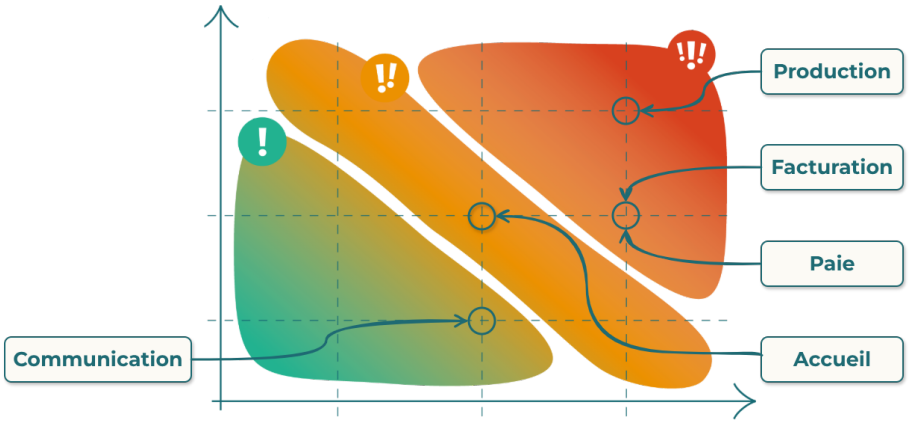


Fig. C.3.1 : Matrice illustrée

Étape 4 : Identifier les composants numériques qui supportent ces processus

Pour chaque processus, identifiez les composants numériques qui le supportent. Un composant peut être un système d'information, une application, une infrastructure, ou un service numérique.

Méthode : Demandez-vous : *« Quels systèmes numériques permettent à ce processus de fonctionner ? »*

Exemples de correspondance processus → composants :

Processus métier	Composants numériques associé
Production automatisée	Système SCADA, automates industriels, réseau OT, serveur de supervision
Paie	Logiciel de paie, système RH (SIRH), serveur d'authentification, base de données RH
Facturation	Module facturation de l'ERP, base de données clients (CRM), système de paiement en ligne
Vente	Site web e-commerce, CRM, système de paiement, plateforme d'hébergement
Logistique	Module logistique de l'ERP, système de gestion d'entrepôt (WMS), lecteurs de codes-barres
Communication	Messagerie électronique, visioconférence, intranet, serveur de fichiers

Point crucial sur les interdépendances : un composant numérique peut supporter plusieurs processus métier. Les travaux de Rinaldi et ses collègues [56] ont démontré que les interdépendances créent des cascades de défaillances qui amplifient considérablement l'impact d'une panne initiale.

De même, il faut évaluer les interdépendances entre les fonctions métier afin de bien les positionner dans la matrice et de surévaluer les fonctions qui sont des dépendances pour plusieurs autres..

Exemples d'interdépendances numériques :

Un serveur de base de données qui alimente à la fois la production, la facturation et la logistique est bien plus critique qu'un serveur isolé, même s'ils ont la même fonction technique.

Un système d'authentification centralisé (Active Directory, SSO) qui contrôle l'accès à tous les systèmes devient un point de défaillance unique dont la criticité dépasse celle de chaque système pris isolément.

Un bus applicatif qui orchestre les échanges entre systèmes (ERP ↔ CRM ↔ logistique) peut paralyser l'ensemble des processus métier s'il défaille.

C.4 Conclusion : de l'évaluation métier à l'action numérique

La matrice de criticité est un outil de décision pour identifier et prioriser ce qui est réellement critique pour votre pérennité. En partant des processus métier plutôt que des systèmes techniques, vous restez maître de l'analyse et assurez que les investissements en résilience servent réellement votre mission.

Cette méthodologie permet de passer d'une vision technique (« Quels sont mes systèmes ? ») à une vision métier (« Qu'est-ce qui est vraiment critique pour ma pérennité ? »), puis de redescendre vers le numérique de manière ciblée (« Quels composants numériques dois-je protéger en priorité ? »).

Une fois cette évaluation réalisée, vous pourrez appliquer les deux principes de résilience (non-régression et renforcement de la redondance) et décliner les actions concrètes à travers les trois tours de renforcement progressif détaillés dans les chapitres suivants. La matrice structure votre démarche en permettant de commencer par les processus et composants en zone rouge, puis de traiter progressivement ceux en zone orange, et enfin d'interroger la pertinence de ceux en zone verte dans une logique de sobriété numérique [67].

La matrice est votre boussole pour naviguer par temps d'incertitude. Elle aide à choisir le bon cap en fonction de vos contraintes et de vos priorités métier.

---

[56] Steven M. Rinaldi, James P. Peerenboom et Terrence K. Kelly. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". In : *IEEE Control Systems Magazine* 21.6 (2001), p. 11-25. DOI : 10.1109/37.969131. URL : https://doi.org/10.1109/37.969131.

[67] Stéphane Crozat. *Vers une ataraxie numérique : low-technicisation et convivialité*. 2021. URL : https://aswemay.fr/co/040011.html.

[118] Celia Paulsen et al. *Criticality Analysis Process Model : Prioritizing Systems and Components*. Rapp. tech. NIST Interagency Report 8179. National Institute of Standards et Technology, 2018. DOI : 10.6028/NIST.IR.8179. URL : https://doi.org/10.6028/NIST.IR.8179.

Pour aller plus loin

[119] International Organization for Standardization. *Security and resilience — Business continuity management systems — Requirements*. Rapp. tech. ISO 22301 :2019. ISO, 2019.

[120] National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. Rapp. tech. Special Publication 800-53 Revision 5. NIST, 2020.

Annexe D

La spirale progressive et intégrative

D.1 Introduction : pourquoi une spirale ?

La spirale progressive et intégrative de résilience numérique organise votre parcours de renforcement de la résilience numérique selon une logique d'amélioration continue. Chaque tour effectué vous élève à un niveau supérieur de maturité, de connaissance et de compétences, sans interruption ni rupture.

Cette méthodologie s'ancre dans les travaux de Peter Senge sur l'organisation apprenant [63]. Senge démontre que les organisations qui réussissent dans la durée construisent des capacités d'apprentissage collectif continu. La spirale incarne cette dynamique : chaque tour devient une opportunité d'apprentissage organisationnel qui enrichit les tours précédents et suivants. Vous ne répétez pas les mêmes actions, vous les réalisez à un niveau de compréhension et de maîtrise supérieur.

D.2 Anatomie de la spirale

Fig. D.2.1 : La spirale de résilience du numérique

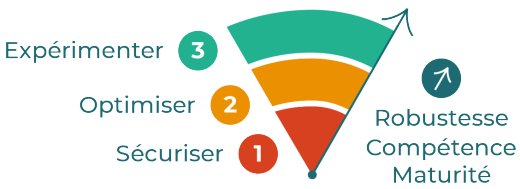


Fig. D.2.2 : La progressivité

La spirale intègre une triple progressivité qui structure votre montée en maturité à trois niveaux complémentaires.

Entre les tours de la spirale, vous montez en maturité organisationnelle : vous passez de concepts proches de vos habitudes à des concepts plus radicaux. Cette progression permet d'aborder en douceur des transformations de plus en plus ambitieuses.

Dans chaque tour, sont explorées trois facettes complémentaires de la zone de criticité concernée. Ces trois

facettes garantissent une vision complète des vulnérabilités et des solutions applicables. Elles sont parallèles et se renforcent mutuellement sans créer de dépendance séquentielle. Les facettes ne sont pas exhaustives et sont données à titre d'illustration. Elles peuvent être différentes, plus ou moins nombreuses, selon votre contexte opérationnel.

Pour chaque facette, une progression pédagogique se structure en six étapes standardisées. Cette structure s'inspire du cycle expérientiel de Kolb (1984)[64] qui établit que l'apprentissage se construit par itérations successives à travers quatre phases : expérience concrète, observation réflexive, conceptualisation abstraite et expérimentation active. Elle intègre également la taxonomie de Bloom (1956)[65] qui démontre que l'apprentissage cognitif progresse du simple au complexe à travers six niveaux : connaissance, compréhension, application, analyse, synthèse et évaluation.

Cette méthodologie spiralée permet de construire progressivement votre résilience numérique en partant de vos acquis, en accroissant votre maturité à chaque tour, et en consolidant vos apprentissages par un dernier tour qui enrichit l'ensemble de votre démarche.

La structure de chaque facette

Chaque facette suit une progression pédagogique identique en six étapes qui guide de l'expérience concrète à l'action opérationnelle.

Exercice de pensée (Kolb : expérience concrète / Bloom : application) — Vous imaginez une interruption des systèmes numériques critiques. Cet exercice vous place en situation réelle et active votre compréhension intuitive des vulnérabilités. Vous ne théorisez pas, vous vivez mentalement la crise.

Mécanisme de fragilisation (Kolb : observation réflexive / Bloom : compréhension) — Vous analysez les mécanismes profonds qui expliquent pourquoi votre système est fragile. Vous passez de l'intuition (« je sens que c'est fragile ») à la compréhension (« je comprends pourquoi c'est fragile »). Cette étape mobilise des concepts académiques et des modèles théoriques.

Scénario d'application (Kolb : conceptualisation abstraite / Bloom : analyse) — Vous étudiez un incident réel qui illustre le mécanisme identifié. CrowdStrike, Spruce Pine, inondations de datacenters : ces cas concrets vous permettent de voir comment le mécanisme se manifeste dans le monde réel et quelles ont été les conséquences. Vous pouvez imaginer comment ce type de scénario vous affecterait, afin de compléter l'exercice de pensée.

Inspiration (Bloom : synthèse) — Vous découvrez des exemples historiques ou contemporains d'organisations qui ont réussi à construire leur résilience face à des défis similaires. Wellington, Oseja… : ces inspirations montrent que la résilience est possible et donnent des pistes concrètes, adaptées ou adaptables à votre contexte.

Solutions (Kolb : expérimentation active / Bloom : évaluation) — Vous construisez des propres solutions selon votre contexte. Vous appliquez les premières métriques pour évaluer votre résilience, votre autonomie, vous mettez en place des redondances, vous testez vos capacités de bascule. Cette étape transforme la compréhension en action.

Bénéfices — Vous identifiez les gains concrets apportés par cette facette : capacités nouvelles, vulnérabilités réduites, confiance renforcée. Cette étape ancre votre apprentissage et prépare la suite du parcours.

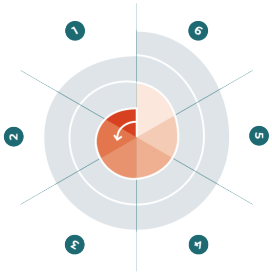
Cette structure standardisée crée des repères constants qui facilitent votre progression. Vous savez toujours où vous êtes dans le parcours et ce qui vous attend à l'étape suivante.

D.3 Parcourir la spirale

La matrice de criticité active la spirale

La matrice de criticité, présentée précédemment, active la spirale en structurant votre parcours d'apprentissage selon une logique de priorité et de progressivité.

Tour 1 : parcours de renforcement de la zone rouge



La zone rouge regroupe les processus métier les plus critiques, ceux dont la défaillance menacerait aussitôt votre pérennité. C'est là que tout commence.

Vous allez doucement sur ces processus critiques : des renforcements ciblés et maîtrisés pour sécuriser le cœur de métier sans perturber les opérations, tout en commençant à découvrir les impacts du numérique, les vulnérabilités qui l'affectent…

Le Tour 1 reste dans un territoire familier. Les concepts mobilisés sont proches de vos habitudes managériales et opérationnelles actuelles. Les solutions proposées relèvent de la sécurisation et de la consolidation de l'existant.

Vous n'abandonnez rien, vous ajoutez des couches de protection ou renforcez la capacité et les compétences humaines, là où c'est réellement nécessaire.

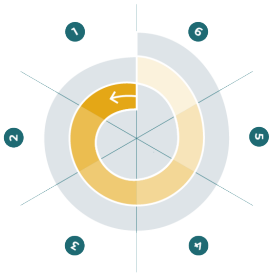
Cette approche prudente permet de construire votre confiance méthodologique sur des bases solides avant d'aborder des concepts plus novateurs.

Les objectifs du Tour 1 :

- Identifier les processus critiques et cartographier leurs dépendances numériques.
- Renforcer la complémentarité entre l'humain et le numérique.
- Construire des redondances robustes et adaptées sur votre cœur de métier.
- Tester les capacités de maintien en mode dégradé.
- Acquérir une méthodologie d'analyse des vulnérabilités applicable à tous les systèmes.

Ces objectifs constituent la base solide sur laquelle vous construirez les tours suivants. Votre zone rouge sera significativement plus résiliente, et vous aurez acquis la confiance requise pour aborder des transformations plus ambitieuses.

Tour 2 : parcours d'optimisation de la zone orange



La zone orange concerne les processus importants, mais non vitaux. Vous pouvez commencer à sortir de votre zone de confort : ayant acquis de la maturité au Tour 1, vous explorez des solutions plus ambitieuses, interrogez l'utilité réelle de certains outils, envisagez des alternatives low-tech, découvrez les blocages qui compliquent les évolutions, testez les pannes comme opportunité de progresser. C'est l'invitation à optimiser, simplifier, explorer des approches nouvelles, peu intrusives, sans mettre en péril votre activité.

Le Tour 2 est le parcours complet d'optimisation des processus importants. Fort de la maturité acquise au Tour 1, vous explorez trois nouvelles facettes de la résilience numérique, cette fois sur des processus dont la défaillance du numérique serait perturbante, mais non vitale. Cette zone offre un peu plus de liberté pour expérimenter des approches nouvelles.

Il vous emmène ainsi dans un territoire moins familier. Vous interrogez des hypothèses que vous teniez pour acquises. Les concepts mobilisés s'éloignent en partie de vos habitudes et remettent en question certains choix technologiques. Les solutions proposées au Tour 2 relèvent de l'hybridation maîtrisée : conserver le numérique pour l'efficacité, mais construire des alternatives simples pour la résilience.

Ce tour marque un premier tournant dans votre démarche. Vous passez de « Comment mieux protéger mes systèmes ? » à « Ai-je vraiment besoin de ces systèmes sous cette forme ? ». C'est l'amorce de l'apprentissage en double boucle théorisé par Argyris et Schön (1978)[66] : vous ne vous contentez plus de corriger l'action (simple boucle), vous interrogez les hypothèses elles-mêmes (double boucle).

Les objectifs du Tour 2 :

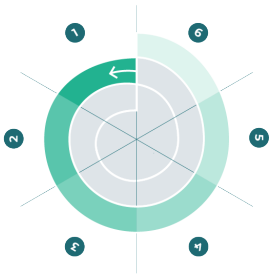
- Simplifier les architectures numériques en éliminant les complexités inutiles.
- Construire des alternatives low-tech viables pour les processus importants.
- Développer une capacité d'évaluation critique de l'utilité réelle des outils.
- Maîtriser l'hybridation entre solutions sophistiquées et solutions simples.
- Réduire votre surface d'attaque et vos coûts de maintenance.

Ces objectifs vous permettront non seulement d'optimiser la zone orange, mais également, plus tard, de revisiter la zone rouge avec un regard neuf. Les principes d'utilité et de low-tech, expérimentés sur la zone orange, puis la zone verte, donneront des idées pour simplifier les systèmes critiques.

Tour 3 : parcours d'expérimentation de la zone verte

La zone verte rassemble les processus les moins critiques, ceux dont l'arrêt du numérique n'aurait qu'un impact limité. C'est là que vous expérimentez des démarches novatrices.

Le Tour 3 est le parcours complet d'expérimentation sur les processus les moins critiques. Cette zone devient votre laboratoire d'innovation en résilience : vous pouvez y tester des approches radicales sans risquer la pérennité de votre organisation.



Il conduit vers des territoires que peu d'organisations explorent. Les concepts mobilisés sont radicaux car ils remettent en question l'impératif technologique lui-même. Vous ne cherchez plus à sécuriser, optimiser ou à hybrider, vous interrogez la pertinence même de certains choix numériques.

Ce principe s'inspire de l'ataraxie numérique théorisée par Stéphane Crozat[67] : la paix de l'esprit passe parfois par moins de technologie, pas plus. Les solutions proposées au Tour 3 relèvent de la sobriété numérique délibérée.

Ce tour exige la maturité la plus élevée. Il demande un leadership fort capable d'expliquer pourquoi « faire moins » peut être « faire mieux ». C'est aussi le tour le plus libérateur : en renonçant au superflu, vous libérez des ressources pour renforcer l'essentiel.

Les objectifs du Tour 3 :

- Maîtriser le renoncement stratégique et de savoir identifier ce qui est superflu.
- Libérer des ressources (budget, compétences, attention) en éliminant des systèmes non essentiels.
- Réduire considérablement votre surface d'attaque et vos vulnérabilités.
- Construire une culture de sobriété numérique qui valorise la simplicité.
- Disposer d'un laboratoire d'expérimentation pour tester de nouvelles approches radicales.

À l'issue du Tour 3, vous avez acquis la maturité maximale en matière de résilience numérique. Les bénéfices du Tour 3 sont les plus transformateurs car ils changent votre rapport même à la technologie.

Le Tour 4 : intégrer et approfondir

La progression précédente a permis de parcourir tous les processus identifiés, respecte en même temps l'urgence opérationnelle (sécuriser d'abord le critique) et la logique d'apprentissage (commencer par le concret avant d'aborder le radical).

Elle a fait grandir votre organisation en maturité, compétences, capacités et permis, sans risque non maîtrisé, de réduire la criticité du numérique pour votre métier.

Toutefois, cette démarche progressive s'est faite sans intégrer les acquis d'un tour dans le ou les tours précédents afin de prendre le temps de monter en maturité et en compétences.

Il est temps maintenant de mettre à profit tous ces acquis avec le Tour 4.

Les acquis du Tour 3 enrichissent les Tours 2 et 1

La spirale ne s'arrête donc pas au Tour 3. Ce dernier tour, où vous revisitez les trois zones, est aussi important que le mouvement d'ascension. Les apprentissages sont consolidés en appliquant aux situations des tours inférieurs les principes découverts aux tours supérieurs.

Du Tour 3 vers le Tour 2 : le principe de renoncement, expérimenté sur vos processus de confort (zone verte), éclaire d'un jour nouveau votre réflexion sur l'utilité (Tour 2). Si vous avez réussi à renoncer à certains outils dans la zone verte sans impact négatif, vous appliquez la même logique à certains éléments de la zone orange. La question du renoncement devient une option stratégique et légitime au Tour 2.

De même, les solutions low-tech expérimentées au Tour 3 inspirent des simplifications dans la zone orange. Vous découvrez qu'une technologie plus simple n'est pas nécessairement moins performante, elle est surtout plus robuste et plus maîtrisable. Cette découverte nourrit votre réflexion sur l'hybridation : doubler un système complexe par une solution simple et non un autre système complexe.

Du Tour 3 vers le Tour 1 : le principe de renoncement interroge même vos processus critiques. Non pas pour renoncer au numérique sur le cœur de métier, mais pour identifier les couches de complexité superflues qui fragilisent les systèmes critiques. Votre ERP a-t-il vraiment besoin de toutes ses fonctionnalités ? Votre infrastructure critique ne pourrait-elle pas être simplifiée dans ses fonctionnalités et non dans sa redondance, sans perte de performance ?

La sobriété numérique, expérimentée au Tour 3, devient un principe de conception à intégrer pour vos systèmes critiques.

Les acquis du Tour 2 enrichissent le Tour 1

Du Tour 2 vers le Tour 1 : les principes d'utilité et de low-tech, explorés dans la zone orange, transforment votre approche de la sur-redondance dans la zone rouge. Vous ne vous contentez plus de doubler les systèmes critiques à l'identique, vous les doublez par des alternatives de nature différente.

Cette approche hybride de la redondance est plus robuste que la simple duplication. Elle protège non seulement contre les pannes techniques, mais encore contre les défaillances systémiques qui affectent simultanément tous les systèmes de même nature (comme l'incident CrowdStrike qui a paralysé des millions de machines Windows en même temps).

Après le Tour 4 : une vision transformée

Après avoir parcouru les quatre tours, vous revenez au point de départ avec une vision profondément transformée. Vous aviez commencé par identifier les vulnérabilités numériques en vous appuyant sur votre expertise en résilience métier. Vous terminez avec une compréhension systémique de la fragilité et de la robustesse qui dépasse largement le seul domaine numérique.

Les principes que vous avez appliqués au numérique (non-régression capacitaire, résilience organisée, hybridation, sobriété, renoncement) sont universels. Ils peuvent ainsi s'appliquer à vos chaînes d'approvisionnement, à vos processus de décision, à votre organisation du travail, à votre stratégie énergétique. La matrice de criticité que vous avez utilisée pour évaluer les dépendances numériques peut évaluer n'importe quelle dépendance.

Pourquoi s'arrêter au numérique ?

Cette question marque la véritable transformation opérée par la spirale. Vous n'avez pas simplement renforcé votre résilience numérique, vous avez construit une capacité d'adaptabilité qui transcende le domaine technologique. Vous êtes passé de l'adaptation (réagir à des événements prévisibles) à l'adaptabilité (anticiper l'imprévisible avec une structure agile capable de se modifier rapidement).

D.4 Conclusion : de l'adaptation à l'adaptabilité

La spirale de résilience numérique transforme votre organisation en un système adaptatif capable de prospérer dans l'incertitude.

L'adaptation est une spécialisation. Vous identifiez des risques spécifiques (cyberattaque, panne cloud, rupture d'approvisionnement) et vous construisez des protections spécifiques. Dans un monde en polycrise, où les chocs sont imprévisibles et se combinent de manière non-linéaire, l'adaptation spécialisée devient une source de fragilité. Vous êtes préparé aux risques que vous avez anticipés, mais vulnérable à tous les autres.

L'adaptabilité est une capacité générique. Vous construisez une structure organisationnelle et technique capable de se reconfigurer rapidement face à l'imprévu. Cette approche s'inspire de l'ingénierie de la résilience (Hollnagel, Woods, Dekker)[68] qui distingue Safety-I (empêcher que les choses aillent mal) de Safety-II (s'assurer que les choses continuent d'aller bien malgré les perturbations). La spirale relève de Safety-II : elle construit une capacité à fonctionner même quand certains éléments tombent.

Cette capacité d'adaptabilité repose sur quatre piliers que la spirale a progressivement construits :

La modularité : vos systèmes critiques sont des ensembles de modules faiblement couplés. Si un module tombe, les autres continuent de fonctionner. Cette architecture modulaire permet de reconfigurer sans tarder vos systèmes en fonction des défaillances rencontrées.

La redondance diversifiée : vous doublez vos systèmes par des alternatives de nature différente, des fournisseurs sans dépendances géopolitiques ou techniques communes. Cette redondance hétérogène protège contre les défaillances systémiques qui affectent simultanément tous les systèmes de même type.

La capacité de renoncement : vous savez identifier et éliminer le superflu. Dans une crise, cette capacité permet de concentrer vos ressources limitées sur l'essentiel, au-delà des gains déjà réalisés lors du parcours de la spirale.

L'apprentissage continu : la spirale est un processus permanent. Chaque incident, chaque test, chaque tour enrichit votre compréhension et améliore vos capacités. Vous devenez, au sens de Senge, une organisation apprenante.

La matrice évolue avec vous

À chaque tour de la spirale, votre matrice de criticité se transforme. Les processus renforcés deviennent moins dépendants du numérique ou plus résilients face à ses défaillances. Un processus initialement en zone rouge peut descendre en zone orange une fois construites des alternatives humaines robustes et des redondances diversifiées. Un processus orange peut glisser vers le vert une fois son architecture numérique simplifiée et réduite selon l'utilité réelle.

Cette évolution matérialise votre progression. La matrice n'est pas une photographie figée des vulnérabilités, c'est une représentation vivante qui reflète votre maturité croissante. Chaque tour réduit votre risque global, allège votre dépendance, renforce votre capacité à fonctionner malgré les perturbations.

Ce mouvement à travers les quatre tours de la spirale ne s'arrête jamais. C'est un processus d'amélioration continue qui transforme progressivement votre organisation en système adaptatif. Chaque cycle enrichit le précédent, chaque tour vous place à un niveau supérieur de maturité.

Cette dynamique permanente fait de la résilience, non pas un état à atteindre, mais une capacité à cultiver. Vous n'êtes jamais « à la fin », vous êtes toujours en progression. Nouveaux outils, nouvelles dépendances, nouveaux risques : chaque nouvel élément entre dans la spirale et bénéficie de votre maturité acquise. Vous savez tout de suite où le positionner dans la matrice, quels principes lui appliquer, comment l'intégrer dans votre architecture de résilience.

Cette démarche transforme la contrainte de la polycrise en opportunité stratégique. Dans un monde avec lequel vos concurrents subissent les pannes, être celui qui maintient le service devient un différenciateur puissant. Dans un monde avec lequel la complexité technologique croît exponentiellement, être celui qui maîtrise la sobriété devient un avantage compétitif. Dans un monde avec lequel l'imprévisible devient la norme, être celui qui sait toujours s'adapter devient la condition de survie.

C'est cette capacité, bien plus que n'importe quelle technologie, qui fera la différence dans le monde qui vient.

---

[63] Peter M. Senge. *The Fifth Discipline : The Art and Practice of the Learning Organization*. Doubleday, 1990.
[64] David A. Kolb. *Experiential Learning : Experience as the Source of Learning and Development*. Prentice Hall, 1984.
[65] Benjamin S. Bloom. *Taxonomy of Educational Objectives : The Classification of Educational Goals*. Longmans, Green, 1956.
[66] Chris Argyris et Donald A. Schön. *Organizational Learning : A Theory of Action Perspective*. Addison-Wesley, 1978.
[67] Stéphane Crozat. *Vers une ataraxie numérique : low-technicisation et convivialité*. 2021. URL : https://aswemay.fr/co/040011.html.
[68] Erik Hollnagel, David D. Woods et Nancy Leveson. *Resilience Engineering : Concepts and Precepts*. Ashgate Publishing, 2006.

Pour aller plus loin

[69] Sidney Dekker. *Drift into Failure : From Hunting Broken Components to Understanding Complex Systems*. Ashgate Publishing, 2011.
[70] Nassim Nicholas Taleb. *Antifragile : Things That Gain from Disorder*. Random House, 2012.
[71] Donella H. Meadows. *Thinking in Systems : A Primer*. Chelsea Green Publishing, 2008.

Annexe E

Mécanismes et scénarios détaillés

Pour illustrer concrètement nos propos, nous avons identifié les vulnérabilités et analysé des scénarios concrets.

Chaque scénario que nous proposons permet ainsi de se placer dans une situation critique, d'identifier les vulnérabilités potentielles et de fournir des exemples avec impacts chiffrés.

Afin de mieux les comprendre, ces scénarios sont positionnés par rapport à six mécanismes de fragilisation que notre monde 📖VUCA génère, montrant ainsi l'interdépendance entre les différentes crises et l'amplification qui en résulte.

E.1 Une approche fondée sur l'expertise mondiale

Toutes les informations de cette annexe sont fondées sur l'annexe Ressources majeures, sauf indication dans une bibliographie spécifique.

Les mécanismes de fragilisation et scénarios présentés dans ce document s'appuient sur une base empirique solide.

Ils reflètent les observations convergentes de plus de **27 000 experts mondiaux** consultés par les principales institutions d'analyse des risques.

Cette expertise révèle des tendances préoccupantes mais mesurées : **92 % des experts** observent une augmentation des crises interconnectées (AXA 2024 [39]), tandis que **87 %** estiment que notre environnement est devenu plus vulnérable. L'OCDE (2025) [45] confirme cette analyse en documentant des signes de fragilité systémique dans l'ensemble des **177 contextes** qu'elle a analysés.

De manière particulièrement significative, les trois leaders mondiaux de l'assurance et de la réassurance convergent vers un diagnostic similaire :

– **Swiss Re (2024) [49]** observe que « la résilience des chaînes d'approvisionnement mondiales face aux risques d'interruption d'activité s'affaiblit ».

– **Allianz (2025) [38]** confirme que l'interruption d'activité demeure dans le top 2 des risques depuis une décennie.

– **AXA (2024) [39]** place l'instabilité géopolitique, le changement climatique et la cybersécurité dans le trio de tête pour la troisième année consécutive Cette convergence s'inscrit dans ce que la communauté scientifique nomme désormais la **« polycrise »**, définie par Nature Communications (2025) [44] comme « l'enchevêtrement causal de crises dans de multiples systèmes globaux », où selon le World Economic Forum (2023), « l'impact global dépasse largement la somme de chaque partie ».

L'importance de cette convergence tient au fait que ces institutions portent financièrement les conséquences de ces risques, représentant plusieurs milliers de milliards d'euros d'exposition mondiale. Leur analyse n'est donc pas théorique, mais ancrée dans la réalité économique des risques contemporains.

Les six mécanismes de fragilisation qui suivent offrent ainsi un cadre structuré pour comprendre ces évolutions, tandis que les scénarios illustrent leurs manifestations concrètes.

E.2 Mécanismes de fragilisation

Fragilités géopolitiques

Pensez à votre chaîne d'approvisionnement numérique non plus comme une simple ligne logistique, mais comme une carte géopolitique remplie de points de tension. La fabrication des composants les plus critiques, comme les semi-conducteurs, est concentrée dans des zones de conflit potentiel comme Taïwan, tandis que les matières premières essentielles sont sous le contrôle quasi-exclusif de la Chine.

Dans un monde dans lequel les sanctions technologiques deviennent des armes courantes, chaque maillon de votre chaîne de valeur est une vulnérabilité potentielle. L'indépendance numérique n'est plus un slogan, mais une question de survie qui exige une diversification radicale pour ne pas voir votre activité paralysée par une décision politique prise à l'autre bout du monde.

Allianz (2025) [38] confirme que « l'impact des émeutes civiles est l'exposition que les entreprises craignent le plus, suivie par la guerre et les impacts sur les chaînes d'approvisionnement ». Cette fragilité géopolitique est identifiée comme top 3 des risques mondiaux par AXA (2024) [39] pour la troisième année consécutive.

Exemples :

- Taïwan : plus de 50 % de la production mondiale des semi-conducteurs dans un contexte de tensions croissantes.
- Terres rares : monopole chinois et vulnérabilité aux sanctions.
- Câbles sous-marins : points de rupture physiques ou géopolitiques.
- Sanctions technologiques comme armes dans un monde multipolaire.
- Indépendance numérique impossible sans diversification.

Fragilités physiques/climatiques face à l'incertitude environnementale

L'infrastructure numérique sur laquelle repose votre entreprise, a une empreinte physique bien réelle, et cette dernière est de plus en plus exposée aux aléas climatiques. Un datacenter sur cinq est déjà menacé par des risques comme les inondations ou les canicules, et la consommation massive d'eau et d'énergie du secteur rend vulnérables aux sécheresses et aux crises énergétiques. Ces fragilités ne sont plus des risques lointains, mais des menaces opérationnelles directes. Ignorer la dépendance de vos activités à la stabilité du climat et à l'abondance des ressources, c'est exposer votre entreprise à des ruptures brutales et imprévisibles.

Swiss Re (2024) [49] souligne les « cascading effects of natural catastrophes » (« effets en cascade des catastrophes naturelles ») sur les infrastructures numériques, tandis que Scheffran (2025) [48] identifie ces risques comme « evolving threats » (« menaces évolutives ») — des menaces en constante évolution qui dépassent nos capacités d'adaptation.

- 22 % des datacenters menacés climatiquement : sous-estimation des risques.
- Consommation d'eau et stress hydrique croissant : concurrence avec d'autres secteurs (agriculture par exemple) ou simplement avec les êtres vivants.
- Dépendance énergétique totale dans un contexte de transition.
- Vulnérabilité aux événements extrêmes imprévisibles.
- Chaînes logistiques longues et fragiles.

Fragilités techniques et complexité systémique

Les systèmes informatiques qui font tourner votre entreprise sont devenus si complexes que plus personne ne les maîtrise entièrement. Cette complexité exponentielle crée un nouveau type de risque : la panne systémique. Un simple bug dans un logiciel de sécurité, comme nous l'avons vu avec CrowdStrike, peut paralyser des milliers d'entreprises simultanément. Cette « dette technique » accumulée au fil des ans est une bombe à retardement.

Swiss Re (2024) [49] identifie explicitement « Big Tech — a dependency risk » (« Les géants de la tech — un risque de dépendance ») et met en garde contre les « unintended insurance impacts » (« impacts imprévus sur l'assurance ») de l'IA et les risques de « silent cyber ». Allianz (2025) [38] ajoute que « l'automation et la digitalisation ont significativement accéléré les processus, qui peuvent parfois submerger les individus en raison du rythme rapide et de la complexité ».

- Complexité exponentielle dépassant les capacités de maîtrise.
- Bugs systémiques (CrowdStrike) : quand la sécurité devient vulnérabilité.
- Dette technique accumulée et maintenance impossible.
- Incompatibilités croissantes et fragmentation.

Mécanismes de contagion et ambiguïté des interdépendances

Votre entreprise est connectée à un écosystème de partenaires, de fournisseurs et de services dont vous ne soupçonnez pas toutes les interdépendances. Une faille chez un fournisseur de rang 3 peut, par un effet domino, paralyser vos propres opérations. Ces « points de défaillance uniques » sont souvent masqués dans la complexité des réseaux modernes, rendant les cascades d'incidents complètement imprévisibles. Dans cet environnement, les protections traditionnelles ne suffisent plus ; le véritable enjeu est de cartographier ces dépendances invisibles pour anticiper et contenir la contagion avant qu'elle ne se généralise.

Liu & Renn (2025) [43] distinguent scientifiquement les « disruptions intra-systémiques qui se propagent via des chaînes causales contagieuses » des « disruptions inter-systémiques qui débordent vers d'autres systèmes ». Scheffran (2025) [48] avertit : « Quand le nombre d'événements interconnectés dépasse un seuil critique, la dynamique dévastatrice se propage d'elle-même comme une réaction en chaîne incontrôlée ».

- Chaque Point de défaillance unique (Single Point of Failure / SPOF) masqué
- Cascades d'incidents imprévisibles
- Interdépendances invisibles et effets domino
- Absence de « pare-feu » systémiques

Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)

Les choix technologiques que vous avez faits par le passé, souvent pour des raisons de coût ou de commodité, vous ont enfermés dans des écosystèmes dont il est aujourd'hui extrêmement coûteux, voire impossible, de sortir. Que ce soit la dépendance à un seul fournisseur de cloud, à un logiciel propriétaire ou à un standard de fait, ce « verrouillage » a éliminé les alternatives et atrophié nos compétences internes. Cette Dépendance au sentier (Path Dependency) nous rend non seulement vulnérables aux décisions de ces acteurs dominants, mais elle nous empêche également d'innover et de nous adapter, créant une rigidité stratégique majeure face à un monde qui exige de l'agilité.

Center for Creative Leadership (2025) [40] identifie ce phénomène parmi les 14 barrières systémiques au changement, soulignant la « surconfiance dans la technologie comme solution universelle » qui crée des dépendances irréversibles.

- Dépendance au sentier (Path Dependency) irréversible violant le principe de non-régression.
- Coûts de sortie prohibitifs et perte d'alternatives.
- Standards propriétaires dominants.
- Perte de compétences alternatives et savoir-faire.
- Accoutumance collective et résistance au changement.

Impacts sociétaux dans un contexte d'incertitude croissante

Le numérique n'est plus un simple outil, il façonne la société. Les conséquences de nos technologies — surcharge informationnelle, surveillance, dépendance aux algorithmes — créent un climat de méfiance et d'incertitude qui affecte directement votre entreprise. Cette érosion de la confiance se traduit par une pression réglementaire accrue, une difficulté à recruter des talents en quête de sens, et un risque de rejet de vos produits ou services s'ils sont perçus comme nuisibles. Ignorer ces impacts sociétaux, c'est se couper de la réalité de vos clients, de vos employés et des citoyens, et risquer de perdre votre Licence sociale d'opérer.

PolyCIVIS (2025) [47] documente « l'érosion de la confiance publique » amplifiée par la désinformation, tandis qu'AXA (2024) [39] révèle le paradoxe de la surconfiance : 80 % des experts pensent pouvoir détecter la désinformation, mais seulement 25 % croient que les autres en sont capables.

- Fracture numérique persistante et inégalités amplifiées.
- Aliénation cognitive et surcharge informationnelle.
- Surveillance généralisée et érosion des libertés.
- Perte d'autonomie décisionnelle et dépendance algorithmique.
- Érosion démocratique et concentration du pouvoir.

Le Monde [18] documente l'accélération brutale de cette transformation. PwC Royaume-Uni a réduit ses embauches de débutants de 13 % en un an, citant explicitement l'IA comme cause. Accenture, soupçonné de ne pas adopter l'IA assez rapidement, a vu son action chuter de 33 % et licencie désormais les consultants « dont la requalification ne constitue pas une solution viable ». Le message est clair : « point de salut sans l'IA », créant une pression existentielle sur les travailleurs.

- Fracture numérique persistante et inégalités amplifiées.
- Aliénation cognitive et surcharge informationnelle.
- Surveillance généralisée et érosion des libertés.
- Perte d'autonomie décisionnelle et dépendance algorithmique.
- Érosion démocratique et concentration du pouvoir.
- Obsolescence accélérée des compétences et darwinisme numérique.

E.3 De la théorie à la pratique : six scénarios d'illustration

Les mécanismes de fragilisation que nous venons de décrire ne restent pas abstraits. Ils se manifestent concrètement à travers des événements qui, bien que parfois improbables individuellement, deviennent inévitables collectivement dans un environnement de polycrise.

Les six scénarios qui suivent illustrent comment ces mécanismes peuvent se combiner et s'amplifier mutuellement. Chaque scénario est positionné par rapport aux mécanismes qu'il active principalement, tout en montrant les effets de cascade qui touchent l'ensemble du système. Ces scénarios ne sont pas des prédictions, mais des outils de réflexion pour identifier les vulnérabilités et préparer des réponses adaptées.

La mégapanne systémique par bug ou cyberattaque

Un bug dans une mise à jour critique ou une cyberattaque sophistiquée paralyse 40 % de l'infrastructure numérique mondiale.

Narratif

Imaginez un matin durant lequel, progressivement, les services numériques que nous tenons pour acquis cessent de fonctionner. Les terminaux de paiement dans les commerces affichent « erreur de connexion », les plateformes de travail collaboratif sont inaccessibles, les feux de circulation intelligents se désynchronisent et les chaînes de production automatisées s'arrêtent net.

La cause ? Une mise à jour, déployée automatiquement pendant la nuit sur un composant logiciel fondamental (comme un système d'exploitation ou un service cloud), contenait une erreur critique. Ou alors, un groupe de cybercriminels (étatique ou non) a réussi à infiltrer la chaîne de développement d'un fournisseur technologique majeur. Ils ont injecté un code malveillant (un 🕮 *Ransomware (Rançongiciel)*, un 🕮 *Wiper (Logiciel effaceur)* qui efface les données ou un simple agent de chaos) dans une mise à jour qui semblait être légitime.

Conséquences pour le numérique et les entreprises

Une telle panne aurait des conséquences immédiates et dévastatrices :

- Paralysie économique et extorsion : en plus de l'arrêt des activités, une cyberattaque à grande échelle pourrait inclure une demande de rançon colossale pour restaurer les systèmes, créant un dilemme mondial – payer et financer les attaquants, ou refuser et faire face à une reconstruction longue et coûteuse.

- Destruction ou vol de données : contrairement à un bug qui paralyse, une attaque peut viser à *détruire ou exfiltrer* des données sensibles. Les entreprises pourraient perdre des années de propriété intellectuelle, de données clients et de secrets commerciaux. La confiance des consommateurs serait anéantie.

- Guerre de l'information et chaos social : les attaquants pourraient manipuler les informations, couper les communications pour semer la panique ou cibler spécifiquement les médias et les services gouvernementaux pour déstabiliser des régions entières.

- Complexité de la remédiation : alors qu'un bug peut être corrigé par un patch, une cyberattaque nécessite une décontamination complète des systèmes. Il faut s'assurer qu'aucune « Backdoor (Porte dérobée) » n'a pas été laissée par les attaquants, ce qui rend la restauration beaucoup plus lente et incertaine.

- Crise géopolitique : si l'attaque est attribuée à un acteur étatique, elle pourrait être considérée comme un acte de guerre, déclenchant une escalade des tensions internationales et des représailles.

Exemples d'organisations déjà touchées et impacts réels

AXA (2024) [39] mentionne explicitement « la panne de CrowdStrike » comme événement majeur précédant leur enquête. Allianz (2025) [38] confirme que l'interruption d\'activité, conséquence typique de telles pannes, reste le risque #1 ou #2 depuis 10 ans, affectant 3 778 experts dans 106 pays.

Des attaques ont déjà illustré ce potentiel de paralysie ciblée :

- ***NotPetya (2017)*** : Souvent cité comme l'attaque la plus dévastatrice économiquement, NotPetya a commencé comme une attaque ciblée sur l'Ukraine via un logiciel de comptabilité compromis. Cependant, le ver s'est propagé de manière incontrôlable à l'échelle mondiale.

  - Impacts réels :

    - *Maersk* : le géant du transport maritime a perdu le contrôle de 76 ports et de 800 navires. L'entreprise a dû réinstaller 4 000 serveurs et 45 000 PC. Le coût total a été estimé à plus de 300 millions de dollars.

    - *FedEx (via sa filiale TNT Express)* : l'attaque a paralysé les opérations de TNT, entraînant des pertes estimées à 400 millions de dollars

    - *Merck* : le groupe pharmaceutique a vu sa production mondiale interrompue, avec des pertes évaluées à plus de 800 millions de dollars.

  - NotPetya n'était pas un Ransomware (Rançongiciel) classique (il rendait les données irrécupérables, même avec une clé), mais un *Wiper (Logiciel effaceur)* déguisé. Son impact total a dépassé les *10 milliards de dollars*, démontrant comment une attaque initialement localisée peut causer un chaos économique mondial.

- ***L'attaque de la chaîne d'approvisionnement SolarWinds (2020)*** : des espions russes présumés ont compromis le logiciel de gestion informatique Orion de SolarWinds. Ils ont inséré une porte dérobée dans les mises à jour logicielles, qui ont ensuite été installées par plus de 18 000 clients, y compris de nombreuses agences gouvernementales américaines (Département du Trésor, de la Sécurité Intérieure) et des entreprises du Fortune 500.

  - Impacts réels : l'objectif n'était pas la paralysie, mais l'espionnage. Les attaquants ont eu un accès discret et prolongé aux réseaux de milliers d'organisations parmi les plus sécurisées au monde. Le coût de l'audit, du nettoyage et de la sécurisation des réseaux affectés s'est chiffré en milliards, sans parler de la perte incalculable de secrets stratégiques.

Positionnement dans les six mécanismes de fragilisation

- Mécanisme principal : Mécanismes de contagion et ambiguïté des interdépendances
  - Justification : le cœur du scénario est la propagation ultra-rapide d'une faille (bug ou code malveillant) à travers un écosystème hyper-connecté. L'interdépendance des systèmes (une seule mise à jour affecte des millions d'appareils) est le moteur de la crise. L'exemple de NotPetya, qui s'est propagé de manière incontrôlable bien au-delà de sa cible initiale, est l'archétype de ce mécanisme.
- Mécanisme secondaire : Fragilités techniques et complexité systémique
  - Justification : la crise naît d'une vulnérabilité technique intrinsèque : soit une erreur humaine dans le code (dette technique), soit une faille dans la sécurité de la chaîne d'approvisionnement logicielle (comme pour SolarWinds).
- Mécanisme tertiaire : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)
  - Justification : la panne a un impact aussi massif parce que nous dépendons d'un faible nombre de fournisseurs pour les systèmes d'exploitation, les services cloud ou les logiciels de sécurité (ex : Microsoft, AWS, CrowdStrike). Ce verrouillage crée un point de défaillance unique (*single point of failure*) à l'échelle mondiale.

Opportunités dans la crise

Une telle crise, bien que dévastatrice, agirait comme un électrochoc mondial. Elle créerait une opportunité unique de promouvoir des architectures numériques plus résilientes et décentralisées. Pour une entreprise, survivre à une telle panne grâce à des systèmes résilients et des sauvegardes déconnectées deviendrait un avantage concurrentiel majeur, un véritable argument de confiance et de fiabilité pour ses clients. Cela pourrait également accélérer l'adoption de standards de sécurité plus élevés et d'une culture de la « résilience par conception » (resilience by design).

La rupture géopolitique

Découplage technologique fort, voire total, USA/Europe/Chine : embargo sur les composants, les minerais, les technologies, les services.

Narratif

Les tensions commerciales, qui couvaient depuis des années, atteignent un point de rupture. En réponse à des différends sur la propriété intellectuelle, la sécurité nationale et la domination technologique, les grands blocs mondiaux (USA/Europe d'un côté, Chine de l'autre) formalisent leur séparation. Des « rideaux de fer numériques » s'abattent. Les exportations de semi-conducteurs avancés, de logiciels spécialisés et même de matières premières critiques comme les terres rares sont soumises à des embargos stricts. Une entreprise européenne qui fabrique des objets connectés voit sa production s'arrêter net : ses microprocesseurs, conçus aux États-Unis, sont fabriqués à Taïwan avec des équipements néerlandais, mais assemblés en Chine avec des composants locaux. Du jour au lendemain, sa chaîne d'approvisionnement n'est plus seulement complexe, elle est devenue illégale.

Conséquences pour le numérique et les entreprises

Confirmé par les données terrain : risque dans le top 3 mondial (AXA, 2024)[39], avec une montée particulière en France et UK où il entre dans le top 5 (Allianz, 2025)[38].

Ce découplage forcerait une réorganisation brutale de l'économie numérique mondiale :

- Fragmentation d'Internet : l'Internet unique et mondial pourrait se scinder en plusieurs « Internets » régionaux (un occidental, un chinois, etc.), avec des normes, des protocoles et des services incompatibles. La collaboration internationale en ligne deviendrait un casse-tête.

- Pénuries et inflation technologique : l'arrêt des importations de composants clés (puces, batteries, écrans) créerait des pénuries massives et ferait flamber les prix des appareils électroniques. L'innovation ralentirait, faute d'accès aux meilleurs composants mondiaux.

- Relocalisation forcée et coûteuse : les entreprises seraient contraintes de relocaliser leurs usines et de reconstruire des chaînes d'approvisionnement entièrement nouvelles à l'intérieur de leur bloc géopolitique. Ce processus serait extrêmement long, coûteux et entraînerait une perte de compétitivité.

- Guerre des talents et des normes : les talents de l'ingénierie et de la recherche devraient « choisir un camp ». Les standards technologiques (comme la 5G, le Wi-Fi ou les formats de données) divergeraient, rendant les produits d'un bloc inutilisables dans un autre.

- Obsolescence forcée : les équipements existants qui dépendent de mises à jour logicielles ou de maintenance provenant d'un bloc rival pourraient progressivement devenir obsolètes ou non sécurisés.

Exemple de réglementation : Guaranteeing Access and Innovation for National Artificial Intelligence Act of 2025

La loi de 2025 sur la garantie de l'accès et de l'innovation pour l'intelligence artificielle nationale (GAIN AI Act), introduite dans le cadre de la loi sur l'autorisation de la défense nationale, exigera des développeurs américains de processeurs d'IA qu'ils accordent la priorité aux commandes nationales de processeurs à haute performance avant de les fournir aux acheteurs étrangers.

Objectifs de la loi GAIN AI :

- Les fabricants américains de puces doivent donner la priorité aux acheteurs américains avant d'exporter ;
- les puces avancées au-dessus des seuils de puissance doivent être autorisées à exporter ;
- maintenir le matériel d'IA à la disposition des organisations américaines ;
- viser à renforcer la sécurité nationale et le leadership de l'IA aux États-Unis.

Nvidia précise que c'est déjà le cas dans les faits, mais c'est sans compter l'explosion de la demande et la combinaison avec des impacts d'événements extrêmes sur la chaîne de fabrication ou tout autre aléa qui limiterait la capacité de production. Dans ce cas-là, les projets hors territoire américain pourrait être retardés de plusieurs mois, voire années.

Exemples d'organisations déjà touchées et impacts réels

Nous assistons déjà aux prémices de ce scénario :

- Huawei (depuis 2019) : l'entreprise chinoise est l'exemple le plus emblématique de ce découplage. À la suite d'un décret du gouvernement américain, Huawei a été placé sur une « liste d'entités », lui coupant l'accès à des technologies américaines cruciales.
    - Impacts réels :
        - Perte de l'écosystème Google : les nouveaux smartphones de Huawei ne peuvent plus intégrer les services Google (Play Store, Gmail, Google Maps), ce qui a fait chuter ses ventes de smartphones de manière spectaculaire en dehors de la Chine.
        - Accès aux puces : Huawei a perdu l'accès aux puces les plus avancées conçues avec des logiciels américains et fabriquées par des fondeurs comme TSMC. Son activité de semi-conducteurs (HiSilicon) a été gravement handicapée.
        - Impact financier : en 2021, Huawei a annoncé sa plus forte baisse de revenus annuelle de l'histoire, près de 29%, en grande partie à cause des sanctions. L'entreprise a dû se réorienter massivement vers le marché chinois et de développer son propre système d'exploitation (HarmonyOS) et ses propres services pour survivre.

- ASML et l'industrie des semi-conducteurs (depuis 2022) : l'entreprise néerlandaise ASML détient un monopole mondial sur les machines de lithographie EUV (Extreme Ultraviolet), indispensables pour fabriquer les puces les plus modernes. Sous la pression des États-Unis, le gouvernement néerlandais a restreint les exportations de ces technologies vers la Chine.

    - Impacts réels :

        - Frein à l'ambition chinoise : cette restriction empêche la Chine de développer sa propre industrie de semi-conducteurs de pointe, la maintenant dépendante de technologies étrangères ou la forçant à investir des milliards dans des alternatives moins performantes.

        - Incertitude pour ASML : bien que son carnet de commandes soit plein, ASML perd l'accès à un marché potentiellement énorme et fait face à une pression géopolitique constante qui pèse sur sa stratégie à long terme.

Positionnement dans les six mécanismes de fragilisation

- Mécanisme principal : Fragilités géopolitiques

    - Justification : le scénario est entièrement défini par des décisions politiques (embargos, sanctions) qui fracturent les chaînes d'approvisionnement mondialisées. La dépendance de l'Occident pour la fabrication asiatique (Taïwan pour les puces, Chine pour l'assemblage) et la dépendance de la Chine pour les technologies de conception occidentales (logiciels, machines ASML) sont les points de pression exploités.

- Mécanisme secondaire : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)

    - Justification : la crise est si grave parce que des monopoles ou des oligopoles de fait se sont créés. ASML pour la lithographie EUV, TSMC pour la fonderie de puces avancées. Il n'existe pas d'alternative à court terme, ce qui donne un pouvoir immense aux États qui contrôlent ces « nœuds » de la chaîne de valeur.

Opportunités dans la crise

Ce découplage forcé, bien que coûteux, peut devenir une opportunité stratégique. Il peut justifier et accélérer la relocalisation de savoir-faire critiques, le développement de filières locales ou régionales plus résilientes, et stimuler l'innovation pour créer des produits moins dépendants de chaînes d'approvisionnement complexes. Pour une entreprise, maîtriser une chaîne de valeur plus courte et plus locale peut devenir un puissant argument d'indépendance, de traçabilité et de fiabilité, très valorisé par les clients et les investisseurs.

L'effondrement climatique en cascade

Canicule extrême de plusieurs semaines paralysant les infrastructures numériques européennes.

Narratif

L'été 2027 restera dans les mémoires comme celui qui a brisé tous les records. Une masse d'air surchauffé, bloquée par un anticyclone persistant, maintient l'Europe sous un dôme de chaleur pendant six semaines consécutives. Les températures dépassent 50°C dans le sud de la France, 45°C à Paris, et même Londres suffoque sous 42°C. Ce n'est plus une canicule, c'est un nouveau régime climatique temporaire qui met à nu la fragilité de nos infrastructures numériques, conçues pour un monde plus tempéré.

Conséquences pour le numérique et les entreprises

Swiss Re (2024) documente les « effets en cascade » des catastrophes naturelles sur les infrastructures numériques, avec 22 % des datacenters déjà menacés climatiquement.

- Surchauffe généralisée des datacenters : les systèmes de refroidissement, dimensionnés pour des températures « normales », ne parviennent plus à maintenir les serveurs dans leurs plages de fonctionnement. Les datacenters commencent à s'arrêter automatiquement pour éviter la destruction du matériel.

- Pénurie d'eau et conflits d'usage : les datacenters consomment des quantités massives d'eau pour leur refroidissement. Avec les restrictions d'eau imposées aux particuliers et à l'agriculture, l'opinion publique se retourne contre ces « gaspilleurs numériques ».

- Surcharge et effondrement du réseau électrique : la demande de climatisation explose, créant des pics de consommation que le réseau électrique ne peut absorber. Les coupures en cascade privent les infrastructures numériques de leur alimentation.

Exemples d'organisations déjà touchées et impacts réels

- Inondations en Thaïlande (2011) : ces inondations massives ont submergé de nombreux parcs industriels. La Thaïlande était à l'époque le second plus grand producteur mondial de disques durs (HDD).

    - Impacts réels :

        - Western Digital & Seagate : les usines de ces deux géants ont été gravement touchées, voire complètement arrêtées. La production mondiale de disques durs a chuté de près de 30% au trimestre suivant.

        - Pénurie mondiale et hausse des prix : une pénurie mondiale de disques durs s'en est ensuivi, provoquant une augmentation des prix de plus de 100% en quelques semaines. Des entreprises comme Apple et Dell ont été directement affectées, subissant des contretemps de production pour leurs ordinateurs. L'impact s'est fait sentir pendant plus d'un an.

- Vague de chaleur au Royaume-Uni (2022) : en juillet 2022, une vague de chaleur record a frappé le Royaume-Uni, avec des températures dépassant les 40°C.
    - Impacts réels :
        - Google Cloud et Oracle : plusieurs de leurs data centers basés à Londres ont subi des pannes. Les systèmes de refroidissement n'ont pas réussi à compenser la chaleur extrême, forçant les entreprises à mettre hors service une partie de leurs serveurs pour éviter des dommages permanents.
        - Pannes de services : des clients de ces services cloud, comme WordPress et des plateformes d'e-commerce, ont connu des interruptions de service et des ralentissements, démontrant que même les géants de la tech ne sont pas à l'abri des extrêmes climatiques.
- Sécheresse à Taïwan (2021) : Taïwan a connu en 2021, sa pire sécheresse en plus d'un demi-siècle. Or, l'île abrite TSMC (Taïwan Semiconductor Manufacturing Company), qui produit plus de 50 % des semi-conducteurs mondiaux et plus de 90 % des puces les plus avancées.
    - Le problème : la fabrication de semi-conducteurs est un processus extrêmement consommateur en eau ultra-pure, nécessaire pour nettoyer les « wafers » de silicium entre les centaines d'étapes de gravure. Une seule usine de TSMC peut consommer des dizaines de milliers de tonnes d'eau par jour.
    - Impacts réels :
        - Rationnement et pression sur la production : le gouvernement taïwanais a dû imposer un rationnement d'eau drastique, affectant l'agriculture et la population. Pour préserver son industrie stratégique, il a maintenu l'approvisionnement des usines de puces, mais la menace d'un arrêt planait.
        - Coûts supplémentaires massifs : pour sécuriser leur production, TSMC et d'autres fabricants ont dû faire venir des dizaines de camions-citernes d'eau chaque jour, une solution logistique coûteuse et non durable.
        - Aggravation de la pénurie mondiale : cette sécheresse est survenue en pleine pénurie mondiale de puces post-COVID. Elle a ajouté une pression immense sur une chaîne d'approvisionnement déjà à genoux, contribuant aux retards de production dans l'automobile, l'électronique grand public et l'informatique. Cet événement a démontré que la production des composants les plus sophistiqués au monde pouvait être menacée par un manque de la ressource la plus élémentaire : l'eau.

Positionnement dans les six mécanismes de fragilisation

- Mécanisme principal : Fragilités physiques/climatiques face à l'incertitude environnementale
  - Justification : la cause première de la crise est l'impact direct d'événements climatiques (canicules, inondations, sécheresses) sur les infrastructures physiques du numérique. Les exemples des centres de données de Google en surchauffe, des usines de disques durs inondées en Thaïlande, ou de la production de puces à Taïwan menacée par le manque d'eau sont des illustrations parfaites.
- Mécanisme secondaire : Fragilités géopolitiques
  - Justification : la vulnérabilité est exacerbée par la concentration géographique de la production. Le fait que plus de 90 % des puces les plus avancées soient fabriquées à Taïwan, une île exposée à des risques climatiques et géopolitiques, est une fragilité en soi.

Opportunités dans la crise

La prise de conscience brutale de la vulnérabilité physique du numérique obligerait le secteur à une innovation radicale. Ce serait une opportunité de développer et de promouvoir des technologies de « low-tech » et d'« informatique frugale » (des services moins énergivores et moins voraces en ressources).

Les entreprises qui investiraient dans des infrastructures durables (centres de données éco-conçus, circuits d'approvisionnement en eau recyclée) pourraient à la fois réduire leurs risques opérationnels, et transformer cette résilience en un avantage de marque et un argument commercial puissant.

La régulation drastique

Adoption d'une réglementation européenne drastique sur l'empreinte carbone du numérique.

Narratif

Face à l'urgence climatique et à la pression citoyenne, l'Union européenne adopte le « Digital Carbon Act » en 2026. Cette loi révolutionnaire impose des quotas carbone stricts à toutes les entreprises numériques et instaure une « taxe carbone numérique » proportionnelle à l'empreinte énergétique des services. Du jour au lendemain, chaque email, chaque requête de recherche, chaque heure de streaming a un coût carbone calculé et facturé.

Les entreprises doivent choisir : réduire drastiquement leurs services numériques ou payer des taxes qui peuvent représenter un pourcentage important de leur chiffre d'affaires.

Conséquences pour le numérique et les entreprises

- Bouleversement des modèles économiques : les plateformes gratuites financées par la publicité deviennent insoutenables. Les géants du numérique sont contraints de facturer leurs services ou de les rationner drastiquement.

- Fracture numérique européenne : les entreprises et citoyens européens se retrouvent désavantagés face à leurs concurrents américains et chinois, non soumis aux mêmes contraintes. Un exode numérique vers des juridictions plus permissives commence.

- Innovation bridée : les startups européennes, incapables de supporter les coûts de conformité, voient leurs projets d'IA et de cloud computing devenir économiquement impossibles.

Nuance du « Regulatory Wild West » – Allianz (2025) identifie aussi le risque inverse : un « Far West réglementaire » notamment sur crypto et IA, où l'absence de régulation claire crée autant de chaos qu'une sur-régulation.

Exemples d'organisations déjà touchées et impacts réels

Ce scénario est encore prospectif, mais des réglementations existantes en sont les prémices :

- L'impact du RGPD (depuis 2018) : le Règlement Général sur la Protection des Données en Europe est la première étape de ce scénario.

    - Impacts réels :

        - Meta (Facebook) : l'entreprise a été condamnée à des amendes records, dont une de 1,2 milliard d'euros en 2023 pour des transferts de données illégaux vers les États-Unis. Le RGPD a forcé Meta à revoir en profondeur ses pratiques publicitaires en Europe, réduisant sa capacité de ciblage, et donc ses revenus.

        - Coûts de mise en conformité : toutes les entreprises opérant en Europe ont dû investir dans des Délégués à la Protection des Données (DPO), des audits et des modifications de leurs services.

        - « Fatigue du consentement » : les bannières de cookies omniprésentes sont un effet direct, montrant la tension entre la réglementation et l'utilisation.

- Le Digital Services Act (DSA) et Digital Markets Act (DMA) en Europe (depuis 2023) : ces nouvelles lois européennes s'attaquent au pouvoir des « gatekeepers » (les GAFAM).
  - Impacts réels (en cours) :
    - Apple : a été contraint d'autoriser des magasins d'applications alternatifs sur l'iPhone (Sideloading (Chargement latéral)) en Europe, une brèche majeure dans son écosystème fermé.
    - Google : doit modifier ses pages de résultats de recherche pour ne plus favoriser ses propres services (Google Shopping, Google Flights).
    - Ces régulations sont un premier pas vers une limitation du pouvoir des plateformes et une plus grande transparence, préfigurant des contraintes encore plus fortes.

Positionnement dans les six mécanismes de fragilisation

- Mécanisme principal : Impacts sociétaux dans un contexte d'incertitude croissante
  - Justification : ce scénario n'arrive pas de nulle part. C'est la conséquence d'une prise de conscience et d'une réaction politique aux impacts négatifs du numérique : son empreinte environnementale, les abus liés à la collecte de données, la désinformation, etc. La régulation (RGPD, taxe carbone) est une tentative de corriger ces externalités négatives.
- Mécanisme secondaire : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)
  - Justification : la régulation vise souvent à démanteler ou à contraindre les monopoles (les « gatekeepers » du DMA) dont le pouvoir est devenu un problème sociétal. Le modèle économique de ces géants, fondé sur la collecte massive de données, est directement remis en cause.
- Mécanisme indirect : Fragilités géopolitiques
  - Justification : en cas de restriction trop forte en Europe, par exemple, les USA pourraient, en représailles, filtrer les accès aux services cloud des GAFAM.

Opportunités dans la crise

Une régulation sévère, bien que contraignante, clarifie les règles du jeu et récompense les organisations vertueuses. C'est une opportunité pour les entreprises ayant déjà adopté une approche de « privacy by design » et de sobriété numérique de prendre une longueur d'avance. De nouveaux marchés émergeraient autour de la conformité, de l'audit algorithmique et des technologies respectueuses de la vie privée. Pour une entreprise, démontrer une transparence et une éthique exemplaires deviendrait un différenciant clé pour attirer les talents et gagner la confiance des consommateurs.

L'accélération IA

Déploiement massif d'IA générative créant des vulnérabilités systémiques inédites.

Narratif

En 2026, l'IA générative atteint un point de bascule. Chaque entreprise, chaque administration, chaque service public intègre des assistants IA dans ses processus critiques. Ces systèmes, entraînés sur des données publiques, prennent des décisions automatisées à une échelle et une vitesse inhumaines.

Mais cette révolution cache un piège : ces IA, malgré leur sophistication apparente, restent des « boîtes noires » imprévisibles, sujettes aux biais, aux hallucinations et aux manipulations. Quand elles commencent à interagir entre elles, créant des boucles de rétroaction automatisées, le système global devient ingouvernable.

Conséquences pour le numérique et les entreprises

Swiss Re (2024) met en garde contre les « impacts imprévus sur l'assurance » de l'IA et les leçons du « silent cyber » - des risques cachés qui ne se révèlent qu'en cascade.

- Hallucinations en cascade : une IA génère une information erronée qui est reprise par d'autres IA, créant une spirale de désinformation automatisée impossible à arrêter.
- Biais systémiques amplifiés : les préjugés contenus dans les données d'entraînement se propagent à l'échelle industrielle, créant des discriminations massives dans l'emploi, le crédit, la justice.
- Perte de contrôle humain : les décisions critiques sont déléguées à des systèmes que personne ne comprend vraiment, créant une « dictature algorithmique » de fait.

Exemples d'organisations déjà touchées et impacts réels

Ce scénario est en pleine accélération. Les impacts sont déjà visibles :

- Industrie du jeu vidéo et des effets spéciaux : des artistes et des designers commencent d'être remplacés ou voient leurs tâches radicalement modifiées par des IA génératrices d'images et de modèles 3D (Midjourney, Stable Diffusion, etc.). Des studios peuvent désormais créer des environnements ou des personnages en une fraction du temps et du coût.
    - Impact réel : en 2023, le syndicat des acteurs d'Hollywood (SAG-AFTRA) s'est mis en grève, en partie pour obtenir des protections contre l'utilisation de leur image par des IA pour créer des « doubles numériques » sans leur consentement ni leur compensation.
- Secteur du développement logiciel : des outils comme GitHub Copilot (basé sur GPT) sont massivement adoptés.
    - Impact réel : des études montrent que les développeurs utilisant Copilot sont jusqu'à 55 % plus rapides. Si cela augmente la productivité, cela redéfinit aussi le rôle du développeur : moins de temps à écrire du code « boilerplate » , plus de temps à l'architecture, à la relecture et à la résolution de problèmes complexes. Les postes de développeurs juniors, centrés sur des tâches de codage simples, sont directement menacés.

- Les entreprises de contenu et de traduction : des entreprises comme Duolingo ont déjà licencié une partie de leurs traducteurs contractuels, annonçant qu'une grande partie du processus de création de contenu de cours peut désormais être gérée par l'IA.

    - Impact réel : cela montre une tendance où les tâches de production de contenu à grande échelle sont les premières à être automatisées, forçant les professionnels humains à se concentrer sur des tâches à plus haute valeur ajoutée comme la supervision, l'édition finale ou la stratégie créative.

- Secteur du conseil et de l'audit (2025) : l'adoption forcée de l'IA frappe désormais les métiers intellectuels à haute valeur ajoutée.

    - PwC Royaume-Uni : a réduit ses embauches de débutants de 13 % en un an (1 300 en 2025 vs 1 500 en 2024), citant explicitement l'IA. Son patron, Marco Amitrano, met en garde : « Les offres d'emploi pour les professions exposées à l'IA progressent moins vite que pour celles moins exposées, et cet écart se creuse. »

    - Accenture : soupçonné de ne pas adopter l'IA assez rapidement, le géant du conseil a vu son action chuter de 33 % depuis début 2025. Sa patronne, Julie Sweet, annonce des licenciements ciblés : « Nous faisons sortir, dans un calendrier serré, les personnes dont la requalification ne constitue pas une solution viable. » Malgré une formation massive (555 000 consultants sur 780 000), 29 % de l'effectif est considéré comme non-requalifiable.

    - Impact réel : le message est devenu existentiel : « point de salut sans l'IA ». Les entreprises qui n'adoptent pas l'IA assez vite sont attaquées en Bourse, créant une pression maximale sur les travailleurs pour s'adapter ou disparaître.

Positionnement dans les six mécanismes de fragilisation

- Mécanisme principal : Impacts sociétaux dans un contexte d'incertitude croissante

    - Justification : la conséquence la plus massive et la plus visible de ce scénario est le bouleversement du marché du travail, l'obsolescence des compétences et la polarisation de la société. C'est un impact sociétal de très grande ampleur qui remet en question le contrat social.

- Mécanisme secondaire : Fragilités techniques et complexité systémique

    - Justification : l'accélération elle-même est une forme de fragilité. Le rythme du progrès est si rapide qu'il crée une « dette d'adaptation » : la société, les entreprises et les individus n'ont pas le temps d'assimiler le changement, de développer de nouvelles normes ou de mettre en place des garde-fous.

- Mécanisme tertiaire : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)

    - Justification : le développement de l'IA de pointe est extrêmement coûteux et concentré entre les mains d'un très petit nombre d'acteurs (OpenAI/Microsoft, Google, Anthropic). Ce scénario renforce donc le verrouillage et la dépendance pour ces quelques entreprises.

Opportunités dans la crise

L'automatisation massive des tâches intellectuelles représente une opportunité de repenser fondamentalement l'organisation du travail. Les entreprises agiles peuvent en profiter pour libérer leurs équipes des tâches répétitives et à faible valeur ajoutée, leur permettant de se concentrer sur la créativité, la stratégie et la relation client.

C'est également une chance de créer de nouveaux services et produits innovants, établis sur une collaboration homme-machine efficace. L'enjeu devient de transformer la menace de l'obsolescence en une opportunité de montée en compétences généralisée.

La crise de confiance généralisée

Perte massive de confiance du public dans les institutions et les technologies numériques.

Narratif

L'accumulation des scandales — fuites de données, manipulations algorithmiques, surveillance de masse, désinformation — finit par créer un rejet massif du numérique. La population, échaudée par des années de promesses non tenues et de violations de leur vie privée, se détourne en masse des services numériques. Les mouvements de « déconnexion volontaire » se multiplient, les entreprises tech voient leurs valorisations s'effondrer, et les gouvernements peinent à maintenir leurs services publics numériques face à une population qui refuse de les utiliser.

Conséquences pour le numérique et les entreprises

PolyCIVIS (2025) documente comment « la pandémie a exposé les liens entre scepticisme sur l'action gouvernementale, méfiance sociale accrue, et désengagement des processus démocratiques ». AXA (2024) confirme que la désinformation amplifiée par l'IA devient « un outil souvent utilisé dans les conflits géopolitiques ».

- Effondrement des modèles économiques numériques : sans utilisateurs, les plateformes perdent leur valeur. L'économie de l'attention s'effondre.
- Retour au physique coûteux : les entreprises doivent reconstruire des infrastructures physiques (magasins, guichets, centres d'appel humains) qu'elles avaient supprimées.
- Fracture générationnelle : les « natifs numériques » se retrouvent en opposition avec les générations plus âgées, créant des tensions sociales majeures.

Exemples (prémices) déjà observés

Ce scénario n'est plus de la science-fiction. Des versions à plus petite échelle ont déjà eu lieu :

- Manipulation financière (2023) : une image générée par IA montrant une explosion près du Pentagone est devenue virale sur Twitter. En quelques minutes, elle a provoqué une baisse brève, mais significative de l'indice S&P 500, les algorithmes de trading ayant réagi à la « nouvelle » avant que les humains ne puissent la vérifier. Cela a démontré la capacité d'une seule fausse information à affecter les marchés financiers.
- Fraude à l'entreprise (2024) : un employé d'une multinationale à Hong Kong a été trompé par une arnaque sophistiquée. Il a versé 25 millions de dollars à des fraudeurs après avoir participé à une visioconférence avec plusieurs personnes qu'il pensait être ses collègues et son directeur financier, mais qui étaient en réalité un 🕮 Deepfake (Hypertrucage) créé à partir d'images publiques.
- Interférence politique (2023) : lors des élections en Slovaquie, un enregistrement audio généré par IA, imitant la voix d'un leader de parti progressiste discutant d'un plan pour truquer les élections, a été diffusé deux jours avant le vote, à un moment où un moratoire interdisait aux médias de couvrir le sujet, laissant le champ libre à la désinformation.

Positionnement dans les six mécanismes de fragilisation

- Mécanisme principal : Impacts sociétaux dans un contexte d'incertitude croissante
  - Justification : le cœur de la crise est l'effondrement d'un pilier de la société : la confiance partagée dans une réalité commune. L'impact est avant tout social, psychologique et politique, avant d'être technique.
- Mécanisme secondaire : Mécanismes de contagion et ambiguïté des interdépendances
  - Justification : la crise est amplifiée par la nature même des réseaux sociaux, conçus pour une propagation virale et rapide de l'information, sans friction ni vérification. La contagion n'est plus celle d'un virus informatique, mais celle d'une idée ou d'une fausse nouvelle.
- Mécanisme tertiaire : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)
  - Justification : notre dépendance à un petit nombre de plateformes (Facebook, X, WhatsApp, TikTok) pour nous informer crée un verrouillage. Leurs algorithmes, optimisés pour l'engagement plutôt que pour la vérité, deviennent des accélérateurs de la crise de confiance.

Opportunités dans la crise

Dans un monde où la confiance s'effondre, celle-ci devient la ressource la plus précieuse. Une entreprise qui parvient à être perçue comme une source d'information fiable et authentique acquiert un capital de marque inestimable. C'est une opportunité de se différencier en investissant dans des technologies de certification et de traçabilité (comme la blockchain), en adoptant une communication radicalement transparente et en développant des relations directes et fortes avec ses communautés. Devenir un « îlot de confiance » dans un océan de doutes est une stratégie de long terme extrêmement puissante.

Ils en parlent aussi

- Cascading effects : « Effets en cascade où une défaillance déclenche une série de défaillances dans d'autres systèmes » (Swiss Re, 2024).
- Silent cyber : « Risques cyber non explicitement couverts ou identifiés qui se révèlent lors d'incidents » (Swiss Re, 2024).
- Dependency risk : « Risque créé par la dépendance excessive à un nombre limité de fournisseurs technologiques » (Swiss Re, 2024).
- Polycrise : « Enchevêtrement causal de crises dans de multiples systèmes globaux » (Nature Communications, 2025).
- Seuil critique : « Point au-delà duquel les événements interconnectés déclenchent une réaction en chaîne incontrôlée » (Scheffran, 2025).

Références

Fragilités géopolitiques

[51] Henry Farrell et Abraham L. Newman. "Weaponized Interdependence : How Global Economic Networks Shape State Coercion". In : *International Security* 44.1 (2019), p. 42-79. URL : https://direct.mit.edu/isec/article/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic.

[52] Chaire Digital, Gouvernance et Souveraineté. *Souveraineté numérique et crise géopolitique*. 2022. URL : https://www.sciencespo.fr/public/chaire-numerique/2022/12/09/compte-rendu-retour-sur-la-conference-annuelle-2022-souverainete-numerique-et-crise-geopolitique/.

Fragilités physiques et climatiques

[53] Groupe d'experts intergouvernemental sur l'évolution du climat (GIEC). *Climate Change 2022 : Mitigation of Climate Change*. AR6 Working Group III. 2022. URL : https://www.ipcc.ch/report/ar6/wg3/downloads/report/IPCC_AR6_WGIII_SummaryVolume.pdf.

[54] The Shift Project. *Rapport intermédiaire sur les consommations énergétiques et impacts climatiques des infrastructures numériques*. 2025. URL : https://theshiftproject.org/app/uploads/2025/04/2025_03_06-TSP-Rapport-intermediaire-IA-quelles-infra-num-monde-decarbone.pdf.

[55] The Shift Project. *Intelligence artificielle, données, calculs : quelles infrastructures dans un monde décarboné ?* 2025. URL : https://theshiftproject.org/publications/intelligence-artificielle-centres-de-donnees-rapport-final/.

Fragilités techniques

[56] Steven M. Rinaldi, James P. Peerenboom et Terrence K. Kelly. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". In : *IEEE Control Systems Magazine* 21.6 (2001), p. 11-25. DOI : 10.1109/37.969131. URL : https://doi.org/10.1109/37.969131.

[57] Sobhan Sean Arisian et al. "Cyber risk mitigation in critical supply chains". In : (2025). URL : https://www.researchgate.net/publication/396455676_Cyber_risk_mitigation_in_critical_supply_chains.

Fragilités de contagion et systémique

[58] Dirk HELBING. “Globally networked risks and how to respond”. In : *Nature* 497 (2013), p. 51-59. URL : https://www.nature.com/articles/nature12047.

[59] *S’inspirer de l’épidémiologie pour lutter contre les cybermenaces*. URL : https://www.polytechnique-insights.com/tribunes/digital/sinspirer-de-lepidemiologie-pour-lutter-contre-les-cybermenaces/.

Fragilités socio-techniques

[60] Everett M. ROGERS. *Diffusion of Innovations*. 5e éd. Free Press, 2003. URL : https://teddykw2.wordpress.com/wp-content/uploads/2012/07/everett-m-rogers-diffusion-of-innovations.pdf.

[61] Laure LAHAYE. *Femmes et vulnérabilité numérique : causes et conséquences*. Soralia, 2022. URL : https://www.soralia.be/accueil/etude-2022-femmes-et-vulnerabilite-numerique-quelles-causes-pour-quelles-consequences/.

Fragilités des impacts sociétaux

[62] Shoshana ZUBOFF. *The Age of Surveillance Capitalism*. PublicAffairs, 2019. URL : https://www.hbs.edu/faculty/Pages/item.aspx?num=56791.

Annexe F

Exemples inspirants

L’innovation en matière de résilience ne vient pas toujours des grandes entreprises technologiques. Des communautés et territoires à travers le monde développent des stratégies remarquables face aux crises, offrant des leçons transposables à toute organisation.

F.1 Oseja de Sajambre : l'autonomie énergétique comme fondement de la résilience

Dans les montagnes reculées du nord de l'Espagne, le village d'Oseja de Sajambre (300 habitants) a transformé une vulnérabilité critique en force stratégique. Confronté à des coupures électriques récurrentes, le village a construit une autonomie énergétique complète.

Cette transformation est remarquable : micro-réseaux hydroélectriques locaux alimentés par les rivières de montagne, stockage communautaire par batteries permettant 48 heures d'autonomie, gestion intelligente mais décentralisée de la distribution [4, 3, 5].

Le résultat : quand le réseau national défaille, Oseja continue de fonctionner normalement. Le village a transformé son isolement géographique en atout de résilience, avec une réduction de 40 % de la facture énergétique collective et une attractivité accrue pour de nouveaux résidents.

Le principe clé : **ne pas dépendre d'une infrastructure unique qu'on ne contrôle pas**. Oseja a compris qu'une dépendance totale au réseau national créait un point de défaillance unique inacceptable.

Cette approche est directement transposable à votre infrastructure numérique. Comme Oseja avec l'électricité, développez des capacités locales pour les services critiques : edge computing pour les traitements sensibles, serveurs on-premise pour les données critiques, capacités de traitement autonomes fonctionnant sans Internet, fournisseurs locaux ou régionaux pour réduire les dépendances géopolitiques.

L'investissement initial est compensé par la continuité de service garantie. Quand AWS tombe en panne et paralyse des milliers d'entreprises, votre infrastructure locale continue de servir vos utilisateurs.

F.2 Wellington : anticiper les chocs systémiques

Wellington, capitale de la Nouvelle-Zélande, est construite sur l'une des failles sismiques les plus actives au monde. Face à cette menace permanente, la ville a développé une approche systémique unique de résilience.

Le Resilient Cities Network documente leur stratégie : infrastructures redondantes d'approvisionnement en eau avec 77 points d'accès communautaires autonomes, systèmes de communication d'urgence multiples (radio, satellite, mesh networks), exercices de simulation réguliers impliquant toute la population [24].

Le plus remarquable : Wellington teste régulièrement ses systèmes en mode dégradé. Chaque quartier peut fonctionner 72 heures en autonomie complète. Cette « résilience distribuée » garantit qu'aucun point de défaillance unique ne peut paralyser la ville entière. Lors du séisme de Kaikōura en 2016 (magnitude 7.8), Wellington a maintenu ses services essentiels opérationnels malgré des dégâts importants.

Le principe fondamental : **concevoir pour la défaillance, pas pour la perfection**. Wellington assume que tout peut tomber en panne et construit ses systèmes en conséquence.

Pour votre organisation, testez régulièrement les systèmes en mode dégradé. Organisez des « Game Days » où vous simulez des pannes majeures et observez comment les équipes réagissent. Concevez les services pour qu'ils fonctionnent en mode dégradé : un site e-commerce qui continue de prendre des commandes même si le système de recommandation est hors ligne.

Pensez-vous que votre organisation peut tenir 72 heures en cas d'aléa majeur ? Wellington vous montre le chemin : identifiez vos services critiques, construisez des capacités d'autonomie, testez régulièrement, documentez les leçons apprises.

F.3 Les maisons flottantes des Tausug : l'adaptation permanente comme mode de vie

Aux Philippines, la communauté Tausug vit depuis des siècles dans l'un des environnements les plus hostiles : typhons dévastateurs, inondations massives, élévation du niveau de la mer. Plutôt que de lutter contre ces forces par des infrastructures rigides, les Tausug ont développé une approche radicale : construire des maisons sur pilotis en bambou conçues pour s'adapter.

La BBC Future révèle leur secret : structures flexibles qui plient sans se rompre, matériaux locaux facilement remplaçables, conception modulaire permettant des réparations rapides, transmission intergénérationnelle des savoir-faire [25].

Cette architecture repose sur un principe contre-intuitif : la fragilité apparente est une force. Une maison en béton résiste mieux à un typhon modéré, mais s'effondre catastrophiquement face à un typhon majeur. Une maison Tausug plie, se déforme, mais reste debout et peut être réparée en quelques jours avec des matériaux locaux. Le coût de reconstruction est dérisoire, et la communauté conserve son autonomie. Le bambou pousse rapidement, absorbe plus de CO_2 que la plupart des arbres, et le coût initial est 10 à 20 fois inférieur aux constructions en béton.

Le principe fondamental : **concevoir pour la réparation plutôt que pour la perfection**. Un système parfait mais irréparable est moins résilient qu'un système imparfait mais facilement réparable.

Dans votre architecture numérique, privilégiez des systèmes modulaires où chaque composant peut être remplacé indépendamment, documentez exhaustivement pour que n'importe qui puisse intervenir, choisissez des technologies ouvertes plutôt que propriétaires, formez vos équipes à la réparation.

Comme le bambou qui plie sous la tempête, les systèmes doivent absorber les chocs sans se rompre. Préférez une architecture microservices où la défaillance d'un service n'affecte pas les autres, plutôt qu'un monolithe où tout s'effondre ensemble.

F.4 L'Égypte et les barrières de roseaux : solutions simples pour problèmes complexes

Face à l'érosion côtière accélérée par le changement climatique, le delta du Nil fait face à une menace existentielle. Les solutions conventionnelles – digues en béton, enrochements – coûtent des centaines de millions de dollars. Des communautés égyptiennes ont redécouvert une technique millénaire : les barrières de roseaux.

Le United Nations Development Program documente cette innovation frugale : coût dérisoire (100 fois moins cher que le béton), matériaux locaux et renouvelables, maintenance par les communautés elles-mêmes, efficacité surprenante avec 60 % de réduction de l'érosion [26].

Le mécanisme est élégant : les barrières ralentissent les vagues et favorisent la sédimentation naturelle. Au lieu de combattre la mer par la force, elles travaillent avec les processus naturels. Les roseaux se renouvellent naturellement, créant un système auto-entretenu.

Cette approche génère des bénéfices multiples : les barrières créent des nurseries pour les poissons, filtrent l'eau, offrent un habitat pour les oiseaux migrateurs.

La leçon : **les solutions les plus robustes ne sont pas nécessairement les plus sophistiquées**. Un système de sauvegarde sur bandes magnétiques, technologie des années 1960, reste imbattable pour l'archivage long terme : pas de dépendance au cloud, pas de risque de ransomware, durée de vie de 30 ans. Une documentation papier des procédures critiques garantit la continuité en cas de panne totale.

Résistez à la tentation du « toujours plus sophistiqué ». Avant d'adopter la dernière technologie, posez-vous la question : une solution plus simple pourrait-elle résoudre le même problème ? Cette complexité apporte-t-elle une valeur proportionnelle ? Pourrions-nous utiliser une technologie éprouvée plutôt qu'une nouveauté non testée ?

Comme les barrières de roseaux, les solutions les plus durables sont souvent les plus simples.

F.5 Fairphone : la durabilité comme stratégie de résilience

Dans un secteur dominé par l'obsolescence programmée, Fairphone démontre qu'une approche radicalement différente est viable. Fondée en 2013, cette entreprise sociale a construit son modèle sur un principe subversif : créer des smartphones conçus pour durer, être réparés et évoluer.

Leur smartphone modulaire défie le modèle dominant : conception modulaire permettant le remplacement de chaque composant par l'utilisateur, documentation complète et outils fournis, chaîne d'approvisionnement transparente et diversifiée, support logiciel étendu (7 ans minimum contre 2-3 ans) .

Les résultats : un Fairphone fonctionne deux fois plus longtemps qu'un smartphone classique, réduisant la dépendance aux chaînes d'approvisionnement globales. Quand la pénurie de semi-conducteurs a frappé en 2021-2022, les utilisateurs ont simplement continué d'utiliser leurs appareils ou remplacé uniquement les composants défaillants. L'entreprise est profitable depuis 2019, avec une fidélité client exceptionnelle (Net Promoter Score de 70, contre 30-40 pour la concurrence).

Le principe clé : **la durabilité n'est pas une contrainte, mais un avantage stratégique**. En concevant pour la longévité, Fairphone a construit une résilience structurelle face aux chocs d'approvisionnement.

Cette philosophie s'applique à vos systèmes : privilégiez les architectures ouvertes basées sur des standards plutôt que des solutions propriétaires verrouillées. Documentez exhaustivement pour que n'importe quel développeur puisse maintenir. Choisissez des technologies matures et stables plutôt que les dernières modes. Investissez dans la qualité du code plutôt que l'ajout permanent de fonctionnalités.

Un système conçu pour durer 10 ans coûte moins cher qu'un système remplacé tous les 2 ans.

F.6 Infomaniak : la sobriété comme levier de robustesse

L'hébergeur suisse Infomaniak démontre qu'une approche radicale de sobriété peut être un puissant levier de robustesse. Fondée en 1994 et restée indépendante, cette entreprise a construit son avantage sur un principe contre-intuitif : **prolonger la durée de vie des serveurs jusqu'à 15 ans**, soit deux à trois fois plus que la moyenne (5-7 ans).

Cette approche est rendue possible par l'achat de matériel évolutif et réparable, l'optimisation logicielle continue, et une culture valorisant la frugalité .

Les bénéfices sont multiples. Sur le plan environnemental, Infomaniak affiche un PUE de 1.06 contre 1.8 en moyenne européenne, grâce au refroidissement par air extérieur et à l'allocation dynamique des ressources. Cette efficacité se traduit par des coûts 40 % inférieurs à la concurrence. Sur le plan stratégique, la longévité des équipements réduit la dépendance aux chaînes d'approvisionnement – un avantage décisif lors de la pénurie de semi-conducteurs de 2021-2022.

Cette sobriété génère une résilience organisationnelle remarquable. En maîtrisant des infrastructures utilisées depuis 10-15 ans, les équipes ont développé une expertise profonde permettant de résoudre les problèmes rapidement. Cette stabilité permet de maintenir une équipe réduite (180 personnes pour 400 000 clients).

Le principe : **la sobriété n'est pas l'ennemie de la performance, mais l'alliée de la robustesse**. En refusant le renouvellement permanent, Infomaniak a construit une organisation plus simple, stable, rentable et résiliente.

La leçon : en prolongeant la durée de vie des équipements et en optimisant les logiciels, vous réduisez votre exposition aux chocs externes et construisez une organisation plus autonome.

Cela nécessite un changement de mentalité : valoriser la durabilité plutôt que la nouveauté, l'optimisation plutôt que le remplacement, la maîtrise technique plutôt que l'externalisation.

F.7 Mine urbaine : transformer les déchets en ressources stratégiques

Face à la raréfaction des matières premières et aux tensions géopolitiques sur les chaînes d'approvisionnement, le concept de « mine urbaine » émerge comme une stratégie de résilience. L'International Copper Association documente cette approche : les déchets électroniques contiennent des concentrations de métaux précieux (or, argent, cuivre, terres rares) souvent supérieures aux minerais naturels.

Une tonne de cartes électroniques contient jusqu'à 200 grammes d'or, contre 5 grammes par tonne de minerai aurifère [32].

Le principe fondamental : **vos équipements obsolètes ne sont pas des déchets, mais des gisements de ressources**. Plutôt que de dépendre exclusivement des chaînes d'approvisionnement mondiales pour vos composants critiques, vous pouvez développer une capacité locale de récupération et de réutilisation. Cette approche, documentée par l'économie circulaire, transforme la contrainte réglementaire (gestion des déchets) en opportunité stratégique (autonomie d'approvisionnement).

Pour le numérique, cela signifie créer une « Digital Urban Mine » organisationnelle ou territoriale. Plutôt que de « jeter » les serveurs, les ordinateurs et les équipements réseau en fin de vie, vous constituez un stock de composants réutilisables : disques durs pour stockage froid, mémoires pour environnements de test, cartes réseau pour infrastructures secondaires, alimentations et ventilateurs pour pièces de rechange.

Cette stratégie, combinée avec une gouvernance de bien commun inspirée des travaux d'Elinor Ostrom [35], permet de mutualiser ces ressources entre plusieurs organisations d'un même territoire.

Les bénéfices sont multiples : réduction de la dépendance aux approvisionnements externes (particulièrement critique en période de pénurie), diminution drastique des coûts de maintenance (composants gratuits ou à prix marginal), réduction de l'empreinte environnementale (éviter la fabrication de composants neufs), création d'emplois locaux qualifiés (démantèlement, test, reconditionnement).

F.8 Chaos Engineering : apprendre par l'échec contrôlé

En 2008, Netflix subit une panne majeure de sa base de données qui paralyse le service pendant trois jours. Cette défaillance met en évidence une vulnérabilité critique : l'architecture monolithique de l'entreprise crée un point de défaillance unique inacceptable. Face à ce constat, Netflix prend une décision radicale : migrer vers le cloud AWS et construire une architecture distribuée capable de résister aux pannes.

Mais Netflix va plus loin. Plutôt que de simplement espérer que le système résiste, l'entreprise développe une approche révolutionnaire : introduire volontairement des pannes dans les systèmes de production pour tester leur capacité à y résister.

Cette discipline, baptisée « Chaos Engineering », repose sur un principe simple mais puissant : **si vous ne testez pas régulièrement les systèmes en conditions dégradées, vous ne découvrirez leurs faiblesses que lors d'une vraie crise** [103].

La méthode consiste à formuler des hypothèses sur le comportement attendu du système (« si ce serveur tombe, le trafic doit être automatiquement redirigé »), puis à tester ces hypothèses en production en introduisant des perturbations contrôlées : arrêt aléatoire de serveurs (« Chaos Monkey »), simulation de latence réseau, saturation de ressources, corruption de données. Les résultats révèlent les points de défaillance cachés, les dépendances non documentées, les hypothèses erronées dans l'architecture.

Cette approche transforme radicalement la culture organisationnelle. Au lieu de craindre les pannes, les équipes les provoquent délibérément dans un cadre maîtrisé. Au lieu de découvrir les failles lors d'incidents critiques à 3 heures du matin, elles les identifient le mardi après-midi avec toute l'équipe disponible.

Au lieu de supposer que les systèmes sont résilients, elles le vérifient empiriquement et régulièrement.

Les organisations qui pratiquent le Chaos Engineering rapportent une réduction significative de la durée et de la fréquence des incidents en production. Plus important encore, elles développent une confiance fondée sur des preuves concrètes plutôt que sur des espoirs théoriques.

Comme le formule Netflix : « Nous ne faisons pas confiance à nos systèmes parce qu'ils n'ont jamais échoué, mais parce que nous les avons vus échouer et se rétablir des centaines de fois ».

F.9 Antifragilité : bénéficier du désordre

Nassim Nicholas Taleb introduit un concept qui dépasse la simple résilience : l'antifragilité. Un système résilient résiste aux chocs et retrouve son état initial. Un système antifragile, lui, s'améliore grâce aux chocs [70].

Comme les muscles qui se renforcent par l'exercice, certains systèmes bénéficient du stress, de la volatilité et du désordre.

Cette distinction est fondamentale pour concevoir des organisations robustes. Un système fragile se brise sous la pression (architecture monolithique où une défaillance provoque l'effondrement total). Un système résilient absorbe les chocs et se rétablit (architecture redondante qui bascule sur des systèmes de secours). Un système antifragile tire parti des perturbations pour devenir plus fort (architecture qui apprend de chaque incident et s'adapte automatiquement).

Dans le domaine numérique, l'antifragilité se manifeste par des architectures qui évoluent en réponse aux stress. Les systèmes de détection d'intrusion qui affinent leurs règles après chaque tentative d'attaque. Les algorithmes de routage qui découvrent de meilleurs chemins lors des congestions. Les bases de données qui optimisent leurs index en fonction des requêtes réelles. Les équipes qui documentent systématiquement chaque incident et transforment chaque erreur en amélioration permanente.

La clé de l'antifragilité réside dans trois principes : la redondance (avoir des options multiples pour absorber les chocs), la variabilité (exposer régulièrement le système à de petits stress pour le renforcer), et l'apprentissage (capturer et intégrer les leçons de chaque perturbation).

Comme l'écrit Taleb : « Le vent éteint les bougies mais attise les incendies ». L'objectif n'est pas d'éviter le vent, mais de devenir un incendie plutôt qu'une bougie.

F.10 37signals (Basecamp) : la sobriété comme stratégie

Dans un secteur obsédé par la croissance et la complexité, 37signals (créateur de Basecamp) démontre qu'une approche radicalement sobre peut être extraordinairement performante. Avec seulement 60 personnes et 6 outils internes, l'entreprise génère 100 millions de dollars de revenus annuels [34].

Leur règle d'or : **« Si ça ne sert pas directement le client, on ne le fait pas »**.

Cette philosophie se traduit par des choix contre-intuitifs. Pas de réunions régulières (sauf exception justifiée). Pas d'objectifs de croissance arbitraires. Pas de levées de fonds. Pas de tableaux de bord complexes. Pas de processus standardisés imposés. Chaque outil, chaque processus, chaque poste doit justifier son existence par sa contribution directe à la valeur client.

Tout le reste est éliminé sans pitié.

Le résultat : une organisation d'une efficacité remarquable. Le ratio revenus par employé (1,67 million de dollars) dépasse largement la moyenne du secteur. La satisfaction client atteint des niveaux exceptionnels car toute l'énergie est concentrée sur le produit. Les employés travaillent dans un environnement simple et prévisible, sans la surcharge cognitive des organisations complexes. La rentabilité permet une totale indépendance stratégique.

Pour votre organisation, la leçon est claire : la complexité n'est pas une fatalité, mais un choix. Chaque outil ajouté à votre bibliothèque technologique a un coût caché : formation, intégration, maintenance, support, licences, mais surtout charge cognitive pour vos équipes.

En adoptant une discipline de sobriété radicale – auditer régulièrement les outils, éliminer systématiquement ceux qui ne servent pas directement les utilisateurs, résister à la tentation d'ajouter « juste un outil de plus » – vous pouvez construire une infrastructure à la fois plus simple, plus robuste et plus performante.

F.11 L'Estonie : l'État numérique minimaliste

L'Estonie a construit l'un des systèmes de gouvernance numérique les plus avancés au monde avec une approche étonnamment minimaliste. Pour 1,3 million de citoyens, le pays emploie seulement 13 personnes dédiées à l'infrastructure IT gouvernementale, avec un budget annuel de 50 millions d'euros — contre plus d'un milliard pour des pays de taille comparable [115].

Le résultat : 99 % des services publics disponibles en ligne, 98 % de satisfaction citoyenne, et une efficacité administrative qui fait référence mondiale.

Le secret de cette performance tient en deux principes architecturaux. Premier principe : **l'interopérabilité par conception**. Plutôt que de construire des systèmes isolés pour chaque administration, l'Estonie a développé X-Road, une couche d'échange de données sécurisée qui permet à tous les systèmes publics et privés de communiquer entre eux. Un citoyen n'entre ses données qu'une seule fois; elles sont ensuite réutilisées par tous les services autorisés. Cette architecture évite la duplication des données, réduit drastiquement les coûts de développement et garantit la cohérence de l'information.

Deuxième principe : **une identité numérique unique et sécurisée**. Chaque citoyen dispose d'une carte d'identité électronique qui lui permet de s'authentifier auprès de n'importe quel service, de signer des documents numériquement, et même de voter en ligne. Cette infrastructure de confiance élimine le besoin de systèmes d'authentification multiples et permet des transactions entièrement dématérialisées. Résultat concret : déclarer ses impôts prend 3 à 5 minutes, créer une entreprise prend 18 minutes, et 99 % des prescriptions médicales sont numériques.

En adoptant une approche « API-first » où chaque service expose ses fonctionnalités de manière standardisée, en investissant dans une couche d'identité et d'authentification unifiée, et en privilégiant la réutilisation plutôt que la duplication, l'architecture devient plus simple et donc plus résiliente.

Pour votre organisation, l'Estonie démontre qu'une architecture simple, fondée sur des standards ouverts et l'interopérabilité, surpasse largement les approches complexes et propriétaires.

F.12 Amsterdam, ville donut : l'équilibre comme boussole

Amsterdam est devenue en 2020 la première grande ville au monde à adopter le modèle du Donut de Kate Raworth comme cadre stratégique pour guider ses politiques publiques. La « Amsterdam Donut Coalition » fédère citoyens, entreprises, municipalité et institutions de recherche autour d'une mission commune : faire vivre la région « dans le Donut » — c'est-à-dire au-dessus du plancher social (répondre aux besoins fondamentaux de tous) et en dessous du plafond écologique (respecter les limites planétaires) [37].

Cette approche transforme radicalement la prise de décision. Chaque projet, chaque politique, chaque investissement est évalué selon deux critères : contribue-t-il à élever ceux qui sont sous le plancher social ? Réduit-il la pression sur les limites écologiques ? À travers des festivals annuels, des laboratoires vivants et des rencontres régulières, la coalition rend visibles les efforts collectifs et inspire d'autres territoires à adopter cette boussole pour prospérer dans un espace juste et sûr.

Les résultats concrets commencent à émerger : réduction de 55 % des émissions de CO_2 d'ici 2030 (objectif inscrit dans la stratégie municipale), développement massif de l'économie circulaire (objectif : 100 % circulaire en 2050), politiques de logement social renforcées, investissements dans les infrastructures vertes.

Plus important encore, le Donut fournit un langage commun qui permet aux différents acteurs de la ville — du secteur privé aux associations citoyennes — de collaborer autour d'objectifs partagés.

Pour votre organisation, Amsterdam démontre la puissance d'une vision claire et partagée. En adoptant le Donut comme cadre d'évaluation des services numériques — Quels services contribuent au bien-être social ? Lesquels dépassent les limites écologiques acceptables ? — vous pouvez aligner votre stratégie IT sur des objectifs de durabilité tout en renforçant votre licence sociale d'opérer.

Cette approche transforme la contrainte environnementale en opportunité d'innovation et de différenciation.

F.13 Patagonia : la transparence radicale comme stratégie de résilience

Le 25 novembre 2011, jour du Black Friday, Patagonia publie une publicité pleine page dans le New York Times : « Don't Buy This Jacket »[114]. Sous l'image de leur polaire R2, l'entreprise détaille l'impact : 135 litres d'eau, 9 kilos de CO_2, deux tiers de son poids en déchets.

Alors que toutes les marques multiplient les promotions, Patagonia demande à ses clients de ne pas acheter et révèle les coûts environnementaux réels de ses produits. Cette transparence s'inscrit dans la Common Threads Initiative encourageant la réparation plutôt que l'achat.

Le résultat défie toute logique : les ventes augmentent de 30 %, le chiffre d'affaires passant de 400 millions de dollars à 543 millions en un an. En alignant parfaitement son discours avec ses valeurs, Patagonia transforme ses clients en partenaires d'une mission commune. Le programme Worn Wear se développe massivement, la confiance client atteint des niveaux exceptionnels.

Le principe clé : la transparence radicale sur ses limites construit une confiance inébranlable. Dans un contexte où le greenwashing mine la crédibilité, cette honnêteté différencie radicalement l'entreprise. La marque ne prétend pas être parfaite ; elle expose ses contradictions et invite ses clients à faire partie de la solution.

Pour votre infrastructure numérique, l'approche est directement transposable : affichez la consommation énergétique de vos serveurs, les émissions de votre cloud, le coût environnemental de vos fonctionnalités. Communiquez vos efforts, mais aussi vos échecs. Créez des tableaux de bord d'impact accessibles, développez des mécanismes de réduction d'empreinte.

Cette transparence ne nuit pas à votre activité — elle la renforce. Votre communauté devient votre meilleur défenseur. La résilience se construit sur la confiance, et la confiance naît de la transparence, même quand elle révèle des imperfections.

[3] ENTSO-E. *Factual Report : 28 April 2025 Iberian Blackout*. European Network of Transmission System Operators for Electricity, 2025. URL : https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/.

[4] Nicolás BOULLOSA. *The Asterix village in the dark : resilience in a blacked-out world*. Avr. 2025. URL : https://faircompanies.com/articles/the-asterix-village-in-the-dark-resilience-in-a-blacked-out-world/.

[5] ONE MEDIA. *Le village autonome qui a échappé au blackout électrique*. 2025. URL : https://onemedia.fr/actualite/le-village-autonome-qui-a-echappe-au-grand-blackout-electrique/.

[24] RESILIENT CITIES NETWORK. *Building Wellington's Resilient Community Water Access*. 2020. URL : https://resilientcitiesnetwork.org/wellington-water-security/.

[25] BBC. *Floating bamboo houses keep this indigenous tribe safe*. 2024. URL : https://www.bbc.com/future/article/20240531-the-floating-houses-built-to-withstand-typhoons-and-flooding-in-the-philippines.

[26] UNITED NATIONS DEVELOPMENT PROGRAM. *Learning from local ingenuity – how simple reed fencing has unlocked a solution to rising sea levels in Egypt*. 2022. URL : https://www.undp.org/arab-states/blog/learning-local-ingenuity-how-simple-reed-fencing-has-unlocked-solution-rising-sea-levels-egypt/.

[32] INTERNATIONAL COPPER ASSOCIATION. *Mines urbaines*. URL : https://internationalcopper.org/fr/policy-focus/climate-environment/urban-mining/.

[34] 37SIGNALS. *Getting Real : The smarter, faster, easier way to build a successful web application*. URL : https://basecamp.com/gettingreal.

[35] Elinor OSTROM. *Governing the Commons*. Cambridge University Press, 1990.

[37] *Amsterdam, ville donut*. URL : https://amsterdamdonutcoalitie.nl/.

[114] PATAGONIA. *Don't Buy This Jacket*. 2011. URL : https://eu.patagonia.com/fr/fr/stories/planete/activisme/dont-buy-this-jacket-black-friday-and-the-new-york-times/story-18615.html.

[115] E-ESTONIA. *We have built a digital society and so can you*. URL : https://e-estonia.com/.

Annexe G

Vulnérabilités paradoxales — Protection défaillante et dépendances invisibles

G.1 Deux catastrophes révélatrices de notre fragilité systémique

Les concepts théoriques de la polycrise prennent une dimension concrète à travers deux incidents récents qui illustrent parfaitement les trois caractéristiques de la polycrise numérique : l'interconnexion structurelle, la synchronisation temporelle et l'amplification non-linéaire. Ces événements révèlent deux types de vulnérabilités paradoxales : d'un côté, une protection qui devient menace (CrowdStrike), de l'autre, une dépendance invisible mais critique (Spruce Pine).

G.2 L'incident CrowdStrike : quand la sécurité devient vulnérabilité

Le 19 juillet 2024 est le jour où un simple fichier de 40 KB a paralysé l'économie mondiale. À 04h09 UTC, CrowdStrike, l'un des leaders mondiaux de la cybersécurité protégeant 29 000 organisations, a déployé une mise à jour défectueuse de son agent Falcon. En quelques minutes, 8,5 millions de machines Windows sont entrées dans une boucle de redémarrage fatal, le fameux « Blue Screen of Death » [109].

Les conséquences ont été immédiates et systémiques, illustrant parfaitement le phénomène d'amplification non-linéaire décrit dans la théorie de la polycrise :

Transport aérien : Delta Airlines a dû annuler plus de 6 000 vols, affectant 500 000 passagers, avec des effets en cascade sur l'ensemble du trafic mondial [121]

Santé : le système de santé britannique NHS a reporté des milliers d'interventions chirurgicales, mettant potentiellement des vies en danger [122]

Commerce : les supermarchés australiens Woolworths et Coles ont dû fermer leurs caisses automatiques, paralysant les achats de millions de consommateurs [123]

Finance : les banques américaines ont suspendu les transactions, gelant temporairement des milliards de dollars

Au total, Parametrix estime les pertes directes à 5,4 milliards de dollars, sans compter les effets de cascade et les pertes de productivité qui pourraient doubler ce montant [16].

Ce qui a évité une catastrophe bien plus grave est le déploiement progressif des mises à jour par fuseau horaire. En effet, dès que les premières alertes ont été remontées, l'éditeur a arrêté le déploiement de la mise à jour ; imaginons un instant qu'au lieu d'être un bug, c'était une cyberattaque qui ne se déclenchait que 24 heures après la première mise à jour…

Le paradoxe est ainsi saisissant : c'est précisément un outil conçu pour protéger les systèmes qui les a mis à genoux. CrowdStrike, censé être le gardien de la cybersécurité, est devenu le vecteur d'une des plus grandes pannes informatiques de l'histoire. Cette ironie révèle une vérité fondamentale : dans un système hyper-connecté et hyper-dépendant, chaque point de protection peut devenir un point de défaillance unique (SPOF – Single Point of Failure). L'interconnexion structurelle qui devait renforcer notre sécurité collective est devenue notre talon d'Achille.

G.3 La mine de Spruce Pine : la faiblesse invisible de l'économie numérique

Plus troublant encore car totalement imprévisible pour ceux qui n'ont pas encore une approche systémique : en septembre 2024, l'ouragan Helene a frappé la Caroline du Nord avec une violence inédite. Parmi les dégâts, un site industriel méconnu du grand public, mais crucial pour l'économie mondiale : les mines de quartz de Spruce Pine, exploitées par Sibelco et The Quartz Corp. Ces deux entreprises fournissent 80 à 90 % du quartz ultra-pur mondial, un matériau indispensable et non substituable à ce jour pour la fabrication des semiconducteurs et des panneaux solaires [124].

Le quartz de Spruce Pine n'est pas un composant parmi d'autres : sa pureté exceptionnelle (99,9999 % de SiO_2) est nécessaire pour fabriquer les creusets dans lesquels sont fondus les lingots de silicium. Sans ce quartz spécifique :

- Pas de semiconducteurs de dernière génération
- Pas de processeurs pour smartphones, ordinateurs, serveurs
- Pas d'infrastructure pour l'IA ou le cloud computing
- Pas de composants pour les véhicules modernes
- Pas de transition énergétique avec les panneaux solaires

Wired qualifie à juste titre Spruce Pine de « most important place you've never heard of » (le lieu le plus important dont vous n'avez jamais entendu parler) [125].

L'ouragan a stoppé la production pendant deux mois. Les experts estiment qu'au-delà de trois mois d'arrêt, les stocks mondiaux seraient épuisés, entraînant une paralysie progressive de toute la chaîne de production électronique mondiale [126]. Un simple événement météorologique localisé dans les Appalaches aurait pu mettre à genoux l'économie numérique planétaire — parfait exemple de ce que Nassim Taleb appelle un « cygne noir », cet événement imprévisible aux conséquences catastrophiques [83].

Cette vulnérabilité illustre la synchronisation temporelle de la polycrise : avec l'intensification des événements climatiques extrêmes due au réchauffement, ce qui était autrefois un risque théorique devient une menace récurrente. Et si demain, ce n'était pas un, mais deux ou trois ouragans successifs qui frappaient la région ?

G.4 L'aveuglement systémique : quand l'optimisation prime sur la résilience

Le plus inquiétant dans l'affaire Spruce Pine est que cette vulnérabilité était connue mais délibérément ignorée. Dès 2018, des rapports du département américain de la Défense alertaient sur la criticité de ce site pour la sécurité nationale [127]. Le Bureau de l'industrie et de la sécurité du département du Commerce avait classé le quartz de haute pureté comme « matériau critique » [128]. Pourtant, aucune diversification n'a été entreprise, aucun stock stratégique suffisant constitué, aucune source alternative développée.

La raison ? L'optimisation économique prime systématiquement sur la résilience tant que la catastrophe n'est pas advenue. Créer des redondances, diversifier les sources, constituer des stocks stratégiques — tout cela a un coût que les marchés financiers, focalisés sur les résultats trimestriels, refusent d'assumer. Comme le souligne le rapport de la Maison Blanche sur les chaînes d'approvisionnement critiques : « Le marché seul ne peut pas résoudre les vulnérabilités de nos chaînes d'approvisionnement » [129].

G.5 Leçons pour une résilience systémique

Ces deux incidents révèlent les mêmes dysfonctionnements structurels :

La concentration excessive crée des points de défaillance uniques qui peuvent s'avérer fatals pour le système.

L'optimisation à outrance privilégie l'efficacité au détriment de la robustesse.

L'aveuglement collectif amplifié par le biais de confirmation, nous empêche d'agir sur des vulnérabilités pourtant identifiées.

L'interconnexion non maîtrisée transforme des incidents locaux en catastrophes mondiales.

Face à ces défis, la construction d'une véritable résilience systémique nécessite un changement de paradigme : accepter les coûts de la redondance, privilégier la robustesse sur l'efficacité pure, et surtout, développer une gouvernance capable d'arbitrer entre profits à court terme et survie à long terme.

[16] Parametrix. *CrowdStrike's Impact on the Fortune 500*. Analyse économique estimant les pertes directes à 5,4 milliards de dollars pour les entreprises du Fortune 500 (hors Microsoft). 24 juill. 2024. URL : https://www.parametrixinsurance.com/reports-white-papers/crowdstrikes-impact-on-the-fortune-500.

[83] Nassim Nicholas Taleb. *The Black Swan : The Impact of the Highly Improbable*. Ouvrage de référence sur les événements rares et imprévisibles aux conséquences catastrophiques (cygnes noirs). Random House, 2007.

[109] CrowdStrike. *Post-Incident Analysis Report*. Rapp. tech. Rapport officiel post-incident détaillant la mise à jour défectueuse du 19 juillet 2024 qui a affecté 8,5 millions de machines Windows. 2024. URL : https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

[121] Delta Air Lines. *Delta Air Lines Announces September Quarter 2024 Financial Results*. Rapport financier Q3 2024 documentant l'impact de la panne CrowdStrike : plus de 6 000 vols annulés, 500 000 passagers affectés, 500 millions dollars de pertes. 10 oct. 2024. URL : https://ir.delta.com/news/news-details/2024/Delta-Air-Lines-Announces-September-Quarter-2024-Financial-Results/default.aspx.

[122] BBC News. *CrowdStrike : NHS services disrupted by global IT outage*. Documentation médiatique de l'impact sur le système de santé britannique NHS, avec report de milliers d'interventions chirurgicales. 19 juill. 2024.

[123] Sources médias australiennes. *Impact de la panne CrowdStrike sur Woolworths et Coles*. Documentation de la fermeture des caisses automatiques dans les supermarchés australiens suite à la panne. 2024.

[124] NPR. *Spruce Pine just got hit by Helene. The fallout on the tech industry could be huge*. Article documentant le rôle critique de Spruce Pine (80-90% du quartz ultra-pur mondial) et l'impact de l'ouragan Helene. 30 sept. 2024. URL : https://www.npr.org/2024/09/30/nx-s1-5133462/hurricane-helene-quartz-microchips-solar-panels-spruce-pine.

[125] Wired. *Hurricane Helene Will Send Shockwaves Through the Semiconductor Industry*. Analyse approfondie de l'impact de l'ouragan Helene sur les mines de quartz de Spruce Pine et les répercussions sur l'industrie des semiconducteurs. 1er oct. 2024. URL : https://www.wired.com/story/hurricane-helene-shockwaves-semiconductor-industry-microchips-spruce-pine-north-carolina-sand-high-quality-quartz/.

[126] CNN. *Devastation from Hurricane Helene could bring semiconductor supply chain to its knees*. Analyse des experts estimant que les stocks mondiaux de quartz haute pureté seraient épuisés au-delà de trois mois d'arrêt de production. 2 oct. 2024. URL : https://www.cnn.com/2024/10/02/tech/semiconductor-supply-chain-north-carolina-helene.

[127] Defense Logistics Agency. *Supply Chain Illumination in the Department of Defense*. Rapp. tech. Rapport du département de la Défense mentionnant Spruce Pine comme point critique de la chaîne d'approvisionnement en matériaux stratégiques. 13 jan. 2025. URL : https://dbb.defense.gov/Portals/35/Documents/Reports/2025/DBB%20Supply%20Chain%20Illumination%20Report%20CLEARED.pdf.

[128] U.S. Department of Energy. *2023 Critical Materials Assessment*. Rapp. tech. Évaluation des matériaux critiques pour l'énergie et la sécurité nationale, incluant les matériaux nécessaires à la fabrication de semiconducteurs. 27 mai 2023. URL : https://www.energy.gov/sites/default/files/2023-05/2023-critical-materials-assessment.pdf.

[129] White House. *2021–2024 Quadrennial Supply Chain Review*. Rapp. tech. Revue quadriennale des chaînes d'approvisionnement critiques, soulignant que "le marché seul ne peut pas résoudre les vulnérabilités". Déc. 2024. URL : https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/12/20212024-Quadrennial-Supply-Chain-Review.pdf.

Annexe H

La polycrise — Du diagnostic à l'action

Le concept de polycrise, dont les racines remontent aux travaux du sociologue Edgar Morin[72], a été popularisé plus récemment par l'historien Adam Tooze[73] et adopté au plus haut niveau politique, notamment par l'ancien président de la Commission Européenne, Jean-Claude Juncker, pour décrire l'enchevêtrement des défis continentaux[74]. Souvent évoqué dans le contexte de l'Anthropocène, il est devenu essentiel pour comprendre la nature des défis contemporains. Il ne s'agit plus d'une simple succession de crises, mais d'un système complexe où les chocs s'entremêlent et s'amplifient mutuellement.

H.1 Anatomie

Les trois mots-clés importants à retenir sont : *interconnexion*, *synchronisation* et *amplification*.

Plusieurs institutions de premier plan ont défini ce phénomène. Le Cascade Institute parle d'un « enchevêtrement causal de crises [...] qui dégrade significativement les perspectives de l'humanité » [75]. Le réseau académique européen PolyCIVIS met l'accent sur les « effets transfrontaliers, une causalité multiple et des propriétés systémiques complexes » qui défient la gouvernance traditionnelle [47]. De son côté, le chercheur Jürgen Scheffran, dans la revue Global Sustainability, la caractérise comme une situation où des crises multiples, en s'aggravant, déclenchent des « réactions en chaîne en cascade qui dépassent les efforts de contrôle » [74]. Ces définitions convergent vers trois caractéristiques fondamentales identifiées par Thomas Homer-Dixon [78] :

1. L'interconnexion structurelle : les systèmes économiques, technologiques, sociaux et environnementaux sont désormais si étroitement imbriqués qu'une perturbation dans l'un se propage inévitablement aux autres. La crise financière de 2008, née du marché immobilier américain, s'est propagée en crise économique globale, puis en crise sociale et géopolitique. Le Forum Économique Mondial documente dans son Global Risks Report 2024 comment les risques technologiques, climatiques et géopolitiques s'entremêlent selon des boucles de rétroaction complexes [79].

2. La synchronisation ou concentration temporelle : les cycles de crise, autrefois décalés, se synchronisent et s'accélèrent. Changement climatique, tensions géopolitiques, disruptions technologiques, instabilités sociales – ces phénomènes qui évoluaient sur des temporalités différentes convergent désormais. Le GIEC note que la fenêtre d'action climatique (2020-2030) coïncide avec la transformation numérique accélérée et la reconfiguration géopolitique post-COVID [80]. Cette accélération réduit notre capacité d'adaptation : les crises se succèdent à un rythme qui dépasse notre capacité de résilience traditionnelle.

3. L'amplification non-linéaire : dans un système complexe sous tension, de petites perturbations peuvent déclencher des cascades catastrophiques. La théorie des systèmes complexes montre que les systèmes proches de points de bascule (tipping points) deviennent hypersensibles [81]. C'est la nature même du risque systémique : un choc qui, au lieu d'être confiné à une partie du système, est capable d'affecter son intégralité, menant à des « crises enchevêtrées » (entangled crises) aux conséquences imprévisibles [82]. Comme le souligne Nassim Taleb avec son concept de « cygnes noirs », ces événements aux conséquences disproportionnées deviennent paradoxalement plus probables dans un monde hyper-connecté [83]. Un cargo bloqué dans le canal de Suez en est une illustration, ayant perturbé 12 % du commerce mondial [84].

H.2 Vulnérabilités spécifiques du monde numérique

Cette dynamique de polycrise est particulièrement critique pour le monde numérique. L'OCDE définit la fragilité comme la combinaison d'une exposition aux risques et d'une résilience insuffisante pour les absorber [45]. Le secteur numérique illustre parfaitement cette définition à travers plusieurs dimensions de fragilité :

- Concentration oligopolistique extrême : cinq entreprises (Amazon, Microsoft, Google, Alibaba, IBM) contrôlent 77 % du marché mondial du cloud selon Synergy Research [85]. Cette concentration transforme chaque acteur majeur en point de défaillance unique (SPOF - Single Point of Failure). Quand AWS (Amazon Web Services) connaît une panne majeure, comme en décembre 2021, c'est Netflix, Disney+, Uber, et des milliers d'autres services qui s'arrêtent simultanément, affectant des centaines de millions d'utilisateurs [86].

- Dépendance géopolitique asymétrique :

  - 92 % du marché des semiconducteurs avancés (< 7nm) est concentré entre Taïwan (TSMC) et la Corée du Sud (Samsung) [87]. Les tensions croissantes autour de Taïwan ne menacent pas seulement la paix régionale mais l'approvisionnement technologique mondial. Le « Taïwan Semiconductor Manufacturing Company » produit les puces pour Apple, NVIDIA, AMD ; son arrêt paralyserait la production et l'innovation technologique mondialement. La première sortie officielle du dernier né de la flotte militaire chinoise, le Fujian, porte-avions nucléaire, s'est faite au large de Taïwan en mai 2024 – tout un symbole de cette vulnérabilité géostratégique.

  - 83 % du marché européen du cloud-logiciel est contrôlé par des acteurs américains (AWS, Microsoft Azure, Google Cloud), représentant 260 milliards d'euros de valeur créée aux États-Unis [88]. Cette dépendance asymétrique transforme le cloud en levier géopolitique. Ainsi, en mai 2025, Microsoft a suspendu le compte email de Karim Khan, procureur de la Cour Pénale Internationale de La Haye, suite aux sanctions imposées par l'administration Trump contre la CPI. Cette coupure – qui a également touché le juge français Nicolas Guillou – a contraint l'institution judiciaire internationale à migrer vers Proton Mail [89], symbolisant cette vulnérabilité stratégique européenne face au pouvoir de contrainte numérique américain.

- Vulnérabilité des infrastructures physiques : 99 % du trafic internet intercontinental transite par seulement 485 câbles sous-marins [90]. Ces câbles, souvent vieux de plusieurs décennies, sont vulnérables aux ancres de navires (30 % des coupures), aux séismes (15 %), et désormais aux sabotages délibérés. Les coupures mystérieuses de câbles en mer Baltique en 2022 et 2023 révèlent cette nouvelle dimension de vulnérabilité géopolitique de notre infrastructure numérique [91].

- Complexité incontrôlable : la dette technique mondiale – l'accumulation de code obsolète, de systèmes incompatibles et de correctifs temporaires devenus permanents – est estimée par le Consortium for Information & Software Quality (CISQ) à 1 520 milliards de dollars pour l'année 2022 uniquement [92]. Cette fragilité structurelle croissante rend nos systèmes de plus en plus vulnérables aux défaillances en cascade, comme l'illustre parfaitement l'incident Spruce Pine décrit dans l'encart correspondant.

H.3 De la polycrise aux polysolutions : vers une gouvernance systémique

Face à ce diagnostic, la tentation de l'inaction est grande. Elle est alimentée non seulement par des biais cognitifs individuels comme la préférence pour le court terme (hyperbolic discounting) [47], mais aussi par des barrières à l'action collective systémiques, telles que la défense d'intérêts particuliers ou le manque de volonté politique. La logique économique dominante, privilégiant l'efficacité immédiate sur la résilience à long terme, nous enferme dans la construction de systèmes optimisés mais fragiles.

Cependant, des cadres d'action émergent pour dépasser ces blocages. Le réseau académique PolyCIVIS, soutenu par l'UE, a théorisé le concept de « polysolutions », qui vise à construire des « approches intégrées et multifacettes qui s'attaquent aux causes profondes des crises interconnectées » [47]. Cette vision trouve un écho dans le domaine du leadership, où des institutions comme le Center for Creative Leadership (CCL) appellent à développer des stratégies à fort effet de levier (high-leverage strategies) capables de surmonter simultanément les barrières structurelles et mentales [93].

Qu'on les nomme "polysolutions" ou "stratégies à fort effet de levier", l'objectif est le même : passer d'une logique de réparation réactive à une gouvernance proactive et systémique. Appliquée à la résilience numérique, une telle approche se fonde sur la coopération interdisciplinaire, une gouvernance adaptative, et la prospective stratégique. Concrètement, cela signifie agir de manière coordonnée sur plusieurs leviers : la décentralisation des infrastructures et la redondance pour éliminer les points de défaillance uniques ; la simplification volontaire pour maîtriser la complexité et réduire la dette technique ; le développement d'une indépendance numérique pour mitiger les dépendances géopolitiques ; et enfin, une anticipation systémique basée sur la modélisation des risques en cascade et des tests de résistance rigoureux.

Adopter une telle stratégie est un changement de paradigme fondamental. Il s'agit de reconnaître que dans un monde en polycrise, la résilience n'est pas un coût, mais l'investissement le plus stratégique pour assurer la pérennité de nos organisations et de nos sociétés.

[45] OCDE. *États de fragilité 2025*. OCDE, organisation internationale de 38 pays membres. Rapport analysant la fragilité dans 61 pays via un cadre multidimensionnel de 56 indicateurs couvrant 6 dimensions (politique, sociétale, sécuritaire, environnementale, économique, humaine). 25 ans d'expertise sur la fragilité. 2025. URL : https://www.oecd.org/content/dam/oecd/fr/publications/reports/2025/02/states-of-fragility-2025_c9080496/3797ea0f-fr.pdf.

[72] Edgar MORIN et Anne Brigitte KERN. *Homeland Earth : A Manifesto for the New Millennium*. Hampton Press, 1999. URL : https://archive.org/details/homelandearthman0000mori.

[73] Adam TOOZE. *This is why 'polycrisis' is a useful way of looking at the world right now*. World Economic Forum, 2023. URL : https://www.weforum.org/stories/2023/03/polycrisis-adam-tooze-historian-explains/.

[74] Jean-Claude JUNCKER. *Speech by President Jean-Claude Juncker at the Annual General Meeting of the Hellenic Federation of Enterprises*. 2016. URL : https://europa.eu/rapid/press-release_SPEECH-16-2293_fr.htm.

[75] CASCADE INSTITUTE. *What Is a Global Polycrisis ?* Rapp. tech. Cascade Institute, 2022. URL : https://cascadeinstitute.org/wp-content/uploads/2022/04/What-is-a-global-polycrisis-v2.pdf.

[76] F. SCHREIBER et al. *From Polycrisis to Polysolutions : An Interdisciplinary Approach to Complex Global Challenges*. Foundational Brief. PolyCIVIS, mars 2025. URL : https://civis.eu/storage/files/1foundational-brief-polycrisis-and-policy-series-formatted-version2-schreiber-etal-mar-2025.pdf.

[77] Jürgen SCHEFFRAN. "Systemic Risks and Governance of the Global Polycrisis in the Anthropocene". In : *Global Sustainability* (2023). URL : https://www.cambridge.org/core/journals/global-sustainability/article/systemic-risks-and-governance-of-the-global-polycrisis-in-the-anthropocene-stability-of-the-climateconflictmigrationpandemic-nexus/95EF7C378D08AD2806659BBACFABBAF5.

[78] Thomas HOMER-DIXON et al. "Global polycrisis : the causal mechanisms of crisis entanglement". In : *Global Sustainability* (2023). URL : https://www.cambridge.org/core/journals/global-sustainability/article/global-polycrisis-the-causal-mechanisms-of-crisis-entanglement/06F0F8F3B993A221971151E3CB054B5E.

[79] WORLD ECONOMIC FORUM. *Global Risks Report 2024*. Rapp. tech. World Economic Forum, 2024. URL : https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

[80] IPCC. *Climate Change 2023 : Synthesis Report – Sixth Assessment Report*. Rapp. tech. Intergovernmental Panel on Climate Change, 2023. URL : https://www.ipcc.ch/report/ar6/syr/.

[81] SANTA FE INSTITUTE. *Complex Systems and Tipping Points*. 2023. URL : https://www.santafe.edu/events/critical-transitions-in-complex-systems-are-t.

[82] A. GAMBHIR et al. "A Systemic Risk Assessment Methodological Framework for the Global Polycrisis". In : *Nature Communications* (2024). URL : https://www.nature.com/articles/s41467-025-62029-w.

[83] Nassim Nicholas TALEB. *The Black Swan : The Impact of the Highly Improbable*. Ouvrage de référence sur les événements rares et imprévisibles aux conséquences catastrophiques (cygnes noirs). Random House, 2007.

[84] LLOYD'S LIST. *Ever Given : Suez Canal blockage economic impact*. 2021. URL : https://www.lloydslist.com/LL1137492/The-lessons-and-the-aftermath-of-the-Ever-Given-incident.

[85] SYNERGY RESEARCH GROUP. *Cloud Market Share Q2 2024*. Rapp. tech. Synergy Research Group, 2024. URL : https://www.srgresearch.com/articles/cloud-market-growth-stays-strong-in-q2-while-amazon-google-and-oracle-nudge-higher.

[86] AWS. *Post-Incident Analysis December 2021*. Rapp. tech. Amazon Web Services, 2021. URL : https://aws.amazon.com/premiumsupport/technology/pes/.

[87] SIA. *Global Semiconductor Industry Report*. Rapp. tech. Semiconductor Industry Association, 2024. URL : https://www.semiconductors.org/wp-content/uploads/2024/05/SIA-2024-Factbook.pdf.

[88] ASTERèS. *La dépendance technologique aux softwares et services cloud américains : une estimation des conséquences économiques en Europe*. Rapp. tech. ASTERèS, 2025. URL : https://www.cigref.fr/wp/wp-content/uploads/2025/04/Etude-Asteres-La-dependance-technologique-aux-services-de-cloud-et-logiciels-americains-avril-2025.pdf.

[89] Les Échos. *Sous pression géopolitique, la Cour pénale internationale tourne la page Microsoft*. Nov. 2025. URL : https://www.lesechos.fr/tech-medias/hightech/sous-pression-geopolitique-la-cour-penale-internationale-tourne-la-page-microsoft-2199143.

[90] TeleGeography. *Submarine Cable Map*. 2024. URL : https://www.submarinecablemap.com/.

[91] Reuters. *Baltic Sea Cable Cuts : Investigation Reports*. Rapports d'enquête couvrant la période 2023-2025. 2023. URL : https://www.reuters.com/world/europe/estonia-probe-sweden-cable-damage-part-baltic-sea-incident-investigation-2023-10-19/.

[92] CISQ. *The Cost of Poor Software Quality in the US*. Rapp. tech. Consortium for Information et Software Quality, 2024. URL : https://www.it-cisq.org/wp-content/uploads/sites/6/2022/11/CPSQ-Report-Nov-22-2.pdf.

[93] Center for Creative Leadership. *Leading Beyond Barriers : Creating Impact in an Age of Polycrisis*. Rapp. tech. Center for Creative Leadership, 2024. URL : https://cclinnovation.org/wp-content/uploads/2025/02/leadingbeyondbarriers.pdf.

Annexe I

La low-tech, une philosophie de résilience face aux fluctuations

Cette annexe est très largement inspirée par le travail du CIGREF-INR « L'approche low-tech au service de la résilience numérique des organisations » (document en cours de finalisation avant publication), qu'elle synthétise en grande partie. Elle reprend aussi quelques concepts ou exemples du livre blanc pour les positionner dans cette vision low-tech – « Digital Entreprise Mine », Crowstrike… – afin d'en comprendre les apports majeurs que chaque organisation devrait considérer. Elle repositionne aussi des apports possibles de cette démarche low-tech dans les trois zones de notre boussole.

I.1 Qu'est-ce que la démarche low-tech ?

Selon l'ADEME, la démarche low-tech est « une démarche innovante et inventive de conception et d'évolution de produits, de services, de procédés ou de systèmes qui vise à maximiser leur utilité sociale, et dont l'impact environnemental n'excède pas les limites locales et planétaires. »

Loin d'être un retour en arrière, cette philosophie repose sur sept piliers fondamentaux :

Utilité : répondre aux besoins réels, pas aux envies artificielles. Le besoin fait l'objet d'un questionnement systématique visant à formuler des réponses adaptées et proportionnées.

- Un système de caisse capable de basculer sur papier-crayon plutôt qu'une solution 100 % cloud.

Accessibilité : solutions compréhensibles, modifiables, réparables. La simplicité d'usage favorise la transmission des savoirs et le renforcement du lien social.

- Jerry DIT : ordinateurs assemblés collectivement à partir de composants recyclés.

Durabilité : conception pour la longévité et la réparation. Il faut minimiser l'usage de ressources naturelles et réduire les l'empreinte environnementale à chaque étape du cycle de vie.

- Fairphone : 7 ans de support garanti vs 2 ans pour un smartphone classique.

Localité : production et maintenance territoriales. Il est nécessaire de limiter les impacts liés au transport, de renforcer les compétences territoriales et le dynamisme socio-économique.

- Serveurs locaux pour données critiques plutôt que cloud international.

Autonomie : maîtrise des outils par les utilisateurs. La capacité d'appropriation permet d'adapter, de réparer ou d'améliorer les solutions.

- OS durcis et allégés maintenables localement.

Robustesse : maintien du système malgré les fluctuations. C'est la capacité à rester stable et viable face aux perturbations variées. Comme le souligne Olivier Hamant : « La robustesse crée les conditions grâce auxquelles on ne tombe pas. »

- Site du Low-tech Magazine : fonctionne sur solaire, accepte l'intermittence.

Simplicité : réduction de la complexité technologique. La limitation aux fonctionnalités essentielles permet de réduire les points de défaillance.

- Site web du Low-tech Magazine : architecture simplifiée, poids divisé par 5, impact réseau réduit.

I.2 Face à quelles vulnérabilités critiques ?

Le groupe de travail CIGREF-INR a identifié trois scénarios de rupture majeure à horizon 2035-2040, rendant la démarche low-tech non plus souhaitable mais nécessaire :

Rupture des chaînes d'approvisionnement technologique

La concentration extrême de la production (90 % des semi-conducteurs avancés produits à Taïwan, par exemple) et la dépendance aux terres rares créent une fragilité systémique. Exemple vécu : la crise de Spruce Pine (80 à 90 % du quartz ultra-pur mondial) a montré comment une seule mine peut paralyser l'industrie électronique mondiale.

Instabilité économique et financière de toute la chaîne de valeur

L'instabilité croissante des approvisionnements, les interruptions de production induites par des phénomènes climatiques, ainsi que l'augmentation continue des coûts liés à la gestion de crise, fragilisent l'ensemble de la chaîne de valeur des organisations. La valeur générée par les technologies numériques peut s'avérer insuffisante au regard des surcoûts nécessaires à leur maintenance et leur sécurisation.

Rationnement et régulation des usages numériques

L'explosion de la consommation des datacenters (40 % pourraient être limités d'ici 2027 selon Gartner) conduit à des arbitrages : qui aura accès aux services numériques quand l'énergie manquera ?

I.3 La low-tech comme réponse stratégique : le techno-discernement en action

Réduction drastique des points de défaillance

Cas concret : une compagnie ferroviaire a remplacé une solution de traçabilité IoT/5G à 50k€ par wagon par un dispositif low-tech (Raspberry Pi + GPS + LoRa) à 150€, tout aussi efficace et désormais en open source. Les gains et les bénéfices sont remarquables : financiers, écologiques et création d'un commun facile à intégrer.

Plans de Continuité d'Activité « low-tech »

Processus en doublure : maintenir une capacité manuelle pour tout processus numérique vital

Méthode TELED : « Tâches Essentielles Lorsque l'Énergie est Disponible » — adapter l'activité à la variabilité des ressources

Réseaux alternatifs : LoRa sur smartphone, VHF/BLU pour services essentiels

L'entreprise-mine comme application concrète

En considérant votre parc informatique comme une « mine urbaine » :

Réduction significative des besoins en nouveaux équipements

Upcycling industriel : création de nouvelles machines à partir de composants récupérés

Filières locales : compétences de réparation et maintenance sur le territoire

I.4 Comment intégrer la low-tech dans votre trajectoire de robustesse ?

Grille d'action immédiate par zone de criticité

Zone	Action traditionnelle	Alternative low-tech	Gain en robustesse
Rouge	Backup cloud multirégions	Règle 3-2-1(*) avec supports physiques locaux	Indépendance totale en cas de crise
Orange	ERP complexe tout intégré	Modules séparés, interopérables, documentation ouverte	Réparable localement, évolutif
Verte	Visioconférence HD permanente	Audio + documents partagés asynchrones	Division très importante de la bande passante

(*) *1 copie originale + 2 sauvegardes (dont 1 sur bande magnétique exportable)*

Le paradoxe créateur

Une banque a testé son site web en version « low-tech » (sans publicités, popups, fonctions superflues). Résultat : les utilisateurs l'ont trouvé « plus simple et plus rapide », la sécurité était renforcée (moins de surface d'attaque), mais le marketing a refusé de renoncer aux publicités.

I.5 La low-tech n'est pas un plan B, c'est le plan A de la résilience

Dans un monde dans lequel 6 (et depuis peu 7) des 9 limites planétaires sont dépassées, où les chaînes d'approvisionnement peuvent rompre du jour au lendemain (voir CrowdStrike 2024), la low-tech n'est plus une option idéologique, mais une nécessité stratégique.

Elle ne remplace pas le high-tech, mais le complète : pendant que le high-tech optimise la performance en conditions normales, la low-tech garantit la continuité en conditions dégradées. C'est l'essence même de l'antifragilité selon Taleb : non seulement survivre aux chocs, mais s'en trouver renforcé.

Votre premier pas : identifiez UN processus critique de votre organisation. Documentez comment il pourrait fonctionner sans électricité, sans réseau, sans cloud. Vous venez de créer votre première brique low-tech. Dans 10 ans, cette brique pourrait sauver votre activité.

La low-tech est l'assurance-vie de vos systèmes numériques. Ne pas s'y préparer, c'est parier que le monde restera éternellement stable. Un pari perdu d'avance.

Annexe J

La démarche TELED de Neoloco, une démarche opérationnelle.

J.1 Introduction

La méthode TELED de NeoLoco https://neoloco.fr/teled/ est une méthode qui permet aux entreprises ou aux collectivités d'adapter leur organisation à l'accès variable à l'énergie et aux ressources (matières premières, eau, etc.).

La méthode a été mise au point et testée pour la première fois à l'échelle artisanale par NeoLoco en 2019 (utilisation du solaire en boulangerie et torréfaction artisanale), puis traduite en 2022 pour élargir son champ d'application aux outils d'organisation courants.

Dès lors la méthode a suscité l'intérêt d'institutionnels, d'entreprises, et de nombreuses écoles supérieures. En effet les adaptations organisationnelles proposées par la méthode représentent une voie largement inexplorée mais qui semble être une réponse à la nécessité de réduire nos impacts environnementaux dans un monde de plus en plus tendu.

« Il y a un motif d'espoir pour nous Français :
les français sont historiquement très bons dans
l'optimisation sous contrainte et
l'innovation méthodologique.
Or le changement climatique et la diminution des
ressources est un monstrueux problème
d'innovation sous contrainte. »

Jean Marc Jancovici

En effet, l'innovation méthodologique porte ses fruits. Dès les premiers mois du développement de TELED, nous (NeoLoco) nous sommes vite rendu compte que s'adapter à la variabilité énergétique (EnR, risques de pénurie, instabilité des prix) permettait dans le même temps de devenir résilient face à d'autres sources d'instabilité (approvisionnement en matière première par exemple).

Les leviers organisationnels pour s'adapter sont bien souvent les mêmes. TELED qui signifiait au départ « Tâches Énergivores Lorsque l'Énergie est Disponible » devient maintenant « Tâches Essentielles Lorsque l'Essentiel est Disponible ». Car, il s'agit bien de faire de TELED une méthodologie de la robustesse des organisations. Ces idées s'ancrent par ailleurs dans le monde académique.

Enfermez les 100 personnes les plus payées du monde dans un laboratoire pour qu'ils conçoivent la voiture électrique la plus performante du monde. Ils ne feront jamais mieux pour réduire nos impacts environnementaux que la personne qui parvient à supprimer des besoins de transport par des adaptations organisationnelles. Voilà la puissance des organisations.

Les leviers d'adaptation à la variabilité sont partout. Ils sont parfois d'autant plus faciles à identifier qu'ils n'ont jamais été cherchés.

J.2 Diffusion dans différents secteurs de l'économie.

En 2019 est fondée NeoLoco, la première activité de boulangerie et de torréfaction d'Europe à recourir à l'énergie solaire. Arnaud, fondateur de NeoLoco, ingénieur de formation, a réalisé un voyage d'étude sur l'énergie qui lui a enseigné que les enjeux énergétiques peuvent souvent se résoudre en s'intéressant aux enjeux culturels et sociologiques. À la création de NeoLoco, il s'attache donc fortement à questionner les pratiques qui entourent ces deux métiers : la boulangerie et la torréfaction pour concevoir un modèle d'organisation qui lui permette de tirer le meilleur de l'énergie solaire au moment où elle est disponible.

Puis, en 2023, avec Loïc Pérochon, ils traduisent la méthode en langage industriel (à l'aide de VSM Energie, ou VSM ressources) pour l'appliquer au reste de l'économie. Le potentiel est extrêmement grand. Que ce soit à cause de pénurie, d'inflation des prix ou de ressources non pilotables. Les énergies variables sont dès aujourd'hui les énergies qui font l'économie. Il y a urgence à passer d'un monde fondé sur des énergies et des ressources prétendument continues à un monde des énergies variables (et qui facilitera au passage une transition nécessaire). L'objectif du collectif pluridisciplinaire qui développe aujourd'hui la méthodologie TELED est d'offrir un cadre de référence pour penser les organisations autour d'un accès variable aux ressources.

L'enjeu est colossal. Désormais, les énergies renouvelables sont incontournables. De plus, les énergies continues (gaz, fioul, charbon, nucléaire...) doivent être considérées comme variables à cause des risques de pénurie ou de l'inflation des prix qui imposent à certains secteurs de mettre en pause les activités, voire de cesser l'activité (ex. : boulangerie, fonderie, etc.). Il n'y a donc plus d'énergie continue. Ces tensions se ressentent aussi sur d'autres ressources : eau, terres rares, matières premières diverses.

J.3 Une méthode.

Les grands principes de la méthode sont très simples et se résument en 4 étapes :

Lister les tâches nécessaires à la réalisation de la mission de l'organisation étudiée

Identifier les tâches énergivores (ou qui consomme la ressource essentielle)

Prioriser les tâches énergivores les jours d'énergie facile (prioriser les tâches essentielles les jours où les ressources sont disponibles)

Sortir d'une gestion en flux tiré (tendu) de l'organisation pour adopter une gestion d'entreprise par le stock.

Si l'adaptation à la variabilité suscite des objections d'ordre culturel dans un monde dominé par l'hypothèse de la continuité depuis plusieurs décennies, la création de stock constitue la seconde objection d'ordre culturel. En effet, il est courant d'entendre dire : « Le stock c'est de l'argent. » Sous-entendu : constituer des stocks n'est pas sérieux. Or de bons gestionnaires ont un rapport rationnel à l'argent et font des calculs coût-bénéfice.

C'est pourquoi la méthode TELED intègre un outil économique nommé le « point de bascule ». Il s'agit de calculer le ratio des surcoûts liés au stock (trésorerie immobilisée dans le stock, intérêt du financement de la trésorerie par la banque, assurance de stock, surcoût foncier pour l'espace de stockage si nécessaire, ...) divisé par les économies de ressources (calculées en €) offertes par la nouvelle flexibilité d'organisation permettant d'utiliser la ressource lorsqu'elle est disponible ou moins chère.

Il s'avère ainsi que certaines activités peuvent avoir passé ce point de bascule dans l'économie d'aujourd'hui. C'est-à-dire qu'elles sont d'ores et déjà plus rentables avec une organisation de type TELED, adaptée à un accès variable aux ressources plutôt qu'une organisation en flux tendu et dans l'obligation de consommer quelles que soient les contraintes instantanées sur les ressources. Et, pour les organisations qui n'auraient pas encore passé ce point de bascule, il est utile néanmoins de le calculer dès aujourd'hui. Consulter les prévisions d'augmentation des prix de l'énergie ou de matières premières permet de prendre conscience que beaucoup de secteurs économiques auront passé le point de bascule dans les 5, 10 ou 15 ans à venir. Or il est utile pour un bon gestionnaire de savoir dès aujourd'hui quels investissements seront compatibles avec le mode d'organisation le plus viable dans ce futur proche.

La méthode offre ainsi une grille de lecture permettant d'identifier les leviers organisationnels dans tout type de secteur économique afin de rentrer dans le monde de la variabilité. Il apparait ainsi que les ressources variables peuvent alimenter l'économie si nous adoptons les formes d'organisations adaptées.

J.4 TELED dans le numérique.

Internet s'est construit, comme le reste des organisations publiques et privées actuelles, sur l'hypothèse d'un accès continu et illimité aux ressources. Ainsi, l'accès à Internet est synonyme d'accès permanent, 24 h/24 et 7j/7, sans même que nous y pensions. Le fait même de remettre en question cet accès 24 h/24 aux services en ligne peut susciter une objection de principe, tout à fait culturelle : tout simplement parce que nous manquons de représentation sociale de la manière dont le système peut fonctionner autrement.

TELED sert à réduire la hauteur de la marche et nous permet de voir comment intégrer la variabilité de manière fructueuse.

En effet, la grande majorité des sites en ligne pourraient être inaccessibles plusieurs heures par jour sans que cela ne gêne le moins du monde. Prenez la boutique en ligne de NeoLoco qui est à l'image d'une quantité colossale de petits sites internet (https://neoloco.fr). Cette boutique en ligne pourrait être indisponible de 1 heure à 6 heures du matin sans rater la moindre vente. Personne ne se lève jamais la nuit pour acheter ce type de produits. Un hébergeur possède des données macroscopiques, c'est-à-dire que, sans même parcourir le contenu du site, il peut mesurer la répartition des accès en fonction de l'heure et de la saison.

Il serait ainsi possible de regrouper sur les mêmes serveurs des services en ligne aux profils de demande d'accès similaires. Des offres d'hébergement qui assureraient 99,9 % de disponibilité pourraient alors être développées et convenir à la majorité des clients avec une sobriété accrue

de 25 % sur les sites qui sont hors ligne 6 heures par jour. Les services critiques pourraient conserver un hébergement « premium » pour garantir 100 % des connexions et un accès 24 h/24 (voir matrice de la criticité pour identifier ces services).

Il est par ailleurs très facile d'imaginer l'acceptabilité sociale d'un tel changement. Très rapidement, il semble plausible que personne ne trouve choquant que le site internet de la boucherie du quartier, que le chat de la famille, ou que l'accès au site de l'école soient inaccessibles de une à six heures du matin.

Mais, il y a mieux. Lorsqu'on héberge un site, il n'est en réalité pas stocké sur un seul serveur, mais sur deux, trois ou plus : c'est ce qu'on appelle la redondance. Or, il est relativement rare qu'un serveur tombe en panne. Il est donc envisageable de ne maintenir allumé que le serveur principal et de rallumer les redondances uniquement lorsque nécessaire (nous pourrions appeler cela la redondance froide et mutualisée). Aujourd'hui, tous les serveurs sont allumés en permanence !

Pour 95 % (et sans doute plus) des usages, il est très acceptable qu'un service soit interrompu cinq minutes, le temps du redémarrage d'un serveur de sauvegarde, même si cela devait arriver une ou deux fois par an. Il existe donc un levier de sobriété supplémentaire de l'ordre de 66 % (si trois redondances) à 75 % (si quatre redondances) pour les services en ligne non critiques.

Impact sur le cahier des charges des infrastructures du numérique robuste.

Les changements d'organisation ont des impacts sur les infrastructures. Aujourd'hui, les serveurs informatiques reposent sur des cahiers des charges qui intègrent l'injonction sous-jacente de la continuité : les infrastructures doivent être accessibles 24 h/24. Pour rester sur l'exemple des serveurs, ils devront à l'avenir être conçus pour des démarrages et des arrêts plus fréquents.

J.5 TELED pour les autres acteurs de la filière du numérique.

Promouvoir des organisations TELED au sein d'une filière telle que le numérique améliore la robustesse des territoires. Nous avons déjà abordé l'hébergement, mais il est possible d'appliquer l'organisation TELED à l'ensemble des acteurs de la filière (fabricant de matériel, installateurs, fournisseur d'accès, etc.). Les stocks intermédiaires ainsi que les marges de manœuvre mises en œuvre sur les ressources stratégiques permettent d'éviter des situations où l'ensemble d'une filière se voit contraint de se réorganiser en quelques heures. En revanche, elles offrent un délai de plusieurs jours, voire de semaines, pour réajuster les dépendances. Par exemple, les pénuries de puces informatiques qui ont grandement affecté l'industrie automobile récemment ont eu pour conséquence la mise au chômage technique et une forte spéculation.

S'il existe des stocks intermédiaires à tous les échelons, il y a plus de marge de manœuvre pour trouver d'autres solutions que l'arrêt de l'activité, et les tensions favorables aux spéculations se trouvent apaisées.

Ainsi un territoire régional, national, ou des organisations internationales qui faciliteront la compatibilité à la variabilité, avec des organisations de type TELED, auront des réponses opérationnelles à la polycrise.

J.6 TELED pour les clients du numérique

La méthode TELED peut permettre d'adapter les organisations utilisatrices du numérique à palier des fluctuations d'accès programmées ou non du numérique. Ainsi la robustesse du numérique passe aussi par la robustesse de l'environnement économique du secteur du numérique, et la robustesse de ces acteurs vis-à-vis du numérique.

J.7 Le cas Oseja

Cet exemple est excellent pour illustrer comment les leviers de la robustesse (listés dans le reste de ce rapport) permettent de construire un réseau électrique résilient en cas de choc profond dans un monde en polycrise. Mais, c'est aussi un très bon exemple pour illustrer à quel point nous sommes conditionnés culturellement. En effet, en assurant localement un accès continu à l'électricité dans un contexte de blackout global, la petite commune d'Oseja a démontré qu'il était possible d'assurer la robustesse du réseau électrique grâce à un système technique, local, redondant et diversifié.

Cependant, Oseja, en garantissant cette continuité de l'approvisionnement électrique, illustre que l'organisation des activités humaines n'a pas encore été réévaluée afin de s'adapter à un monde en constante évolution, capable de perdurer même en cas d'interruption de l'accès à cette ressource. Et, c'est normal car la barrière culturelle est certainement la plus difficile à franchir.

En effet, voilà 60 à 70 ans que nous vivons dans un monde dans lequel l'ensemble des organisations publiques et privées reposent sur l'hypothèse d'un accès continu et illimité aux ressources. Que ce soit pour rentrer dans les limites planétaires grâce à des énergies renouvelables et en promouvant une circularité des usages de matière. Que ce soit pour s'adapter à un accès de plus en plus variable aux ressources dites « continues » (exemple de

l'histoire récente : rupture d'approvisionnement en gaz russe, instabilité des prix de l'électricité, du pétrole, des terres rares, de l'eau, etc., risques de blackout, tensions géopolitiques sur les ressources, vulnérabilité des routes commerciales mondialisées dans un monde en tension, confinements liés au COVID-19, etc.), les organisations du monde de demain devront être compatibles avec l'hypothèse d'un accès variable aux ressources. Le numérique n'y échappera pas.

Comment organiser la vie d'un territoire, de ses entreprises, de son administration lorsque le système énergétique n'est plus pensé pour assurer un accès à la ressource 24 h/24 ? Comment fonctionnent des services et des infrastructures numériques qui ne reposent plus sur l'hypothèse d'un accès 24 h/24 à l'énergie, à l'eau, aux matières premières ou d'une disponibilité 24 h/24 au réseau internet ?

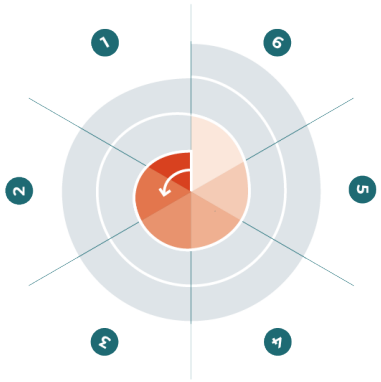
La hauteur de la marche nous semble trop haute pour imaginer ce type de systèmes, car nous n'avons jamais rien vu de tel. Mais, en réalité, ce n'est pas à la limite des possibilités pratiques auxquelles nous sommes confrontés, mais à la limite de notre imaginaire : l'hypothèse de la variabilité ne correspond pas aux fondements de la culture bâtie durant une parenthèse historique exceptionnelle où nous avons pu avoir l'illusion de la continuité pendant quelques décennies.

Mais, le numérique est né lors de ces décennies. Alors comment faire naître de nouvelles pratiques et de nouvelles représentations qui constitueront une nouvelle culture, plus robuste, qui pourra nous paraître tout aussi naturelle que celle d'aujourd'hui dans un avenir plus ou moins lointain.

La méthode TELED (Tâches Essentielles Lorsque l'Essentiel est Disponible) permet de réduire considérablement la hauteur de la marche et de transformer les organisations pour les rendre compatibles avec l'hypothèse de la variabilité.

Annexe K

Tour 1 détaillé — Guide pratique pour renforcer votre zone rouge



Cette annexe est conçue comme un guide opérationnel pour les personnes qui souhaitent approfondir les concepts du Tour 1 et disposer de méthodes pratiques détaillées pour renforcer la zone rouge.
Vous y trouverez des méthodes pas-à-pas, des grilles d'évaluation, des exemples évalués et des outils concrets pour mettre en œuvre les principes de robustesse organisationnelle. Elle se déroule en trois étapes appelées facettes (si nécessaire relire l'annexe La spirale progressive pour comprendre le positionnement et le contenu des facettes).
Cette annexe suit la même structure que le chapitre Tour 1 — Sécuriser dans le corps du livre blanc, mais avec un niveau de détail opérationnel permettant une mise en œuvre immédiate ; elle s'adresse donc plutôt aux équipes expertes qui accompagnent la direction dans la démarche.

Note terminologique

Dans cette annexe, nous utilisons deux concepts complémentaires définis dans le chapitre Poser les bonnes fondations du corps du livre blanc :

- Résilience du numérique : la capacité d'un système numérique à résister aux perturbations et à revenir à un état fonctionnel après l'incident. C'est une propriété technique, réactive et limitée.
- Robustesse de l'organisation : la capacité d'une organisation à maintenir ses fonctions essentielles face aux défaillances du numérique, en créant les conditions pour ne pas tomber. C'est une propriété organisationnelle, préventive et stratégique.

et deux principes définis dans le chapitre Les principes fondamentaux :

- La non-régression pour préserver l'autonomie fondamentale
- La résilience organisée lorsque la non-régression n'est pas possible ou insuffisante

Note importante

Cette annexe propose des méthodes, des grilles d'évaluation et des exemples qui ont fait leurs preuves. Toutefois, ils ne constituent qu'un guide indicatif. Chaque organisation est unique et doit adapter ces outils à son contexte, sa taille, son secteur et sa culture. L'objectif est de l'appropriation des outils proposés : modifiez les grilles, ajustez les méthodes et créez vos propres exemples. L'important n'est pas de suivre ce guide à la lettre, mais d'appréhender la démarche et de progresser dans la construction de votre robustesse organisationnelle.

Par la suite, tous les mécanismes de fragilisation ou les scénarios proposés sont issus de l'annexe dédiée Mécanismes et scénarios et les inspirations de l'annexe Exemples inspirants.

K.1 Comment utiliser cette annexe ?

Pour vous aider dans la démarche, l'approche se structure en trois temps : situez-vous, définissez votre trajectoire, et lancez-vous.

Situez-vous : quel est votre profil de maturité ?

Identifiez le profil qui correspond le mieux à votre organisation aujourd'hui. Cela vous aidera à choisir les actions les plus pertinentes.

Profil	Caractéristiques	Actions prioritaires
Débutant	– Cartographie des dépendances inexistante ou fortement incomplète. – Quasiment aucun 🕮 Point de défaillance unique (Single Point of Failure / SPOF) identifié. – Pas de processus de secours documentés.	– Cartographier les interdépendances. – Identifier chaque 🕮 Point de défaillance unique (Single Point of Failure / SPOF). – Documenter un processus de secours (ou plusieurs selon le contexte).
Intermédiaire	– Cartographie partielle de la zone rouge. – Quelques redondances mises en place. – Processus de secours documentés mais peu testés.	– Éliminer chaque 🕮 Point de défaillance unique (Single Point of Failure / SPOF) critique. – Tester les processus de secours. – Mesurer le taux d'autonomie.
Avancé	– Cartographie complète et maintenue à jour. – Architecture hybride en place. – Tests réguliers de bascule.	– Optimiser le temps de bascule. – Développer une architecture de sobriété. – Augmenter la durée d'autonomie.

Définissez votre trajectoire : le chemin critique en 5 étapes

Quelle que soit votre maturité, la construction de la robustesse suit une logique universelle. Ne vous dispersez pas et suivez ce chemin critique. Selon votre niveau, certaines actions de ce chemin critique ont déjà été réalisées. C'est donc le moment de s'assurer que chaque action a bien été menée et apporte le résultat attendu.

Cartographier (Facette 1) : vous ne pouvez pas protéger ce que vous ne comprenez pas. La cartographie des dépendances est le point de départ requis.

Identifier chaque 🕮 Point de défaillance unique (Single Point of Failure / SPOF) (Facette 1) : une fois la carte établie, ils apparaissent naturellement. C'est votre première cible.

Développer les alternatives (Facette 2) : pour chaque point de défaillance unique, vous devez construire une alternative (processus manuel, solution de secours). C'est le cœur de la non-régression.

Tester et mesurer (Facette 1 & 2) : une alternative non testée n'existe pas. Les exercices de bascule et la mesure de métriques valident votre progression.

Simplifier (Facette 3) : une fois la sécurité de base assurée, vous pouvez vous attaquer à la complexité pour rendre votre robustesse durable.

Lancez-vous : les quick wins dans les premières semaines

Pour créer une dynamique et obtenir des résultats rapides, voici une proposition de cinq actions à lancer dès maintenant (à adapter pour la temporalité et le contenu en fonction du contexte).

1. Semaine 1 : listez les cinq services les plus critiques (un atelier de deux heures).
2. Semaine 2 : pour chaque service, identifiez un 🕮 Point de défaillance unique (Single Point of Failure / SPOF) évident (un atelier de deux heures).
3. Semaine 3 : exportez vos données clients hors de votre CRM et stockez-les hors ligne (un jour).
4. Semaine 4 : testez la bascule sur un service non critique (un jour).
5. Semaine 5 : documentez un processus de secours papier pour une opération critique (deux jours).

K.2 Facette 1 : Contre la contagion, la résilience organisée

Cette première facette explore comment l'interconnexion des systèmes crée une fragilité par contagion et comment la résilience organisée du numérique permet de construire la robustesse de l'organisation.

Exercice de pensée : l'interruption de 24 heures

L'exercice consiste à identifier les 5 à 10 services numériques dont l'arrêt pendant 24 heures paralyserait votre activité principale. L'objectif est non seulement de les lister, mais aussi de quantifier leur criticité pour prendre conscience de l'ampleur du risque. Vous pouvez prolonger l'exercice par une interruption plus longue pour identifier les points de rupture.

Méthode détaillée (durée suggérée : 2 heures)

Cette méthode est proposée à titre indicatif. Adapter la durée, les participants et les étapes selon vos contraintes et votre culture organisationnelle.

1. Participants : réunissez le CODIR, les directeurs métiers, le DSI et les responsables d'applications critiques.

2. Point de départ (30 min) : partez de votre processus métier principal (ex. : la production, la facturation, la livraison). Demandez : « Quel est le processus qui, s'il s'arrête, met en péril l'entreprise à très court terme ? »

3. Remontée de la chaîne (45 min) : pour ce processus, listez tous les systèmes numériques qui le supportent (ERP, CRM, SCADA, etc.). Utilisez un tableau blanc pour visualiser les dépendances.

4. Quantification de l'impact (45 min) : pour chaque système, estimez l'impact réel d'une panne de 24 h. Soyez honnêtes avec vous-mêmes. Pensez à l'impact sur votre métier, mais aussi sur celui de vos clients et de vos fournisseurs.

Modèle : grille d'évaluation de la criticité

Ce modèle est un exemple à adapter en ajoutant vos propres critères (impact réputationnel, réglementaire, etc.) :

- Service critique.
- Processus métier bloqué.
- Impact financier (€/24 h).
- Clients affectés (nombre).
- Temps avant rupture de l'activité.
- …

Mécanisme de fragilisation : Mécanismes de contagion et ambiguïté des interdépendances

Cette section ne détaille pas le mécanisme (voir l'annexe dédiée pour cela), mais aide à l'utiliser pour évaluer le risque.

Le problème n'est plus la panne d'un service, mais la contagion à tout l'écosystème à travers des dépendances invisibles.

Comment utiliser ce mécanisme pour évaluer le risque ?

Le mécanisme de contagion opère sur trois vecteurs à évaluer en matière d'exposition selon trois niveaux : risque faible (poids = 0), risque moyen (poids = 1), risque élevé (poids = 2).

Vecteur	Type de questions	Exposition
Technique	Vos services critiques partagent-ils la même base de données, le même OS, le même cloud ?	
Organisationnel	Vos équipes sont-elles formées pour gérer une crise en cascade ou la panique risque-t-elle de paralyser la décision ?	
Économique	Dépendez-vous d'un seul fournisseur pour plusieurs services critiques ? Connaissez-vous ses propres dépendances ?	

Un score important de 4 (à adapter) indique un risque de contagion systémique élevé et nécessite des actions rapides.

Scénario à envisager : La mégapanne systémique par bug ou cyberattaque

Cette section ne détaille pas le scénario (voir annexe dédiée), mais aide à l'utiliser pour évaluer l'exposition.

L'incident CrowdStrike (juillet 2024) et l'attaque NotPetya (2017) ont montré qu'une cause mineure dans un système hyperconnecté peut entraîner une catastrophe mondiale par contagion.

Votre organisation pourrait-elle subir un CrowdStrike ?

☐ **Absence** de sas de décompression : les mises à jour sont-elles déployées partout simultanément, sans phase de test sur un périmètre limité ?

☐ **Dépendance** à un seul fournisseur : votre sécurité repose-t-elle sur un seul éditeur ?

☐ **Absence** de plan de retour arrière : savez-vous comment désactiver ou désinstaller ce logiciel à distance et massivement en cas de problème ?

☐ **Absence** de plan de continuité manuel : si tous vos postes sont bloqués, comment communiquez-vous ? Comment activez-vous les processus papier ?

Si vous avez coché plus de deux cases ☒, votre organisation est hautement vulnérable à une mégapanne systémique.

Inspiration : Wellington

Face à un risque qui affecte tout le système, l'inspiration vient de Wellington. Construite sur une faille sismique, la capitale de la Nouvelle-Zélande ne cherche pas à empêcher l'effondrement, mais à garantir le fonctionnement de la société malgré le chaos. C'est l'essence même de la résilience organisée.

Wellington applique 4 piliers fondamentaux pour construire sa résilience :

Redondance : ne jamais avoir un Point de défaillance unique (Single Point of Failure / SPOF) pour un service critique.

Diversification : plusieurs technologies, plusieurs fournisseurs, plusieurs sites.

Modularité : chaque service peut fonctionner de manière dégradée, mais autonome.

Tests réguliers : simulation de pannes pour vérifier que les systèmes de secours fonctionnent.

Comment transposer la stratégie de Wellington à votre SI ?

Ce que Wellington a fait	Ce que vous pouvez faire
Redondance : 77 points d'accès communautaires autonomes en eau.	**Architecture hybride :** rapatriez vos services les plus vitaux sur des infrastructures maîtrisées (cloud privé, serveurs locaux) en plus du cloud public.
Diversification : communications par radio et satellite en plus de la fibre.	**Multi-fournisseurs :** ne dépendez pas d'un seul cloud, d'un seul OS, d'un seul opérateur. Il est aussi important de tenir compte des aspects géopolitiques dans la diversification.
Modularité : chaque quartier a un plan d'autonomie de 72 h.	**Isolation des services :** concevez vos services pour qu'ils puissent fonctionner en mode dégradé, sans trop dépendre d'autres services.
Tests réguliers : exercices de simulation de séisme.	**Exercices de bascule :** simulez des pannes trimestrielles et planifiées pour vérifier que vos systèmes de secours fonctionnent et que vos équipes sont prêtes.

Solutions : construire la robustesse de votre organisation

Action 1 : cartographier les interdépendances (Priorité 1)

Délai de mise en œuvre	:	2-4 semaines
Effort estimé	:	3-5 jours x homme
Prérequis	:	aucun
Critères de succès	:	– Cartographie validée par les métiers ET la DSI. – Dépendances jusqu'au niveau physique. – Processus de mise à jour défini.

Action 2 : Éliminer les points de défaillance uniques (Priorité 2)

Délai de mise en œuvre	:	3-6 mois
Effort estimé	:	variable
Prérequis	:	cartographie complète
Critères de succès	:	– Plan de dédoublement pour chaque point de défaillance. – Plus aucun sur les services de la zone rouge.

Action 3 : Adopter une architecture hybride (Priorité 3)

Délai de mise en œuvre	:	6-12 mois
Effort estimé	:	10-20 jours x homme + budget infrastructure
Prérequis	:	points de défaillance traités
Critères de succès	:	– Services les plus vitaux sur infrastructures maîtrisées. – Contrat de réversibilité clair.

Métriques dites Oseja

Le nom d'Oseja pour ces métriques est à prendre comme une typologie. d'indicateurs en relation avec ce livre blanc.

- Métrique Oseja n° 1 — Seuil d'autonomie
  - Définition : le niveau de service minimum acceptable en cas de crise.
  - Comment le mesurer : se définit par des indicateurs métiers qualitatifs.
    Ex : « Pouvoir traiter 50 % des commandes avec un délai de 24 h », « Assurer la sécurité des patients sans accès au dossier informatisé ».

    - Comment l'interpréter : il n'existe pas de seuil universel.
      L'important est de le définir, de le partager et de s'assurer que vos solutions de secours permettent de le tenir, puis de progresser.

- Métrique Oseja n° 2 — Temps de bascule

    - Définition : le temps requis pour activer la solution de secours.

    - Comment le mesurer : chronométrer le temps entre la détection de la panne et le moment où le système de secours est 100 % opérationnel.

    - Comment l'interpréter : l'objectif est de le réduire progressivement. Passer de 8 h à 4 h est déjà une victoire. Viser cinq minutes n'est pas toujours pertinent ni rentable.

ROI (conceptuel) : comment évaluer l'investissement ?

Le ROI de la lutte contre la contagion ne se chiffre pas en euros gagnés, mais en risques évités. Voici une méthode d'évaluation qualitative pour arbitrer vos investissements :

1. Estimez le coût d'une panne de 24 h (ou plus) de votre service le plus critique (chiffre d'affaires perdu, pénalités, coûts de remédiation).

2. Estimez la probabilité d'une telle panne sur cinq ans (faible / moyenne / élevée).

3. Estimez le coût de mise en place des actions de résilience (cartographie, redondance, tests).

4. Comparez : si le (coût de la panne x probabilité) est largement supérieur au coût des actions, l'investissement est justifié.

Cet arbitrage est propre à chaque organisation.

K.3 Facette 2 : Contre le verrouillage, la non-régression

Cette facette explore comment nos choix technologiques passés nous enferment dans des dépendances critiques et comment le principe de non-régression permet de regagner sa liberté pour construire la robustesse de l'organisation.

Exercice de pensée : l'audit de dépendance aux fournisseurs

Pour chaque service de votre zone rouge, menez un audit de dépendance pour évaluer votre niveau de captivité.

Méthode détaillée (durée suggérée : 3 heures)

Cette méthode est proposée à titre indicatif. Adapter la durée, les participants et les étapes selon vos contraintes et votre culture organisationnelle.

1. Participants : DSI, responsable des achats, architectes, responsables applicatifs.
2. Point de départ (30 min) : reprenez la liste des services de la zone rouge.
3. Évaluation (2 h) : pour chaque service, remplissez la grille d'évaluation ci-dessous.
4. Calcul du score (30 min) : calculez le score de verrouillage pour chaque service et identifiez les plus critiques.

Modèle : grille d'évaluation du verrouillage

Ce modèle est un exemple à adapter en ajoutant vos propres critères. L'évaluation se fait avec trois niveaux : risque faible (poids = 0), risque moyen (poids = 1), risque élevé (poids = 2).

Critère	Pondération	Évaluation	Score
Fournisseur unique	3		$P \times \acute{E}$
Coût de migration	2		
Délai de migration	2		
Absence de compétences internes	2		
Format de données propriétaire	1		
Score de verrouillage (/ 10)	$\sum Scores$		

Aide à l'évaluation pour « Fournisseur unique » : 0 = plusieurs alternatives réalistes et testées, 2 = une alternative identifiée mais non testée, 4 = une alternative théorique mais peu réaliste, 5 = aucune alternative connue.

Un score supérieur à 30 indique un verrouillage critique. Ce seuil est indicatif et doit être adapté à votre contexte.

Mécanisme de fragilisation : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)

Cette section ne détaille pas le mécanisme (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre risque.

Le sentiment d'être piégé est le symptôme du verrouillage socio-technique. Pour rappel, les cinq étapes de verrouillage sont :

Adoption : « Cette solution est parfaite pour nos besoins actuels ».

Intégration : « Connectons-la à nos autres systèmes pour plus d'efficacité ».

Dépendance : « Nous ne pouvons plus nous en passer, elle est au cœur de nos processus ».

Atrophie : « Nos équipes ne savent plus faire autrement, les compétences alternatives ont disparu ».

Captivité : « Changer coûterait trop cher, nous sommes prisonniers ».

Évaluez où vous en êtes pour vos services critiques. Si vous êtes à l'étape 4 ou 5 pour un service de la zone rouge, vous êtes en danger ; tout retour arrière devient extrêmement coûteux et risqué.

Scénario à envisager : La rupture géopolitique

Cette section ne détaille pas le scénario (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre exposition.

Le verrouillage devient une menace existentielle face à une rupture géopolitique.

Votre organisation pourrait-elle subir une rupture géopolitique ?

☐ Dépendance à un seul pays : vos fournisseurs de cloud, de logiciels et de matériel sont-ils tous basés dans le même pays ou la même zone géopolitique ?

☐ Absence de clause de réversibilité : vos contrats vous permettent-ils de récupérer vos données facilement et dans un format standard en cas de rupture ?

☐ Dépendance à des composants critiques : vos systèmes dépendent-ils de composants (matériels ou logiciels) dont la production est concentrée dans un seul pays ?

Si vous avez coché plus d'une case ☒, votre exposition au risque géopolitique est élevée.

Inspiration : Les maisons flottantes des Tausug

Pour lutter contre le verrouillage, les Tausug des Philippines nous montrent la voie : en concevant des maisons simples et réparables, ils restent libres et autonomes. Leur principe : concevoir pour la réparation plutôt que pour la perfection. C'est une incarnation du principe de non-régression.

Comment transposer la stratégie des Tausug à votre organisation ?

Ce que les Tausug ont fait	Ce que vous pouvez faire
Concevoir pour la réparation : maisons démontables et remontables facilement.	**Réversibilité technique :** choisir des solutions dont on peut facilement sortir (formats standards, API documentées).
Matériaux simples et disponibles : bambou, feuilles de palmier.	**Technologies** matures et documentées : privilégier des technologies stables et bien comprises plutôt que les dernières nouveautés ; privilégier aussi les technologies les plus simples répondant au besoin.
Savoir-faire partagé : tout le monde sait réparer.	**Compétences** internes : former les équipes aux processus de secours et aux alternatives manuelles.

Solutions : augmenter la robustesse de votre organisation

Action 1 : maintenir et exercer les compétences manuelles (Priorité 1)

Délai de mise en œuvre	:	1-2 mois (pour la première journée)
Effort estimé	:	2-3 jours x homme par trimestre
Prérequis	:	aucun
Critères de succès	:	– Deux « journées Tausug » par an – Fiches de retour d'expérience produites et analysées – Processus de secours améliorés après chaque session.

Action 2 : privilégier les solutions ouvertes et interopérables (Priorité 2)

Délai de mise en œuvre	:	immédiat (pour les nouveaux projets)
Effort estimé	:	1 jour x homme (pour définir la politique)
Prérequis	:	soutien du DSI et des achats
Critères de succès	:	– Politique de réversibilité formalisée. – Grille d'évaluation des fournisseurs mise à jour. – Au moins un projet a choisi une solution open source pour des raisons de réversibilité.

Action 3 : développer une stratégie multi-fournisseurs (Priorité 3)

Délai de mise en œuvre	:	6-18 mois
Effort estimé	:	20-50 jours x homme + budget infrastructure
Prérequis	:	compétences internes sur plusieurs technologies
Critères de succès	:	– Services les plus critiques répartis sur au moins deux fournisseurs. – Procédures de bascule testées.

Métrique Oseja pour la Facette 2

- Métrique Oseja n° 3 — Taux d'autonomie

  - Définition : le pourcentage de vos opérations critiques que vous pouvez maintenir sans services externes.

  - Comment le mesurer :

    1. Listez vos 10 opérations critiques.

    2. Pour chacune, demandez : « Pouvons-nous la maintenir sans accès internet, sans cloud, sans fournisseur externe ? ».

    3. Calculez : (nombre de « oui » / 10) * 100.

  - Comment l'interpréter : il n'existe pas de seuil universel. L'important est de connaître votre niveau actuel et de le faire progresser puis de fixer un objectif de progression (ex. : +10 % par an).

ROI (conceptuel) : comment évaluer l'investissement ?

Le coût du verrouillage n'est pas seulement le prix des licences, comme souvent évoqué. C'est la perte de votre liberté stratégique. Le ROI de la non-régression est l'indépendance. Pour l'évaluer, comparez le coût des actions de déverrouillage (migration, formation) au coût potentiel d'une hausse de 30 % de vos licences ou d'une rupture de service de 48 h. L'arbitrage vous appartient.

K.4 Facette 3 : Contre la complexité, la sobriété intelligente

Cette dernière facette s'attaque à une cause profonde de la fragilité des organisations : la quête d'efficacité qui, paradoxalement, engendre une complexité dangereuse. Nous verrons comment la sobriété intelligente permet de construire la robustesse de l'organisation.

Exercice de pensée : l'audit de complexité

Choisissez le service le plus critique de votre zone rouge et auditez sa complexité.

Méthode détaillée (durée suggérée : 4 heures)

Cette méthode est proposée à titre indicatif. Adapter la durée, les participants et les étapes selon vos contraintes et votre culture organisationnelle.

1. Participants : architectes, développeurs, chefs de projet, utilisateurs clés.
2. Évaluation (3 h) : pour le service choisi, évaluez sa complexité sur quatre dimensions en remplissant la grille ci-dessous.
3. Plan de simplification (1 h) : pour chaque dimension, identifiez 2 à 3 actions de simplification concrètes.

Modèle : grille d'évaluation de la complexité

Ce modèle est un exemple à adapter en ajoutant vos propres critères. L'évaluation se fait avec trois niveaux : risque faible (poids = 0), risque moyen (poids = 1), risque élevé (poids = 2).

Dimension	Questions	Évaluation
Fonctionnelle	Combien de fonctionnalités sont réellement utilisées (< 50 % = 2) ?	
Technique	Combien de systèmes externes y sont connectés (>10 = 2) ?	
Humaine	Combien de personnes comprennent concrètement son fonctionnement (<3 = 2) ?	
Économique	Quel est le coût annuel de maintenance et de licences (>1M€ = 2) ?	
Score de complexité (/ 8))	$\sum \acute{E}valuations$	

Ce modèle est un exemple à adapter en ajoutant vos propres critères et en définissant les seuils de complexité selon le contexte.

Un score supérieur à 4 indique une complexité critique qui doit être adressée. Ce seuil est indicatif et doit être adapté à votre contexte.

Mécanisme de fragilisation : Fragilités techniques et complexité systémique

Cette section ne détaille pas le mécanisme (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre risque.

La complexité exponentielle, ou « dette technique », est souvent le résultat du paradoxe de Jevons – l'amélioration de l'efficacité d'une technologie tend à augmenter sa consommation globale au lieu de la diminuer

Pour l'évaluer :

Auditer la dette technique : demandez aux équipes d'estimer le temps nécessaire pour refactoriser complètement le code des applications critiques. Si le chiffre dépasse 2 ans x homme, votre dette est critique.

Analysez l'évolution de vos coûts : si le coût de maintenance de vos systèmes augmente plus vite que votre chiffre d'affaires, vous êtes dans la spirale du paradoxe de Jevons.

Mesurer la résilience humaine (parfois appelée « Bus Factor » en informatique) : combien de personnes maîtrisent réellement le fonctionnement de votre système ? Si la réponse est 1 ou 2, votre complexité humaine est un risque majeur.

Scénario à envisager : L'effondrement climatique en cascade

Cette section ne détaille pas le scénario (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre exposition.

Une canicule extrême forçant des restrictions d'électricité ou des pannes de climatisation mettra vos datacenters à l'arrêt.

Votre organisation pourrait-elle subir un effondrement en cascade ?

☐ Dépendance à l'électricité : avez-vous mesuré la consommation électrique de vos services critiques ? Savez-vous combien de temps vos onduleurs et groupes électrogènes peuvent tenir ?

☐ Dépendance à la climatisation : vos salles serveurs sont-elles conçues pour résister à une température extérieure de 50°C ?

☐ Absence d'architecture de sobriété : vos applications sont-elles conçues pour être frugales en ressources ?

☐ Absence de plan de délestage : en cas de restriction d'énergie, savez-vous quels services couper en premier ?

Si vous avez coché plus de deux cases ☒, votre organisation est mal préparée à une crise physique.

Inspiration : L'Égypte et les barrières de roseaux

Face à la complexité, l'inspiration vient de solutions frugales. En Égypte, les barrières de roseaux illustrent que les solutions les plus robustes ne sont pas nécessairement les plus sophistiquées. C'est le principe de simplicité stratégique.

Comment transposer la stratégie égyptienne à votre organisation ?

Principe égyptien	Ce que vous pouvez faire
Solution low-tech efficace : barrières de roseaux millénaires.	**Technologies** matures éprouvées : privilégier les solutions simples qui ont fait leurs preuves.
Ressources locales et disponibles : roseaux abondants.	**Ressources** existantes : utiliser et réemployer ce que vous maîtrisez déjà plutôt que d'ajouter de nouvelles technologies.
Maintenance minimale : se régénère naturellement.	**Complexité** réduite : moins de code = moins de bugs, moins de maintenance.

Solutions : viser la sobriété pour construire la robustesse

Action 1 : auditer la valeur par fonctionnalité (Priorité 1)

Pour votre service le plus critique, analysez l'usage réel de chaque fonctionnalité.

Grille de classification des fonctionnalités :

Catégorie	Critères d'usage	Action recommandée
Vitales	Utilisées quotidiennement par plus de 80 % du public cible	Conserver et optimiser
Importantes	Utilisées hebdomadairement par plus de 50 % du public cible	Conserver
Utiles	Utilisées mensuellement par >plus de 20 % du public cible	Évaluer le coût/bénéfice
Superflues	Utilisées annuellement par <moins de 5 % du public cible	Désactiver ou supprimer
Zombies	Jamais utilisées mais consomment des ressources	Supprimer immédiatement

Calcul du « dividende de simplicité » : le dividende de simplicité représente le bénéfice net obtenu en éliminant les fonctionnalités superflues et les applications zombies.

Pour l'évaluer, suivez cette méthode en trois étapes :

1. Étape 1 : identifier les coûts actuels des fonctionnalités inutiles
   - Pour chaque fonctionnalité ou application identifiée comme « zombie » (non utilisée ou sous-utilisée), estimez :
     - Le coût de maintenance annuel (corrections de bugs, mises à jour de sécurité, support technique).
     - Les licences logicielles associées.
     - Le temps de formation des nouveaux utilisateurs (même s'ils ne l'utiliseront jamais).
     - La charge cognitive pour vos équipes (complexité ajoutée au système global).
2. Étape 2 : estimer les gains de la suppression
   - Au-delà des économies directes, la suppression génère des bénéfices indirects :
     - Réduction de la surface d'attaque (moins de vulnérabilités de sécurité potentielles)
     - Amélioration des performances globales du système (moins de ressources consommées)
     - Accélération de l'onboarding de nouveaux collaborateurs (moins à apprendre)
     - Simplification des processus de mise à jour et de migration
3. Étape 3 : calculer le dividende net
   - $Dividende\ de\ simplicité = (Économies\ annuelles + Valeur\ des\ gains\ indirects) - Coût\ de\ décommissionnement$

Délai de mise en œuvre	:	2-3 mois
Effort estimé	:	5-10 jours x homme
Prérequis	:	journaux d'utilisation
Critères de succès	:	– Plan de décommissionnement pour les fonctionnalités non utilisées. – Réduction d'au moins 20 % du nombre de fonctionnalités.

Action 2 : créer des « budgets complexité » (Priorité 2)

Pour chaque nouveau projet, ne vous contentez pas d'un budget financier. Instaurez un « budget complexité ». L'évaluation se fait avec trois niveaux : complexité faible (poids = 0), complexité moyenne (poids = 1), complexité élevée (poids = 2)

Grille d'évaluation de la complexité d'un projet :

Dimension	Poids	Questions	Évaluation
Nouvelles dépendances	25 %	Combien de nouveaux systèmes externes ?	
Nouvelles compétences	25 %	Combien de technologies non maîtrisées ?	
Coût de maintenance	25 %	Quel effort de maintenance supplémentaire ?	
Dette technique	25 %	Quelle complexité ajoutée au code existant ?	
Score général (/ 20)	$\sum \acute{E}valuations$		

Règle de décision : si le score général est > 4, le projet doit être simplifié, voire refusé.

Délai de mise en œuvre	:	1 mois
Effort estimé	:	2 jours x homme
Prérequis	:	soutien de la direction
Critères de succès	:	– Grille d'évaluation de la complexité de projet définie. – Au moins un projet a été simplifié ou refusé sur la base de ce budget.

Action 3 : développer une « architecture de sobriété » (Priorité 3)

Délai de mise en œuvre	:	3-6 mois
Effort estimé	:	15 jours x homme
Prérequis	:	compétences en architecture et actions précédentes réalisées
Critères de succès	:	– Charte d'architecture formalisée. – Technologies de référence définies.

1.1.4.6.4. Métrique Oseja pour la Facette 3

Métrique Oseja n° 4 – Durée d'autonomie

- Définition : le temps pendant lequel vous pouvez maintenir votre seuil d'autonomie sans aucune aide extérieure.
- Comment le mesurer : se mesure en jours ou en semaines. Ex. : « Nous pouvons maintenir la production à 50 % pendant 3 jours sans électricité et sans accès à internet ».
- Comment l'interpréter : c'est votre matelas de sécurité. L'objectif est de l'augmenter pour vous donner le temps de réagir. Passer de 24 h à 72 h est un saut majeur en robustesse.

1.1.4.5. ROI (conceptuel) : comment évaluer l'investissement ?

Le coût de la complexité est insidieux (maintenance, pannes inexplicables). Le ROI de la simplicité est la maîtrise. Pour l'évaluer, comparez le coût de la simplification (refactoring, migration) à l'économie réalisée sur la maintenance et à la réduction du risque de pannes. Une application avec moins de code est moins susceptible de contenir des bugs critiques, nécessite moins de maintenance…

K.5 Conclusion du Tour 1 : vous êtes un peu plus Oseja

Ce premier tour est terminé. Vous disposez désormais de quatre métriques claires pour piloter la robustesse de votre organisation :

- Seuil d'autonomie (métrique Oseja n° 1).
- Temps de bascule (métrique Oseja n° 2).
- Taux d'autonomie (métrique Oseja n° 3).
- Durée d'autonomie (métrique Oseja n° 4).

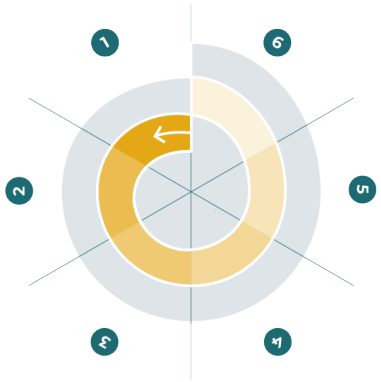
Vous avez également compris la distinction fondamentale entre la résilience du numérique (votre capacité à réparer) et la robustesse de votre organisation (votre capacité à ne pas tomber). D'autres étapes vous attendent, mais vous avez posé les fondations.

K.6 Tableau récapitulatif du Tour 1

Facette	1	2	3
Mécanisme	Mécanismes de contagion et ambiguïté des interdépendances	Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)	Fragilités techniques et complexité systémique
Scénario	La mégapanne systémique par bug ou cyberattaque	La rupture géopolitique	L'effondrement climatique en cascade
Principe	Résilience organisée	Non-régression	Sobriété intelligente
Métriques	n° 1 Seuil n° 2 Temps bascule	n° 3 Taux autonomie	n° 4 Durée autonomie
Actions	Cartographier. Éliminer les SPOF. Créer des architectures hybrides.	Maintenir et renforcer les compétences. Intégrer l'open source. Dépendre de plusieurs fournisseurs.	Lancer des audits valeur. Créer un budget complexité. Privilégier la sobriété.

Annexe L

Tour 2 détaillé — Guide pratique pour optimiser la zone orange



Cette annexe est conçue comme un guide opérationnel pour les personnes qui souhaitent approfondir les concepts du Tour 2 et disposer de méthodes pratiques détaillées pour renforcer la zone rouge.
Vous y trouverez des méthodes pas-à-pas, des grilles d'évaluation, des exemples évalués et des outils concrets pour mettre en œuvre les principes de robustesse organisationnelle. Elle se déroule en trois étapes appelées facettes (si nécessaire relire l'annexe La spirale progressive pour comprendre le positionnement et le contenu des facettes).
Cette annexe suit la même structure que le chapitre Tour 2 — Optimiser dans le corps du livre blanc, mais avec un niveau de détail opérationnel permettant une mise en œuvre immédiate ; elle s'adresse donc plutôt aux équipes expertes qui accompagnent la direction dans la démarche.

Note terminologique

Dans cette annexe, nous utilisons deux concepts complémentaires définis dans le chapitre Poser les bonnes fondations du corps du livre blanc :

- Résilience du numérique : la capacité d'un système numérique à résister aux perturbations et à revenir à un état fonctionnel après l'incident. C'est une propriété technique, réactive et limitée.
- Robustesse de l'organisation : la capacité d'une organisation à maintenir ses fonctions essentielles face aux défaillances du numérique, en créant les conditions pour ne pas tomber. C'est une propriété organisationnelle, préventive et stratégique.

et deux principes définis dans le chapitre Les principes fondamentaux :

- La non-régression pour préserver l'autonomie fondamentale
- La résilience organisée lorsque la non-régression n'est pas possible ou insuffisante

Note importante

Cette annexe propose des méthodes, des grilles d'évaluation et des exemples qui ont fait leurs preuves. Toutefois, ils ne constituent qu'un guide indicatif. Chaque organisation est unique et doit adapter ces outils à son contexte, sa taille, son secteur et sa culture. L'objectif est de l'appropriation des outils proposés : modifiez les grilles, ajustez les méthodes et créez vos propres exemples. L'important n'est pas de suivre ce guide à la lettre, mais d'appréhender la démarche et de progresser dans la construction de votre robustesse organisationnelle.

Par la suite, tous les mécanismes de fragilisation ou les scénarios proposés sont issus de l'annexe dédiée Mécanismes et scénarios et les inspirations de l'annexe Exemples inspirants.

L.1 Comment utiliser cette annexe ?

Pour vous aider dans la démarche, nous vous proposons une approche structurée en trois temps : situez-vous, définissez votre trajectoire, et lancez-vous.

Situez-vous : quel est votre profil de maturité ?

Identifiez le profil qui correspond le mieux à votre organisation aujourd'hui. Cela vous aidera à choisir les actions les plus pertinentes.

Profil	Caractéristiques	Actions prioritaires
Débutant	– Pas d'audit d'utilité des services. – Accumulation de dette technique et d'applications zombies. – Renouvellement matériel systématique tous les 3-5 ans. – Peur de la panne et culture du « zéro défaut ».	– Lancer un audit 3U sur la zone orange. – Identifier les applications zombies. – Inventorier le matériel et estimer sa durée de vie. – Documenter les incidents.
Intermédiaire	– Quelques audits d'utilité menés. – Début de décommissionnement des services inutiles. – Quelques équipements conservés au-delà de leur durée de vie standard. – Incidents documentés mais sans culture d'apprentissage.	– Calculer le dividende de simplicité. – Créer une Digital Enterprise Mine. – Organiser le premier Game Day. – Mettre en place des post-mortems.
Avancé	– Culture de simplicité installée. – Politique de durabilité matérielle formalisée. – Chaos Engineering adapté en place. – Culture d'apprentissage par l'échec.	– Optimiser le MTTR (Mean Time To Recovery). – Développer des solutions low-tech. – Automatiser la résilience. – Partager les apprentissages.

Définissez votre trajectoire : le chemin critique en 5 étapes

Quelle que soit votre maturité, la construction de la performance durable suit une logique universelle. Ne vous dispersez pas et suivez ce chemin critique.

Auditer l'utilité (Facette 4) : vous ne pouvez pas optimiser ce que vous ne comprenez pas. L'audit 3U est le point de départ requis pour identifier ce qui mérite d'être conservé.

Éliminer le superflu (Facette 4) : une fois l'audit établi, les services inutiles apparaissent. C'est votre première cible pour libérer des ressources.

Prolonger la durée de vie (Facette 5) : pour le matériel qui reste, vous devez maximiser sa durée de vie pour réduire votre dépendance aux chaînes d'approvisionnement.

Construire l'autonomie matérielle (Facette 5) : créez votre stock stratégique (Digital Enterprise Mine) pour garantir votre capacité à réparer et maintenir.

S'entraîner à la panne (Facette 6) : une fois la base assurée, vous pouvez transformer votre rapport à l'échec en vous entraînant régulièrement.

Lancez-vous : les quick wins dans les premières semaines

Pour créer une dynamique et obtenir des résultats rapides, voici une proposition de quatre actions à lancer dès maintenant (à adapter pour la temporalité et le contenu en fonction du contexte).

1. Semaine 1 : listez dix services de votre zone orange et évaluez-les selon les critères 3U (un atelier de 3 h).

2. Semaine 2 : identifiez trois applications ou fonctionnalités zombies (non utilisées depuis 6 mois) et planifiez leur décommissionnement (un atelier de 2 h).

3. Semaine 3 : réalisez un inventaire complet de votre matériel informatique et estimez la durée de vie restante de chaque équipement (deux jours).

4. Semaine 4 : organisez un premier Game Day sur un service non critique pour tester votre capacité à gérer une panne (une demi-journée).

L.2 L'outillage

Le concept des 3U : fil conducteur du Tour 2

Les 3U [28] permettent d'identifier si un service répond à un réel besoin, s'appréhende simplement et touche bien la cible visée.

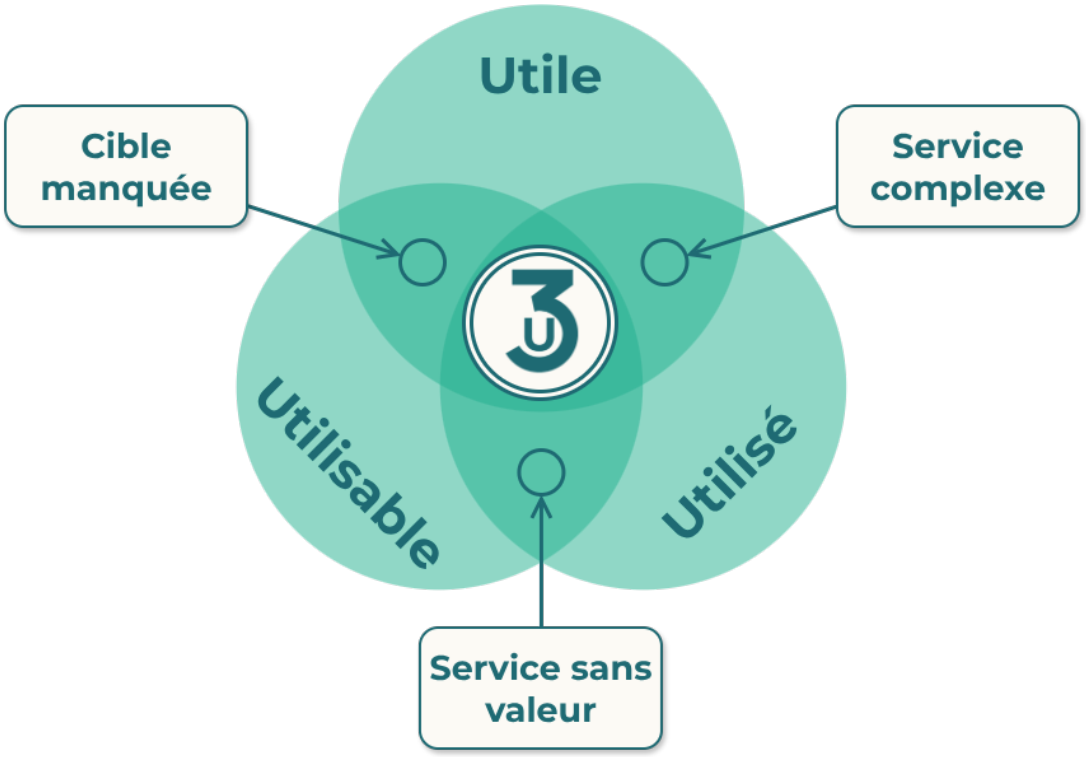


FIG. L.2.1 : Les 3U

Utile : l'utilité peut être associée à la pertinence soit d'un service soit d'une donnée. Il est primordial de s'assurer que cet item est bien un besoin avéré indispensable au service rendu et non une envie ou du confort. C'est le métier, lors de ses expressions de besoin initiales ou lors des phases d'amélioration continue, qui peut décider de l'utilité avec le concours éventuel des retours terrain issus de l'exploitation de la fonctionnalité ou de la donnée.

Utilisable : à partir des spécifications données par le métier, les équipes de développement vont concevoir les services attendus s'appuyant sur les données nécessaires tout en répondant aux exigences liées à l'expérience utilisateur. Si les exigences ne sont pas conciliables, l'item n'est pas utilisable.

Utilisé : à partir des mesures réalisées par les équipes d'exploitation en condition de production sur une durée englobant tous les cycles de vie soit du service soit de la donnée, la comparaison est réalisée par les équipes de développement entre la réalité du terrain et la prévision lors de la déclaration d'utilité. En fonction du résultat le niveau d'utilité de l'item est revu.

Modèle : grille d'évaluation de la pertinence

Ce modèle est un exemple à adapter en ajoutant vos propres critères. L'évaluation des composantes des 3U se fait selon 3 niveaux : faible (poids = 0), moyen (poids = 1), élevé (poids = 2)

- Service.
- Niveau des 3U :
  - Utile, Utilisable, Utilisé.
  - $Score\ 3U = Utile + Utilisable + Utilisé.$
- Coût annuel (k€).
  - $Ratio\ pertinence = {}^{Score}/_{Coût}.$
- Alternative possible.

Interprétation :

- Un score 3U inférieur à 3 indique un service à questionner sérieusement. S'il est inférieur à 5, le service doit être amélioré. S'il est supérieur ou égal à 5, le service est pertinent.
- Un ratio pertinence inférieur à 0,10 suggère un service dont le coût n'est pas justifié par sa valeur.

Les valeurs sont à adapter au contexte.

Le concept des 5R : autre fil conducteur du Tour 2

Le Tour 2 s'appuie sur le concept des 5R [29] , initialement conçu pour l'économie circulaire et adapté ici au numérique. Ce cadre de référence structure les trois facettes de ce tour et vous aide à progresser de manière cohérente.

Les 5R appliqués au numérique :

FIG. L.2.2 : Les 5R

Refuser (Facette 4 - Pertinence) : refuser d'ajouter un nouveau service si le besoin n'est pas explicitement démontré. C'est le premier filtre de la simplicité.

Réduire (Facette 4 - Pertinence) : éliminer les fonctionnalités peu utiles, voire inutiles, simplifier les interfaces. C'est l'audit 3U en action.

Réemployer (Facette 5 - Durabilité) : créer un circuit de réemploi de vos matériels en fonction des besoins cibles. C'est la Digital Enterprise Mine.

Réparer (Facette 5 - Durabilité) : former vos équipes à la réparation, privilégier le matériel réparable. C'est l'autonomie matérielle.

Recycler (Facette 5 - Durabilité) : mettre en place une filière locale de recyclage pour les composants non réutilisables. C'est la circularité complète.

Ce cadre vous permet de structurer votre démarche : commencez par refuser et réduire (Facette 4), puis réemployer, réparer et recycler (Facette 5). La Facette 6 (Antifragilité) vient compléter cette approche en vous préparant à l'inévitable : la panne.

Le concept erooM : un outil complémentaire pour évaluer la pertinence

Le cadre de référence erooM [30, 31] (EROOM Optimization Framework), développé par Boavizta, est un outil d'évaluation complémentaire à l'audit 3U. Il propose une grille d'évaluation détaillée de la pertinence et de l'efficacité des services numériques, en mettant l'accent sur l'impact environnemental et la sobriété.

erooM est l'inverse de Moore : alors que la loi de Moore prédit que la puissance de calcul double tous les 18 mois, la loi d'erooM (Moore à l'envers) observe que les logiciels deviennent de plus en plus lourds, annulant les gains de performance matérielle. Le concept erooM vous aide à inverser cette tendance.

Comment utiliser erooM en complément de l'audit 3U ?

1. Après l'audit 3U : une fois que vous avez identifié les services pertinents (score 3U ≥ 5), utilisez erooM pour évaluer leur efficacité environnementale.

2. Grille d'évaluation erooM : le cadre de référence propose plusieurs dimensions d'évaluation :

   (a) – Efficacité fonctionnelle : le service fait-il ce qu'il doit faire sans fonctionnalités superflues ?

   (b) – Efficacité technique : le code est-il optimisé ? Les ressources sont-elles utilisées efficacement ?

   (c) – Sobriété énergétique : quelle est la consommation énergétique du service ?

   (d) – Durabilité : le service peut-il fonctionner sur du matériel ancien ?

3. Diagnostic rapide erooM : Boavizta propose un outil en ligne gratuit pour réaliser un diagnostic rapide de vos services.

Exemple d'utilisation combinée 3U + erooM :

Service	Score 3U	Verdict 3U	Verdict erooM	Action
Portail client	6	Pertinent	Efficace	Conserver
Intranet	4	À améliorer	Inefficace	Optimiser
CRM	5	Pertinent	Très efficace	Conserver
Application mobile	3	À questionner	Inefficace	Décommissionner

L'audit 3U vous dit quoi garder, le cadre de référence erooM vous dit comment l'optimiser.

L.3 Facette 4 : Contre l'inutilité, la pertinence

Cette première facette explore comment l'accumulation de services inutiles crée une fragilité coûteuse et comment le principe de simplicité permet de construire la pertinence de votre système d'information.

Exercice de pensée : le test de la justification

L'exercice consiste à prendre un service important de votre zone orange et à justifier son existence comme si vous deviez le défendre devant un comité de direction sceptique. L'objectif est de mesurer objectivement la pertinence réelle de ce service.

Méthode détaillée (durée suggérée : 3 heures)

Cette méthode est proposée à titre indicatif. Adapter la durée, les participants et les étapes selon vos contraintes et votre culture organisationnelle.

1. Participants : réunir le CODIR, les directeurs métiers, le DSI et les responsables des services de la zone orange.

2. Sélection des services (30 min) : identifier 5 à 10 services de la zone orange qui existent depuis au moins deux ans. Privilégier ceux dont le coût annuel est significatif.

3. Évaluation 3U (90 min) : pour chaque service, répondre aux trois questions fondamentales :

   - Utile : le service répond-il à un besoin métier réel et stratégique ? Quel est le bénéfice concret et chiffré ?

   - Utilisable : le service est-il simple, intuitif et agréable à utiliser ? Quel est le taux de satisfaction des utilisateurs ?

   - Utilisé : le service est-il réellement adopté ? Combien d'utilisateurs actifs ? Y a-t-il du contournement (shadow IT) ?

4. Identification des alternatives (60 min) : pour chaque service, existe-t-il une solution plus simple ou moins coûteuse qui pourrait rendre 80 % du même service ? Évaluer les solutions low-tech possibles.

Mécanisme de fragilisation : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)

Cette section ne détaille pas le mécanisme (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre risque.

Le problème n'est pas seulement l'accumulation de services inutiles, mais le verrouillage qui nous empêche de nous en défaire. Les choix technologiques passés créent des dépendances qui rendent la migration coûteuse et risquée.

Comment utiliser ce mécanisme pour évaluer votre risque ?

Le mécanisme de verrouillage opère sur trois dimensions. Évaluer l'exposition pour chaque dimension selon 3 niveaux de risque : faible (poids = 0), moyen (poids = 1), élevé (poids = 2) :

Dimension	Questions	Évaluation
Technique	Vos données sont-elles enfermées dans des formats propriétaires ? Pouvez-vous les exporter facilement ?	
Économique	Le coût de migration vers une alternative est-il supérieur à 2 ans de coût d'exploitation du service actuel ?	
Organisationnel	Vos équipes ont-elles développé des compétences spécifiques difficiles à transférer ? Y a-t-il une résistance culturelle au changement ?	
Score de complexité (/ 6)	$\sum \textit{Évaluations}$	

Un score total supérieur à 4 indique un verrouillage fort qui nécessite une stratégie de sortie progressive. Ce seuil est indicatif et doit être adapté à votre contexte.

Scénario à envisager : La crise de confiance généralisée

Cette section ne détaille pas le scénario (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre exposition.

À force de proposer des services qui ne répondent plus aux besoins réels, qui sont trop complexes ou perçus comme intrusifs, les organisations créent une rupture de confiance qui peut se manifester sur deux fronts indépendants mais fortement corrélés :

Crise de confiance externe : vos clients, partenaires et la société se détournent de tout ou partie de vos services numériques, remettant en cause votre « licence sociale d'opérer ».

Crise de confiance interne : vos propres équipes ne croient plus à la pertinence de tout ou partie de vos outils et développent massivement du shadow IT.

Ces deux crises peuvent indépendamment apparaître, mais la présence de l'une est un signal d'alarme fort pour l'autre. Si vous subissez les deux simultanément, la crise est systémique et peut paralyser votre organisation.

Votre organisation pourrait-elle subir une crise de confiance ?

- Crise de confiance externe (clients, partenaires, société) :

  ☐ **Abandon des services** : vos clients abandonnent-ils vos services numériques au profit de concurrents ou de solutions alternatives ?

  ☐ **Méfiance sur les données** : vos clients expriment-ils des inquiétudes sur l'utilisation de leurs données personnelles ?

☐ **Complexité imposée** : vos services numériques sont-ils perçus comme trop complexes ou intrusifs par vos clients ?

☐ **Perte de réputation** : votre organisation est-elle critiquée publiquement pour ses pratiques numériques (surveillance, opacité, etc.) ?

☐ **Désengagement** : observez-vous une baisse du taux d'utilisation de vos services numériques par vos clients ?

☐ **Absence d'écoute** : avez-vous un processus d'écoute des retours clients sur vos services numériques ?

– Crise de confiance interne (équipes, collaborateurs) :

☐ **Services non adoptés** : avez-vous des services officiels dont le taux d'adoption interne est faible par rapport au public ciblé ?

☐ **Shadow IT massif** : vos équipes utilisent-elles massivement des outils non validés (Dropbox, WhatsApp, ChatGPT, Notion, etc.) ?

☐ **Plaintes récurrentes** : recevez-vous régulièrement des plaintes internes sur la complexité ou l'inutilité de vos outils ?

☐ **Contournement systématiqu** e : vos équipes contournent-elles systématiquement les processus officiels ?

☐ **Projets imposés** : vos projets numériques sont-ils décidés sans consultation des équipes finales ?

☐ **Absence de feedback** : avez-vous un processus d'écoute des équipes pour améliorer vos services internes ?

Interprétation :

– 1-2 cases cochées ☒ (dans une seule catégorie) : signal d'alerte précoce, surveillez l'autre front.

– 3+ cases cochées ☒ (dans une seule catégorie) : crise avérée sur un front, l'autre front est probablement déjà touché.

– Cases cochées ☒ dans les deux catégories : crise de confiance systémique, action urgente requise.

Si vous avez coché des cases dans les deux catégories, votre organisation est vulnérable à une crise de confiance généralisée qui peut paralyser à la fois votre transformation numérique et votre relation avec vos clients.

Inspiration : L'Égypte et les barrières de roseaux

Face au piège de la sur-ingénierie, l'inspiration nous vient d'Égypte. Pour lutter contre l'érosion côtière du delta du Nil, au lieu de construire des digues en béton coûteuses et complexes, les communautés locales ont réutilisé une technique millénaire : des barrières de roseaux plantées le long de la côte. Cette solution, d'un coût dérisoire et utilisant des matériaux locaux, s'est avérée plus efficace et durable que les solutions technologiques modernes.

Les barrières de roseaux appliquent 4 piliers fondamentaux de la low-tech :

Utilité : répondre à un besoin réel avec la solution la plus simple.

Accessibilité : utiliser des matériaux locaux et des compétences maîtrisables.

Durabilité : privilégier des solutions qui durent et se réparent facilement.

Sobriété : minimiser l'impact environnemental et les coûts.

Comment transposer la philosophie low-tech (voir chapitre La low-tech) à votre SI ?

Ce que l'Égypte a fait	Ce que vous pouvez faire
Utilité : répondre au besoin d'érosion avec la solution la plus simple (roseaux vs béton).	**Audit** 3U : avant tout projet, vérifiez que le besoin est réel et que la solution proposée est la plus simple possible.
Accessibilité : utiliser des matériaux locaux (roseaux du Nil) et des savoirs traditionnels.	**Solutions** ouvertes : privilégiez les logiciels open source et les formats standards qui peuvent être maintenus en interne.
Durabilité : les roseaux se régénèrent naturellement et ne nécessitent pas de maintenance lourde.	**Architecture** simple : concevez des systèmes modulaires et documentés qui peuvent être maintenus sur le long terme.
Sobriété : coût dérisoire et impact environnemental minimal.	**Frugalité** numérique : éliminez les fonctionnalités superflues, optimisez les ressources, réduisez la consommation énergétique.

Solutions : améliorer votre score de pertinence

Action 1 : mener un audit 3U (Utile, Utilisable, Utilisé) (Priorité 1)

Objectif *: évaluer systématiquement tous les services de la zone orange selon les trois critères de pertinence.*

Méthode à adapter selon le contexte :

1. Créer un comité d'évaluation mixte (métiers + IT).
2. Lister tous les services de la zone orange (applications, plateformes, outils).
3. Pour chaque service, collecter les données d'utilisation (logs, enquêtes utilisateurs).
4. Évaluer selon la grille 3U (voir modèle ci-dessus).
5. Classer les services en 3 catégories :
   (a) – Conserver (score ≥ 5) : services pertinents à maintenir.
   (b) – Améliorer (score 3-4) : services à simplifier ou optimiser.
   (c) – Décommissionner (score < 3) : services à arrêter.

Délai de mise en œuvre	:	2-3 mois
Effort estimé	:	5-10 jours x homme
Prérequis	:	journaux d'utilisation, accès aux données de coûts
Critères de succès	:	– 100 % des services de la zone orange évalués. – Plan de décommissionnement pour les services avec un niveau 3U trop faible. – Roadmap d'amélioration pour les services avec un niveau 3U intermédiaire.

Action 2 : calculer le dividende de simplicité (Priorité 2)

Objectif *: Quantifier le bénéfice économique de l'élimination des services inutiles.*

Méthode :

1. Pour chaque service à décommissionner, estimer les coûts actuels (maintenance, licences, formation).
2. Estimer les gains indirects (réduction surface d'attaque, amélioration performance).
3. Évaluer le coût de décommissionnement (migration données, communication, formation).
4. Calculer le dividende net $Coûts\ actuels + Gains\ indirects - Coût\ de\ décommissionnement$ et le délai de retour sur investissement.
5. Prioriser les décommissionnements selon le dividende en pondérant avec le délai.

Délai de mise en œuvre	:	1-2 mois
Effort estimé	:	3-5 jours x homme
Prérequis	:	audit 3U complété
Critères de succès	:	– Dividende calculé pour chaque service à décommissionner. – Business case validé par la direction. – Réduction d'au moins 20 % du nombre de services ou fonctionnalités.

Action 3 : adopter des solutions low-tech (Priorité 3)

Objectif *: Identifier et mettre en place des alternatives simples aux solutions complexes.*

Méthode à adapter selon le contexte :

1. Pour chaque nouveau projet, poser la question : « Quelle est la solution la plus simple ? »
2. Établir une grille de comparaison high-tech vs low-tech (coût, complexité, maintenabilité, impact environnemental).
3. Privilégier systématiquement la solution low-tech si elle répond à 80 % du besoin (adapter le seuil au contexte).
4. Documenter les choix low-tech et partager les retours d'expérience.
5. Créer une bibliothèque de solutions low-tech validées.

Exemples de solutions low-tech :

- Remplacer un portail intranet complexe par des pages HTML statiques. ou sur la base d'un générateur de pages statiques.
- Remplacer un outil de reporting avancé par des exports automatisés dans un tableur.
- Remplacer un système de ticketing sophistiqué par un simple formulaire web + email.

Délai de mise en œuvre	:	6-12 mois (progressif)
Effort estimé	:	10-15 jours x homme + budget projets
Prérequis	:	culture de simplicité installée
Critères de succès	:	– Au moins 3 projets low-tech réalisés. – Bibliothèque de solutions low-tech créée. – Réduction significative de la complexité moyenne des services.

Métriques dites Oseja pour la Facette 4

Le nom d'Oseja pour ces métriques est à prendre comme une typologie d'indicateurs en relation avec ce livre blanc.

- Métrique Oseja nº 8 — Taux de services utiles
  - Définition : le pourcentage de services de la zone orange ayant un score 3U supérieur ou égal à 4.
  - Comment le mesurer : $\frac{Nombre\ de\ services\ avec\ score \geq 4}{Nombre\ total\ de\ services\ de\ la\ zone\ orange}$
  - Comment l'interpréter : un taux inférieur à 70 % indique une accumulation importante de services peu pertinents. L'objectif est de progresser vers 80-90 %.
- Métrique Oseja nº 9 — Dividende de simplicité
  - Définition : l'économie annuelle réalisée grâce au décommissionnement des services inutiles, exprimée en pourcentage du budget IT.
  - Comment le mesurer : $\frac{Économie\ sannuelles\ réalisées}{Budget\ IT\ total}$
  - Comment l'interpréter : un dividende de 5 à 10 % est un bon résultat pour une première vague de simplification. L'objectif est de réinvestir ce dividende dans l'innovation.

ROI (conceptuel) : le dividende de simplicité

Le ROI de la simplicité ne se chiffre pas uniquement en euros économisés, mais en ressources libérées pour l'innovation. Voici la méthode d'évaluation en trois étapes que nous avons développée.

Étape 1 : Identifier les coûts actuels des fonctionnalités inutiles

Pour chaque fonctionnalité ou application identifiée comme "zombie" (non utilisée ou sous-utilisée), estimez :

- Le coût de maintenance annuel (corrections de bugs, mises à jour de sécurité, support technique).
- Les licences logicielles associées.
- Le temps de formation des nouveaux utilisateurs (même s'ils ne l'utiliseront jamais).
- La charge cognitive pour vos équipes (complexité ajoutée au système global).

Étape 2 : Estimer les gains de la suppression

Au-delà des économies directes, la suppression génère des bénéfices indirects :

- Réduction de la surface d'attaque (moins de vulnérabilités de sécurité potentielles).
- Amélioration des performances globales du système (moins de ressources consommées).

- Accélération de l'onboarding des nouveaux collaborateurs (moins à apprendre).
- Simplification des processus de mise à jour et de migration.

Étape 3 : Calculer le dividende net

- Utiliser la métrique Oseja n° 9 définie ci-dessus.

L.4 Facette 5 : Contre l'obsolescence, la durabilité

Cette deuxième facette explore comment notre dépendance aux chaînes d'approvisionnement mondiales crée une fragilité matérielle et comment le principe de durabilité permet de construire l'autonomie matérielle de votre organisation.

Exercice de pensée : le test de la chaîne d'approvisionnement

L'exercice consiste à cartographier votre dépendance matérielle pour un service important de votre zone orange et à évaluer votre vulnérabilité face aux ruptures d'approvisionnement. L'objectif est de prendre conscience de l'infrastructure physique qui sous-tend vos services numériques.

Méthode détaillée (durée suggérée : 4 heures)

Cette méthode est proposée à titre indicatif. Adapter la durée, les participants et les étapes selon vos contraintes et votre culture organisationnelle.

1. Participants : réunir le DSI, le responsable des achats IT, le responsable infrastructure et les gestionnaires de parc.

2. Inventaire matériel (60 min) : lister tous les équipements qui supportent les services de la zone orange (serveurs, postes de travail, équipements réseau, stockage). Pour chaque catégorie, noter :

   - Quantité actuelle.
   - Âge moyen.
   - Durée de vie standard (selon le fabricant).
   - Durée de vie réelle observée.

3. Cartographie des fournisseurs (60 min) : pour chaque type d'équipement, identifier :

   - Les fournisseurs.
   - Les fournisseurs alternatifs possibles.
   - Le pays de fabrication des composants critiques.
   - Le délai de livraison actuel.

4. Évaluation des risques (90 min) : pour chaque dépendance critique, évaluer :

   - Le risque géopolitique (tensions, embargos).
   - Le risque climatique (catastrophes naturelles dans les zones de production).
   - Le risque économique (pénurie de composants, inflation).

5. Inventaire des ressources dormantes (30 min) : lister tous les équipements réformés mais encore fonctionnels que vous possédez. Estimer leur valeur résiduelle.

L'évaluation des risques peut se faire avec les index suivants :

WGI : Worldwide Governance Indicators
https://databank.worldbank.org/source/worldwide-governance-indicators

FSI : Fragile States Index
https://fragilestatesindex.org/excel/

NDGAIN : Notre Dame Global Adaptation Initiative Country Index
https://gain.nd.edu/our-work/country-index/download-data/

Modèle : grille d'évaluation de la dépendance matérielle

Ce modèle est un exemple à adapter en ajoutant vos propres critères (criticité du service, coût de remplacement, etc.) ; par type d'équipement :

- Quantité,
- Âge moyen,
- Fournisseur principal,
- Pays fabrication,
- Délai livraison,
- Risque géopolitique,
- Risque climatique,
- Score risque total.

Légende d'évaluation : risque faible (poids = 0), risque moyen (poids = 1), risque élevé (poids = 2).

Interprétation : Un score de risque total supérieur à 2 indique une dépendance critique qui nécessite une stratégie d'atténuation (diversification fournisseurs, constitution de stock, allongement durée de vie).

Mécanismes de fragilisation : Fragilités géopolitiques et Fragilités physiques/climatiques face à l'incertitude environnementale

Cette section ne détaille pas les mécanismes (voir annexe dédiée), mais vous aide à les utiliser pour évaluer votre propre risque.

L'illusion d'un numérique infini et toujours disponible masque deux mécanismes de fragilisation critiques qui opèrent simultanément :

Fragilités géopolitiques : la fabrication de vos composants est concentrée dans quelques pays (Chine, Taiwan, Corée du Sud). Un conflit ou un embargo peut instantanément couper votre approvisionnement.

Fragilités physiques/climatiques : votre matériel dépend de chaînes logistiques longues et de ressources (énergie, eau, terres rares) qui sont sous pression climatique.

Comment utiliser ces mécanismes pour évaluer votre risque ?

Ces mécanismes opèrent sur trois dimensions. Évaluez votre exposition pour chaque dimension selon 3 niveaux : faible (poids = 0), moyen (poids = 1), élevé (poids = 2) :

Dimension	Questions	Évaluation
Concentration géographique	Vos composants critiques proviennent-ils d'une seule région géographique ? Avez-vous des fournisseurs alternatifs dans d'autres zones ?	
Dépendance aux ressources rares	Vos équipements dépendent-ils de terres rares ou de composants à forte tension d'approvisionnement ?	
Longueur de la chaîne logistique	Combien d'intermédiaires entre le fabricant de composants et vous ? Quel est le délai total de bout en bout ?	
Score de complexité (/ 6)	$\sum \acute{E}valuations$	

Un score total supérieur à 4 indique une vulnérabilité forte face aux ruptures d'approvisionnement. Ce seuil est indicatif et doit être adapté à votre contexte.

Scénario à envisager : La rupture géopolitique

Cette section ne détaille pas le scénario (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre exposition.

L'incident de la mine de Spruce Pine (Caroline du Nord, 2024) a montré comment une source unique de matière première (quartz ultra-pur pour les semi-conducteurs) peut paralyser une industrie mondiale. Pour la zone orange, l'impact peut être plus insidieux : impossibilité de renouveler le parc, dégradation progressive de la performance, accumulation de dette technique.

Votre organisation pourrait-elle subir une rupture d'approvisionnement ?

☐ **Fournisseur unique** : dépendez-vous d'un seul fournisseur pour une catégorie d'équipements critiques ?

☐ **Concentration géographique** : plus de 70 % de vos composants proviennent-ils d'une seule région (ex. : Asie) ?

☐ **Délais longs** : vos délais de livraison actuels sont-ils supérieurs à 3 mois ?

☐ **Absence de stock** : n'avez-vous aucun stock de pièces de rechange ou d'équipements de secours ?

☐ **Renouvellement systématique** : renouvelez-vous automatiquement votre parc tous les 3-5 ans sans évaluer la durée de vie réelle ?

☐ **Absence de réparabilité** : vos équipements sont-ils conçus pour être jetés plutôt que réparés ?

Si vous avez coché plus de trois cases ☒ , votre organisation est hautement vulnérable à une rupture d'approvisionnement qui pourrait dégrader significativement votre zone orange.

Inspiration : Infomaniak, Fairphone et Mine urbaine

Face à la fragilité des chaînes d'approvisionnement mondiales, l'inspiration nous vient d'acteurs qui ont fait de la durabilité une stratégie de résilience.

Infomaniak, hébergeur suisse, prolonge la durée de vie de ses serveurs jusqu'à 15 ans (contre 5-7 ans dans l'industrie) en choisissant du matériel évolutif et réparable, et en optimisant ses logiciels. Fairphone a conçu un smartphone modulaire et réparable qui dure deux fois plus longtemps qu'un smartphone classique.

Ces deux acteurs appliquent 4 piliers fondamentaux de la durabilité numérique :

Conception pour la durée : choisir du matériel évolutif et modulaire

Réparabilité : privilégier les équipements démontables et documentés

Optimisation logicielle : adapter les logiciels au matériel existant plutôt que l'inverse

Économie circulaire : réemployer, réparer, recycler plutôt que jeter

La Digital Enterprise Mine est l'application concrète de ces principes : transformer vos équipements réformés en ressource stratégique plutôt qu'en déchet. C'est l'équivalent numérique de l'Urban Mining (mine urbaine), qui consiste à extraire des matières premières des déchets urbains plutôt que de les extraire du sol. Votre Digital Enterprise Mine transforme vos équipements obsolètes en « mine » de composants et de matériel réutilisable, réduisant ainsi votre dépendance aux chaînes d'approvisionnement mondiales.

Comment transposer cette stratégie à votre organisation ?

Ce que Infomaniak et Fairphone ont fait	Ce que vous pouvez faire
Conception pour la durée : serveurs évolutifs, smartphone modulaire.	**Critères** d'achat : intégrez la durabilité et la réparabilité comme critères d'achat majeurs (au même niveau que le prix et la performance).
Réparabilité : documentation complète, pièces détachées disponibles.	**Compétences** internes : formez vos équipes à la réparation, créez un atelier de réparation interne.
Optimisation logicielle : adapter les OS pour prolonger la vie du matériel.	**Stratégie** logicielle : privilégiez les OS légers (Linux), optimisez vos applications, évitez les mises à jour qui alourdissent.
Économie circulaire : réemploi systématique des composants.	**Digital** Enterprise Mine : créez votre stock stratégique de composants et d'équipements réformés mais fonctionnels.

Solutions : construire votre autonomie matérielle

Action 1 : Allonger la durée de vie du matériel (Priorité 1)

***Objectif** : Passer d'un cycle de renouvellement systématique 3-5 ans à une approche basée sur la durée de vie réelle.*

Méthode :

1. Réaliser un audit technique du parc pour identifier les équipements qui peuvent être conservés
2. Définir des critères objectifs de fin de vie (performance, sécurité, coût de maintenance)
3. Mettre en place une politique de prolongation de vie :
   (a) Postes de travail : 5-7 ans (au lieu de 3-4 ans).
   (b) Serveurs : 8-10 ans (au lieu de 5-7 ans).
   (c) Équipements réseau : 8-12 ans.
4. Optimiser les logiciels pour qu'ils fonctionnent sur du matériel plus ancien (OS légers, applications optimisées)
5. Former les équipes à la maintenance préventive.

Délai de mise en œuvre	:	3-6 mois
Effort estimé	:	10-15 jours x homme
Prérequis	:	inventaire complet du parc
Critères de succès	:	– Politique de durée de vie formalisée. – Augmentation de la durée de vie moyenne. – Réduction des achats de matériel neuf.

Action 2 : Créer votre Digital Enterprise Mine (Priorité 2)

***Objectif** : Transformer vos équipements réformés en ressource stratégique.*

Méthode :

1. Identifier un espace de stockage dédié (local sécurisé, frais si possible).
2. Créer un inventaire des équipements réformés mais fonctionnels :
   (a) * Postes de travail complets
   (b) Composants (RAM, disques durs, cartes réseau, alimentations).
   (c) Serveurs et équipements réseau.
3. Tester et documenter chaque équipement (état, performances, compatibilités).

4. Créer un système de gestion de stock (simple tableur ou outil dédié).
5. Définir une politique de réemploi :
   (a) Priorité 1 : réutilisation interne (postes de test, environnements de développement)
   (b) Priorité 2 : don à des associations (écoles, associations).
   (c) Priorité 3 : vente ou recyclage responsable.
6. Identifier les trois composants qui tombent le plus souvent en panne et constituez un stock de pièces de rechange

Délai de mise en œuvre	:	3-6 mois
Effort estimé	:	15-20 jours x homme + budget stockage
Prérequis	:	espace de stockage, inventaire du parc
Critères de succès	:	– Mine opérationnelle avec un nombre minimal d'équipements selon le contexte. – Système de gestion en place. – Un minimum de réemplois réussis la première année selon le contexte.

Action 3 : Privilégier le matériel réparable (Priorité 3)

Objectif *: Intégrer la réparabilité comme critère d'achat majeur.*

Méthode :

1. Créer une grille d'évaluation de la réparabilité pour les achats :
   (a) Disponibilité de la documentation technique.
   (b) Disponibilité des pièces détachées (durée, prix).
   (c) Facilité de démontage (outils standards, pas de collage).
   (d) Modularité (composants remplaçables indépendamment).
   (e) Support du fabricant (durée, qualité).
2. Intégrer cette grille dans les appels d'offres (pondération 20-30 % de la note finale)
3. Privilégier les fabricants engagés dans la durabilité.
4. Former les équipes techniques à la réparation (ateliers, certifications).
5. Établir des partenariats avec des réparateurs locaux.

Délai de mise en œuvre	:	6-12 mois (progressif)
Effort estimé	:	10-15 jours x homme + budget projets
Prérequis	:	politique d'achat révisée
Critères de succès	:	– Grille de réparabilité intégrée aux appels d'offres. – 100 % des nouveaux achats évalués selon cette grille. – Au moins 2 équipes formées à la réparation selon les types de matériels.

Métriques Oseja pour la Facette 5

- Métrique Oseja nº 10 — Durée de vie moyenne du matériel
  - Définition : la durée de vie réelle moyenne de vos équipements, de l'achat à la réforme.
  - Comment le mesurer : $\frac{Sommedesduresdeviedetouslesquipementsr formssur1an}{Nombred'quipementsr forms}$.
  - Comment l'interpréter : une durée de vie moyenne inférieure à 4 ans pour les postes de travail ou 6 ans pour les serveurs indique un renouvellement trop rapide. L'objectif est de progresser vers 6-7 ans pour les postes et 8-10 ans pour les serveurs.
- Métrique Oseja nº 11 — Taux d'autonomie matérielle
  - Définition : le pourcentage de vos besoins en remplacement/réparation qui peuvent être satisfaits par votre Digital Enterprise Mine.
  - Comment le mesurer : $\frac{Nombredebesoinssatisfaitsparla Mine}{Nombretotaldebesoins}$ sur une période de 12 mois.
  - Comment l'interpréter : un taux de 20 à 30 % est un excellent résultat pour une Mine en phase de démarrage. L'objectif à long terme est d'atteindre 40-50 % pour les composants standards.

ROI (conceptuel) : comment évaluer l'investissement ?

Le ROI de la durabilité ne se chiffre pas uniquement en coûts évités, mais en autonomie gagnée. Voici une méthode d'évaluation qualitative pour arbitrer vos investissements :

1. Estimez le coût d'une rupture d'approvisionnement de 6 mois : impossibilité de renouveler le parc, dégradation de la performance, perte de productivité, coûts de contournement.
2. Estimez la probabilité d'une telle rupture sur cinq ans (faible / moyenne / élevée) en fonction des tensions géopolitiques et climatiques.
3. Estimez le coût de mise en place d'une stratégie de durabilité (formation, stock, changement de fournisseurs, allongement durée de vie).
4. Comparez : si le (coût de la rupture × probabilité) est largement supérieur au coût de la stratégie de durabilité, l'investissement est justifié.

Exemple illustratif :

Une PME de 200 personnes avec un parc de 200 postes et 20 serveurs :

- Coût d'une rupture de 6 mois : 500 K€ (dégradation performance, perte productivité)
- Probabilité sur 5 ans : moyenne (30 %).
- Coût attendu : 150 K€
- Coût d'une stratégie de durabilité : 80 K€ (formation, stock, allongement durée de vie)
- ROI : positif dès la première année.

L.5 Facette 6 : Contre la fragilité, l'antifragilité

Cette troisième facette explore comment notre quête de perfection et notre peur de l'échec créent une fragilité profonde et comment le principe d'antifragilité permet de transformer les pannes en opportunités d'apprentissage et de renforcement.

Exercice de pensée : le scénario de la panne inattendue

L'exercice consiste à simuler mentalement une panne inattendue sur un service de votre zone orange et à évaluer votre capacité réelle à y faire face. L'objectif est de révéler les faiblesses de vos plans de continuité et de mesurer le 📖 *MTTR (Mean Time To Recovery)*.

Méthode détaillée (durée suggérée : 2 heures)

Cette méthode est proposée à titre indicatif. Adapter la durée, les participants et les étapes selon vos contraintes et votre culture organisationnelle.

1. Participants : réunir le DSI, les responsables d'exploitation, les responsables métiers et les équipes de support.
2. Sélection du service (15 min) : choisir un service important de la zone orange (idéalement un service qui n'a jamais été testé en conditions de panne).
3. Simulation mentale (45 min) : imaginer que ce service tombe en panne demain à 10 h. Dérouler le scénario minute par minute :
   (a) T+0 : La panne se produit. Qui la détecte ? Comment ?
   (b) T+5 min : Qui est alerté ? Par quel canal ?
   (c) T+15 min : Qui prend la décision d'action ? Quelle est la procédure ?
   (d) T+30 min : Qui diagnostique la cause ? Quels outils ? Quelle documentation ?
   (e) T+1 h : Comment restaure-t-on le service ? Quelle procédure ? Quels prérequis ?
4. Identification des faiblesses (45 min) : pour chaque étape, identifier :
   (a) chaque 📖 Point de défaillance unique (Single Point of Failure / SPOF) (SPOF humains : une seule personne sait faire).
   (b) Les procédures manquantes ou obsolètes.
   (c) Les outils de diagnostic absents.
   (d) Les dépendances non documentées.
5. Évaluation du MTTR (15 min) : estimer le temps total de récupération réaliste. Comparer avec votre objectif.

Modèle : grille d’évaluation de la préparation à la panne

Ce modèle est un exemple à adapter en ajoutant vos propres critères (impact client, coût de la panne, etc.) :

- Service,
- Détection (min),
- Alerte (min),
- Diagnostic (min),
- Restauration (min),
- MTTR total,
- SPOF humains,
- Procédure documentée,
- Procédure testée.

Interprétation :

- Un MTTR supérieur à l’indisponibilité maximale pour un service de la zone orange suggère un besoin d’amélioration urgent.
- Un ou plusieurs SPOF humains nécessitent une mise en œuvre de formation au contexte.
- Une ou plusieurs documentations non documentées ou non testées doivent entraîner une mise à jour et la création de cas d’usage pour l’entraînement des équipes.

Mécanismes de fragilisation : Fragilités techniques et complexité systémique et Mécanismes de contagion et ambiguïté des interdépendances

Cette section ne détaille pas les mécanismes (voir annexe dédiée), mais vous aide à les utiliser pour évaluer votre propre risque.

La croyance dans la perfection de nos systèmes nous conduit à une fragilité majeure : nous ne nous préparons pas à l'échec. Deux mécanismes se combinent :

Fragilités techniques et complexité systémique : les systèmes sont devenus si complexes que plus personne ne les maîtrise entièrement. Cette complexité crée un nouveau type de risque : la panne imprévisible.

Mécanismes de contagion : une panne locale peut se propager à tout l'écosystème par des dépendances invisibles.

Comment utiliser ces mécanismes pour évaluer votre risque ?

Ces mécanismes opèrent sur trois dimensions. Évaluer l'exposition pour chaque dimension selon 3 niveaux de risque : faible (poids = 0), moyen (poids = 1), élevé (poids = 2) :

Dimension	Questions	Évaluation
Complexité ,	Combien de composants différents (langages, frameworks, bases de données) dans votre SI ? Quelqu'un comprend-il l'ensemble ?	
Interdépendances	Avez-vous cartographié toutes les dépendances entre vos services ? Connaissez-vous les dépendances de vos fournisseurs ?	
Culture de l'échec	Vos équipes ont-elles peur de la panne ? Les incidents sont-ils cachés ou partagés ? Y a-t-il une culture du blâme ?	
Score de complexité (/ 6)	$\sum \acute{E}valuations$	

Un score total supérieur à 4 indique une vulnérabilité forte face aux pannes systémiques. Ce seuil est indicatif et doit être adapté à votre contexte.

Scénario à envisager : La mégapanne systémique par bug ou cyberattaque

Cette section ne détaille pas le scénario (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre exposition.

L'incident CrowdStrike (juillet 2024) a montré comment un simple bug dans un logiciel de sécurité peut provoquer une panne mondiale massive. Un fichier de configuration défectueux a fait planter 8,5 millions de machines Windows, paralysant des aéroports, des hôpitaux, des banques et des entreprises pendant plusieurs jours.

Votre organisation pourrait-elle subir une mégapanne ?

☐ **Déploiement centralisé** : un logiciel critique (sécurité, gestion, monitoring) est-il déployé sur 100 % de vos machines ?

☐ **Absence de phase de test** : les mises à jour sont-elles déployées partout simultanément, sans phase pilote ?

☐ **Dépendance unique** : votre infrastructure repose-t-elle sur un seul fournisseur, un seul OS, un seul cloud ?

☐ **Absence de plan de retour arrière** : savez-vous comment désactiver rapidement un logiciel défectueux sur toutes vos machines ?

☐ **Absence d'entraînement** : avez-vous déjà simulé une panne majeure avec vos équipes ?

] SPOF humains : une seule personne détient-elle les compétences critiques pour gérer une crise ?

Si vous avez coché plus de trois cases ☒, votre organisation est hautement vulnérable à une mégapanne systémique qui pourrait paralyser votre zone orange pendant plusieurs jours.

Inspiration : Chaos Engineering

Face à l'inévitabilité de la panne, l'inspiration nous vient de Netflix, qui a révolutionné la gestion de la résilience avec l'ingénierie du chaos (Chaos Engineering) [103].

Le principe est contre-intuitif : au lieu de chercher à éviter toute panne, Netflix provoque délibérément des pannes en production pour forcer ses systèmes à devenir résilients. L'outil Chaos Monkey parcourt l'infrastructure et éteint aléatoirement des serveurs, en pleine journée, sans prévenir.

Netflix applique 4 piliers fondamentaux de l'antifragilité :

Régularité : les pannes sont provoquées régulièrement (quotidiennement chez Netflix).

Imprévisibilité : les équipes ne savent pas quand ni où la panne va frapper.

Automatisation : les tests de résilience sont automatisés et continus.

Apprentissage : chaque panne est une opportunité d'amélioration.

Comment transposer l'ingénierie du chaos à votre organisation ?

Vous n'avez pas besoin d'être Netflix pour appliquer ces principes. Voici comment adapter l'approche selon votre maturité :

Ce que Netflix a fait	Ce que vous pouvez faire
Chaos Monkey : pannes automatiques quotidiennes en production.	**Game** Days trimestriels : simulez manuellement une panne sur un service non critique, puis progressez vers les services critiques.
Imprévisibilité totale : les équipes ne savent pas quand la panne va frapper.	**Imprévisibilité** partielle : annoncez la date du Game Day, mais pas le service qui tombera en panne, ou inversement.
Production réelle : les tests sont faits sur l'environnement de production.	**Environnement** de test d'abord : commencez sur des environnements de test, puis progressez vers la production hors heures de pointe, pour finir en production pendant les heures d'utilisation maximale.
Automatisation complète : tout est scripté et automatisé.	**Automatisation** progressive : commencez par des tests manuels, puis automatisez les scénarios les plus fréquents.

Solutions : de l'incertitude à l'entraînement

Action 1 : organiser des Game Days (Priorité 1)

***Objectif** : Instaurer une culture de l'entraînement à la panne par des simulations régulières.*

Méthode :

1. Planifier le premier Game Day (demi-journée) :
   (a) Choisir un service parmi les moins importants de la zone orange.
   (b) Réunir les équipes techniques et métiers.
   (c) Annoncer l'objectif : « Nous allons simuler une panne et mesurer notre capacité à réagir afin de progresser tous ensemble. »
2. Déroulez le scénario :
   (a) T+0 : Provoquez la panne (arrêt d'un serveur, coupure réseau, etc.).
   (b) Laisser les équipes réagir naturellement.
   (c) Chronométrer chaque étape (détection, alerte, diagnostic, restauration).
   (d) Observer les comportements, les blocages, les improvisations.

3. Débriefer immédiatement après (1 heure)
   (a) Qu'est-ce qui a bien fonctionné ?
   (b) Qu'est-ce qui a bloqué ?
   (c) Quelles procédures manquent ?
   (d) Quels SPOF humains avons-nous identifiés ?
4. Documenter les apprentissages et définir les actions correctives
5. Planifier le prochain Game Day (3 mois plus tard) sur un service différent

Progression recommandée :

1. Game Day 1 (Q1) : Service non critique, environnement de test.
2. Game Day 2 (Q2) : Service important, environnement de test.
3. Game Day 3 (Q3) : Service non critique, production hors heures.
4. Game Day 4 (Q4) : Service important, production heures creuses.

Délai de mise en œuvre	:	1 mois pour le Game Day 1
Effort estimé	:	3 jours x homme par Game Day
Prérequis	:	engagement de la direction disponibilité des équipes
Critères de succès	:	– 4 Game Days réalisés la première année. – MTTR réduit de 30 % (à adapter au contexte). – Documentation des procédures mise à jour. – Aucune résistance des équipes graĉe à un accompagnement bienveillant et une participant active

Action 2 : mettre en place des post-mortems sans reproche (Priorité 2)

Objectif *: Transformer chaque incident en opportunité d'apprentissage collectif.*

Méthode :

1. Instaurer une règle simple : tout incident sur un service de la zone orange donne lieu à un post-mortem
2. Organiser la réunion dans les 48 heures suivant l'incident (tant que les mémoires sont fraîches)
3. Structurer le post-mortem selon ce format :
   (a) Chronologie : que s'est-il passé, minute par minute ?
   (b) Causes profondes : pourquoi est-ce arrivé ? (utilisez la méthode des "5 pourquoi")
   (c) Ce qui a bien fonctionné : quelles procédures, quels réflexes ont été efficaces ?
   (d) Ce qui a bloqué : quels obstacles, quelles lacunes ?
   (e) Actions correctives : que devons-nous changer pour éviter la récurrence ?
4. Règle d'or : aucun reproche, aucun blâme. L'objectif est de comprendre et de progresser.
5. Documenter le post-mortem et le partager largement (équipes techniques, direction, métiers)
6. Suivre les actions correctives et mesurer leur efficacité

Template de post-mortem :

- Date et durée de l'incident.
- Services impactés.
- Impact métier (utilisateurs affectés, perte de CA, etc.).
- Chronologie détaillée.
- Causes profondes (technique, organisationnelle, humaine).
- MTTR (détection, diagnostic, restauration).
- Actions correctives (responsable, délai, priorité).
- Apprentissages clés.

Délai de mise en œuvre	:	1 mois
Effort estimé	:	0,5 jours x homme
Prérequis	:	culture de transparence engagement de la direction
Critères de succès	:	– 100 % des incidents donnent lieu à un post-mortem. – Actions correctives suivies. – Réduction significative des incidents récurrents.

Action 3 : implémenter le Chaos Engineering adapté (Priorité 3)

Objectif *: Automatiser progressivement les tests de résilience pour rendre la panne banale.*

Méthode :

1. Commencer par automatiser les tests de résilience existants :
   (a) – Tests de bascule sur site de secours (mensuel).
   (b) – Tests de restauration de sauvegardes (mensuel).
   (c) – Tests de basculement sur serveur secondaire (hebdomadaire).
2. Introduire des pannes aléatoires contrôlées :
   (a) Identifier un service de la zone orange.
   (b) Créer un script qui arrête aléatoirement ce service.
   (c) Exécuter ce script une fois par semaine ou par mois, à un moment aléatoire.
   (d) Mesurer le temps de détection et de récupération.
3. Progresser vers des scénarios plus complexes :
   (a) – Panne d'un composant d'infrastructure (base de données, serveur web)
   (b) – Saturation de ressources (CPU, mémoire, disque).
   (c) – Latence réseau artificielle.
4. 4. Créez un tableau de bord de résilience :
   (a) – Nombre de pannes provoquées.
   (b) – MTTR moyen.
   (c) – Taux de détection automatique.
   (d) – Nombre d'actions correctives déclenchées.

Outils recommandés (selon votre maturité) :

Débutant : scripts bash/PowerShell simples

Intermédiaire : Chaos Toolkit (open source, simple)

Avancé : Gremlin, Chaos Mesh (pour Kubernetes)

Adaptation pour PME/ETI :

- Ne cherchez pas à automatiser tout de suite.
- Commencez par des pannes manuelles planifiées.
- Automatisez uniquement les scénarios les plus fréquents.
- L'important est la régularité, pas la sophistication.

Délai de mise en œuvre	:	6-12 mois
Effort estimé	:	15-20 jours x homme
Prérequis	:	Game Days réussis, culture d'antifragilité installée
Critères de succès	:	– Au moins 3 scénarios automatisés. – Pannes mensuelles sur services les moins importants. – MTTR réduit de 50 %. – Aucune panne non détectée.

Le concept d'hormèse numérique : se renforcer par petites doses de stress

L'hormèse [33] est un phénomène biologique où une faible dose de stress (toxine, radiation, exercice physique) renforce l'organisme au lieu de l'affaiblir. Ce concept s'applique parfaitement à l'antifragilité numérique : de petites pannes contrôlées renforcent progressivement votre résilience globale.

Comment appliquer l'hormèse numérique ?

Doses faibles et régulières : au lieu d'attendre la mégapanne, provoquez de petites pannes contrôlées régulièrement (Game Days trimestriels, tests hebdomadaires).

Progression graduelle : commencez par des services non critiques, puis progressez vers les services importants. Commencez par des pannes courtes (5 min), puis augmentez la durée.

Apprentissage systématique : chaque petite panne est une opportunité d'apprendre et de renforcer vos procédures, vos compétences et vos systèmes.

Renforcement cumulatif : au fil du temps, votre organisation devient naturellement plus résiliente, car les équipes ont intégré les réflexes de gestion de crise.

L'hormèse numérique transforme la panne d'un événement traumatisant en un exercice banal et maîtrisé. C'est l'essence même de l'antifragilité : se bonifier avec les chocs.

Métriques Oseja pour la Facette 6

- Métrique Oseja n° 7 — MTTR (Mean Time To Recovery)
  - Définition : le temps moyen entre la détection d'une panne et le retour à un fonctionnement normal.
  - Comment le mesurer : (Somme des temps de récupération de tous les incidents) / (Nombre d'incidents) sur une période de 12 mois.
  - Comment l'interpréter : un MTTR supérieur à 2 heures pour un service de la zone orange indique une préparation insuffisante. L'objectif est de progresser vers 30-60 minutes.

ROI (conceptuel) : comment évaluer l'investissement ?

Le ROI de l'antifragilité ne se chiffre pas en coûts évités, mais en temps de récupération réduit. Voici une méthode d'évaluation pour arbitrer vos investissements :

1. Mesurer le MTTR actuel : temps moyen de récupération après une panne (basé sur l'historique des incidents).
2. Estimer le coût d'une heure de panne pour un service de la zone orange (perte de productivité, impact client, coûts de remédiation).
3. Estimer le gain potentiel : en réduisant le MTTR de 50 % grâce aux Game Days et à l'entraînement, quels sont les gains annuels ?
4. Estimer le coût de mise en place d'une culture d'antifragilité (Game Days, formation, outils, temps des équipes).
5. Comparer : si le gain annuel est supérieur au coût, l'investissement est justifié.

Exemple illustratif :

Une ETI de 500 personnes avec 10 services en zone orange :

- MTTR actuel : 4 heures.
- Coût d'une heure de panne : 10 K€
- Nombre de pannes par an : 12.
- Coût total des pannes : 480 K€
- Objectif : réduire le MTTR à 2 heures (gain de 240 K€/an)
- Coût de la démarche : 80 K€ (4 Game Days/an + formation + outils).
- ROI : 200 % la première année.

L.6 Conclusion du Tour 2 : de la construction à la transformation

Ce deuxième tour est terminé. Vous disposez désormais de sept nouvelles métriques pour piloter la performance durable de votre organisation :

- Efficacité de pertinence (métrique Oseja n° 5).
- Taux de circularité (métrique Oseja n° 6).
- MTTR (Mean Time To Recovery) (métrique Oseja n° 7).
- Taux de services utiles (métrique Oseja n° 8).
- Dividende de simplicité (métrique Oseja n° 9).
- Durée de vie moyenne du matériel (métrique Oseja n° 10).
- Taux d'autonomie matérielle (métrique Oseja n° 11).

Vous avez également compris la distinction fondamentale entre l'efficacité (faire plus avec moins) et la performance durable (construire sur des fondations solides : pertinence, durabilité, antifragilité). Vous avez appris à questionner l'utilité de vos services, à prolonger la durée de vie de votre matériel et à transformer votre rapport à l'échec.

Votre zone orange est maintenant plus petite (vous avez éliminé l'inutile), plus autonome (vous avez construit votre Digital Enterprise Mine) et plus résiliente (vous vous entraînez régulièrement à la panne). Vous êtes prêt pour le Tour 3, où nous aborderons la zone verte et la résilience collective.

Vous êtes un peu plus Oseja.

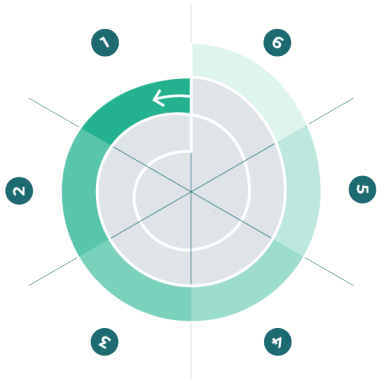
L.7 Tableau récapitulatif du Tour 2

Facette	4	5	6
Mécanisme	Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)	Fragilités géopolitiques Fragilités physiques/climatiques face à l'incertitude environnementale	Fragilités techniques et complexité systémique Mécanismes de contagion et ambiguïté des interdépendances
Scénario	La crise de confiance généralisée	La rupture géopolitique	La mégapanne systémique par bug ou cyberattaque
Principe	Simplicité	Durabilité	Antifragilité
Métriques	n° 5 Efficacité pertinence n° 8 Taux services utiles n° 9 Dividende simplicité	n° 6 Taux circularité n° 10 Durée de vie matériel n° 11 Autonomie matérielle	n° 7 MTTR
Actions	Audit 3U Calculer le dividende Adopter la low-tech	Allonger durée de vie Créer Digital Enterprise Mine Privilégier réparable	Organiser Game Days Post-mortems sans reproche Chaos Engineering adapté

[28] Institute for Sustainable IT. *La règle des 3U*. URL : https://fr.wiki.isit-europe.org/nr/Utile_Utilisable_Utilis%C3%A9.
[29] Race for Water. *La règle des 5R*. 2024. URL : https://www.raceforwater.org/fr/nous-soutenir/eco-gestes/.
[30] Le Web Vert. *La loi d'erooM, de Tristan Nitot*. 2024. URL : https://www.lewebvert.fr/blog/2024-06-20-interview-tristan-nitot/.
[31] Boavizta. *Le diagnostic rapide EROOM*. 2024. URL : https://www.boavizta.org/eroom/diagnostic-rapide.
[33] Centre de l'hormèse. *Qu'est-ce que l'Hormèse ?* 2024. URL : https://www.hormese.com/a-propos/hormese.

Annexe M

Tour 3 détaillé — Parcours d'expérimentation de la zone verte



Cette annexe est conçue comme un guide opérationnel pour les personnes qui souhaitent approfondir les concepts du Tour 3 et disposer de méthodes pratiques détaillées pour renforcer la zone rouge.
Vous y trouverez des méthodes pas-à-pas, des grilles d'évaluation, des exemples évalués et des outils concrets pour mettre en œuvre les principes de robustesse organisationnelle. Elle se déroule en trois étapes appelées facettes (si nécessaire relire l'annexe La spirale progressive pour comprendre le positionnement et le contenu des facettes).
Cette annexe suit la même structure que le chapitre Tour 3 — Expérimenter dans le corps du livre blanc, mais avec un niveau de détail opérationnel permettant une mise en œuvre immédiate ; elle s'adresse donc plutôt aux équipes expertes qui accompagnent la direction dans la démarche.

Note terminologique

Dans cette annexe, nous utilisons deux concepts complémentaires définis dans le chapitre Poser les bonnes fondations du corps du livre blanc :

- Résilience du numérique : la capacité d'un système numérique à résister aux perturbations et à revenir à un état fonctionnel après l'incident. C'est une propriété technique, réactive et limitée.
- Robustesse de l'organisation : la capacité d'une organisation à maintenir ses fonctions essentielles face aux défaillances du numérique, en créant les conditions pour ne pas tomber. C'est une propriété organisationnelle, préventive et stratégique.

et deux principes définis dans le chapitre Les principes fondamentaux :

- La non-régression pour préserver l'autonomie fondamentale
- La résilience organisée lorsque la non-régression n'est pas possible ou insuffisante

Note importante

Cette annexe propose des méthodes, des grilles d'évaluation et des exemples qui ont fait leurs preuves. Toutefois, ils ne constituent qu'un guide indicatif. Chaque organisation est unique et doit adapter ces outils à son contexte, sa taille, son secteur et sa culture. L'objectif est de l'appropriation des outils proposés : modifiez les grilles, ajustez les méthodes et créez vos propres exemples. L'important n'est pas de suivre ce guide à la lettre, mais d'appréhender la démarche et de progresser dans la construction de votre robustesse organisationnelle.

Par la suite, tous les mécanismes de fragilisation ou les scénarios proposés sont issus de l'annexe dédiée Mécanismes et scénarios et les inspirations de l'annexe Exemples inspirants.

Le cadre conceptuel du Tour 3 : de la protection à l'inspiration

Le Tour 3 marque une rupture avec les deux premiers tours. Vous ne cherchez plus à protéger (Tour 1) ni à optimiser (Tour 2), mais à expérimenter et à inspirer par vos choix. Ce tour repose sur trois piliers complémentaires :

La sobriété stratégique (Facette 7) : l'art de l'allocation intelligente des ressources en éliminant le superflu pour renforcer l'essentiel.

La circularité collective (Facette 8) : la transformation des déchets en ressources partagées pour créer une résilience écosystémique.

La vision donut (Facette 9) : la boussole pour prospérer dans un espace juste et sûr, entre un plancher social et un plafond écologique.

Ce cadre vous permet de structurer votre démarche : commencez par libérer des ressources (Facette 7), puis transformez vos déchets en ressources collectives (Facette 8), et enfin adoptez une vision qui guide tous vos choix (Facette 9).

M.1 Comment utiliser cette annexe ?

Pour vous aider dans la démarche, nous vous proposons une approche structurée en trois temps : situez-vous, définissez votre trajectoire, et lancez-vous.

Situez-vous : quel est votre profil de maturité ?

Identifiez le profil qui correspond le mieux à votre organisation aujourd'hui. Cela vous aidera à choisir les actions les plus pertinentes.

Profil	Caractéristiques	Actions prioritaires
Débutant	– Pas d'audit de la zone verte. – Accumulation de services de confort sans justification. – Matériel rendu ou jeté systématiquement. – Pas de vision stratégique au-delà du profit à court terme.	– Lancer un audit du dividende de sobriété. – Identifier les services zombies de la zone verte. – Inventorier les actifs dormants. – Évaluer votre position dans le donut.
Intermédiaire	– Quelques audits menés sur la zone verte. – Début de décommissionnement des services inutiles. – Digital Enterprise Mine mise en place. – Quelques initiatives de responsabilité sociale.	– Calculer le dividende de sobriété total. – Créer une Digital Urban Mine avec 2-3 partenaires. – Adopter des Sunset Policies. – Créer votre Tableau de bord donut.
Avancé	– Culture de sobriété installée. – Digital Urban Mine collective opérationnelle. – Vision donut intégrée dans la stratégie. – Leadership reconnu dans l'écosystème.	– Optimiser le ratio de sobriété (80/20). – Développer la gouvernance de bien commun. – Publier votre Déclaration d'Interdépendance. – Inspirer d'autres organisations.

Définissez votre trajectoire : le chemin critique en 5 étapes

Quelle que soit votre maturité, la construction du leadership par la sobriété suit une logique universelle. Ne vous dispersez pas et suivez ce chemin critique.

Auditer la zone verte (Facette 7) : vous ne pouvez pas arbitrer. ce que vous ne comprenez pas. L'audit du dividende de sobriété est le point de départ requis pour identifier ce qui mérite d'être conservé.

Éliminer le superflu (Facette 7) : une fois l'audit établi, les. services inutiles apparaissent. C'est votre première cible pour libérer des ressources.

Transformer les déchets en ressources (Facette 8) : le matériel. décommissionné devient une mine de composants pour votre écosystème.

Créer un bien commun numérique (Facette 8) : étendez votre Digital. Enterprise Mine en Digital Urban Mine collective avec d'autres organisations.

Adopter la vision donut (Facette 9) : une fois la base assurée, vous pouvez transformer votre rapport à la création de valeur en adoptant une boussole stratégique qui vous guide vers un espace juste et sûr.

Lancez-vous : les quick wins dans les premières semaines

Pour créer une dynamique et obtenir des résultats rapides, voici quatre actions à lancer dès maintenant.

1. Semaine 1 : listez dix services de votre zone verte et calculez leur. dividende de sobriété (un atelier de 3 h).

2. Semaine 2 : identifiez trois services de confort à décommissionner. et planifiez leur arrêt (un atelier de 2 h).

3. Semaine 3 : réalisez un inventaire complet de vos actifs dormants. (matériel mis au rebut dans les 12 derniers mois) et estimez leur valeur en composants réutilisables (deux jours).

4. Semaine 4 : évaluez trois services de votre zone verte selon le modèle du donut (contribution sociale et impact écologique) et visualisez-les sur un graphique (une demi-journée).

M.2 Facette 7 : Contre le gaspillage, la sobriété stratégique

Cette première facette explore comment le gaspillage de ressources dans la zone verte crée une fragilité coûteuse et comment le principe de sobriété stratégique permet de construire un leadership par l'allocation intelligente des ressources.

Exercice de pensée : l'audit du dividende de sobriété

L'exercice consiste à prendre tous les services de votre zone verte et à calculer le « dividende de sobriété » que vous pourriez libérer en les décommissionnant. L'objectif est de quantifier le gisement de ressources que vous pouvez réinvestir dans vos zones critique et importante.

Méthode détaillée (durée suggérée : 4 heures)

Cette méthode est proposée à titre indicatif. Adapter la durée, les participants et les étapes selon vos contraintes et votre culture organisationnelle.

1. Participants : réunissez le CODIR, les directeurs métiers, le DSI et les responsables des services de la zone verte.

2. Inventaire de la zone verte (30 min) : listez tous les services, applications. et infrastructures de votre zone verte. Privilégiez ceux qui existent depuis au moins 2 ans et dont le coût annuel est significatif.

3. Calcul du coût total annuel (60 min) : pour chaque service, calculez. le coût complet en incluant :

   - Licences et abonnements.
   - Infrastructure (serveurs, stockage, réseau).
   - Maintenance et support.
   - Énergie et refroidissement.
   - Temps IT (développement, support, gestion).
   - Coût d'opportunité (temps utilisateur perdu par exemple).

4. Évaluation de la valeur métier (90 min) : pour chaque service, évaluez. sa valeur métier réelle sur une échelle de 0 (faible) à 2 (forte) en répondant à ces questions :

   - Le service répond-il à un besoin métier réel et stratégique ?
   - Quel est le taux d'utilisation réel (pourcentage d'utilisateurs actifs) ?
   - Existe-t-il une alternative plus simple ou moins coûteuse ?
   - Le service est-il contourné par du shadow IT ?

5. Calcul du dividende de sobriété (60 min) ; calculez-le selon la formule :
   $Dividende = Coût\ annuel \times {}^{(2-Valeur\ métier)}/_{2} + (Impact\ CO2 \times Prix\ carbone)$
   Plus la valeur métier est faible, plus le dividende est élevé.

6. Priorisation (30 min) : classez les services par dividende décroissant. et identifiez les « quick wins » (dividende élevé, faible résistance au changement).

Modèle : grille d'évaluation du dividende de sobriété

Ce modèle est un exemple à adapter en ajoutant vos propres critères (conformité réglementaire, impact sur la marque, etc.) :

- Service Zone Verte.
- Coût Annuel Complet.
- Valeur Métier (0-3).
- Taux Utilisation.
- Impact CO2 (tonnes).
- Dividende Sobriété.
- Priorité.

Ce dividende représente les ressources que vous pouvez libérer pour renforcer vos zones critique et importante.

Mécanisme de fragilisation : Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)

Cette section ne détaille pas le mécanisme (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre risque.

Pourquoi est-il si difficile de se défaire d'un service inutile de la zone verte ?

Les choix technologiques que vous avez faits par le passé, souvent pour des raisons de coût ou de commodité, vous ont enfermés dans des écosystèmes dont il est aujourd'hui extrêmement coûteux, voire impossible, de sortir. Vous conservez ces services de confort non pas parce qu'ils sont utiles, mais par simple habitude, parce que les coûts de sortie semblent trop élevés, ou parce que vos équipes ne savent plus faire autrement.

Comment utiliser ce mécanisme pour évaluer votre risque ?

Le mécanisme de verrouillage opère sur trois dimensions. Évaluer l'exposition pour chaque dimension selon 3 niveaux de risque : faible (poids = 0), moyen (poids = 1), élevé (poids = 2) :

Dimension	Questions	Évaluation
Technique	Vos données sont-elles enfermées dans des formats propriétaires ? Pouvez-vous les exporter facilement ?	
Économique	Le coût de migration vers une alternative est-il supérieur à 6 mois de coût d'exploitation du service actuel ?	
Organisationnel	Vos équipes ont-elles développé des compétences spécifiques difficiles à transférer ? Y a-t-il une résistance culturelle au changement ?	
Score de complexité (/ 6)	$\sum \acute{E}valuations$	

Un score total supérieur à 4 indique un verrouillage fort qui nécessite une stratégie de sortie progressive. Ce seuil est indicatif et doit être adapté à votre contexte.

Le vrai coût du confort, c'est la résilience que vous ne vous offrez pas.

Scénario d'application : La crise de confiance généralisée

Cette section ne détaille pas le scénario (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre exposition.

Suite à une conjoncture économique difficile (perte de clientèle faisant suite à une perte de confiance généralisée), votre direction vous impose une coupe de 30 % de votre budget de fonctionnement en 3 mois. La panique s'installe. Sans visibilité sur la valeur réelle de vos services, vous devez couper à la hâte, sans réelle gestion des priorités. Vous sacrifiez l'avenir pour sauver le présent.

Le leader qui a déjà fait l'audit de sa zone verte est dans une position radicalement différente. Il ne subit pas la crise, il la pilote.

Checklist de préparation

1. Avant la crise (préparation)

   ☐ **Audit** du dividende de sobriété réalisé et à jour (moins de 6 mois).

   ☐ **Liste** des services de la zone verte classés par dividende décroissant.

   ☐ **Matrice d'arbitrage** préparée (« Si nous coupons X, nous finançons Y »).

   ☐ **Communication** préparée pour expliquer les arbitrages.

   ☐ **Plan de décommissionnement** technique prêt pour les services prioritaires.

   ☐ **Identification** des résistances au changement et plan d'accompagnement.

2. Pendant la crise (réaction)

   ☐ **Convocation** d'un comité de crise avec le CODIR dans les 48 h

   ☐ **Présentation** de la liste des services de la zone verte et de leur dividende.

   ☐ **Proposition** d'un plan d'arbitrage chiffré (« Nous pouvons libérer X % en décommissionnant ces services »).

   ☐ **Validation** des services à décommissionner par ordre de priorité.

   ☐ **Communication** transparente aux équipes sur les arbitrages et le réinvestissement.

   ☐ **Lancement** du plan de décommissionnement technique.

3. Après la crise (capitalisation)

   ☐ **Mesure** des économies réalisées et du temps de réaction.

   ☐ **Analyse** des résistances rencontrées et des leviers efficaces.

   ☐ **Documentation** des apprentissages pour la prochaine crise.

   ☐ **Mise à jour** de l'audit du dividende de sobriété.

   ☐ **Communication** des résultats et du réinvestissement effectué.

Inspiration et principe de résilience : Patagonia, 37signals (Basecamp), L'Estonie

Comment contrer cette fragilité ? En changeant radicalement de paradigme : passer de l'accumulation à la sobriété stratégique. En effet, refuser systématiquement la complexité libère du temps pour l'essentiel ; la standardisation systématique élimine la complexité et les coûts. La contrainte volontaire et assumée plutôt que subie attire la clientèle et les meilleurs talents

La sobriété stratégique n'est pas la décroissance. C'est l'art de l'allocation intelligente des ressources. C'est un arbitrage conscient entre un confort immédiat mais fragile, et une robustesse durable. C'est un acte de lucidité et de courage.

Comment transposer ces inspirations à votre SI ?

Ce qui est fait	Ce que vous pouvez faire
Patagonia : inspirer en déconseillant d'acheter inutilement et en encourageant à la réparation.	**Réduire** le nombre total d'applications de confort au strict nécessaire. **Prolonger** la vie des systèmes existants par la maintenance et l'optimisation avant tout nouveau développement.
37signals : mise en place d'une approche radicalement sobre et extraordinairement performante.	**Refuser** de nouveaux projets en zone verte pour éviter de consommer . **Auditer** régulièrement chaque outil et éliminer ceux qui ne servent pas directement les utilisateurs.
Estonie : simplification maximale par l'interopérabilité et l'unicité des solutions.	**Unicité** des solutions par catégorie de besoin. **Adopter** une approche API-first avec standards ouverts.

Solutions : maximiser votre dividende de sobriété

Action 1 : instaurer la « Matrice d'arbitrage »

***Objectif** : faire de l'audit du dividende de sobriété un outil de gouvernance permanent*

Méthode à adapter selon le contexte :

1. Réaliser l'audit du dividende de sobriété chaque année, avant la préparation budgétaire.
2. Présenter la liste des services de la zone verte et le dividende associé à leur décommissionnement au CODIR.
3. Proposer un plan d'arbitrage explicite.
4. Faire voter le CODIR sur les arbitrages proposés.
5. Communiquer les décisions de manière transparente aux équipes.

Délai de mise en œuvre	:	1-2 mois
Effort estimé	:	3-5 jours x homme
Prérequis	:	résultats de l'audit du dividende de sobriété, calendrier budgétaire, accès au CODIR
Critères de succès	:	– Matrice d'arbitrage validée par le CODIR – Processus de décision annuel intégré au cycle budgétaire. – Communication transparente des arbitrages aux équipes.

Action 2 : adopter des « Politiques de désengagement » (Sunset Policies)

***Objectif** : automatiser l'élimination des services inutiles pour éviter l'accumulation*

Méthode à adapter selon le contexte

1. Définir une règle simple : toute application qui n'a pas été utilisée de manière significative pendant 12 mois (seuil à adapter) est automatiquement placée sur une liste de décommissionnement.
2. Notifier le propriétaire du service qui a trois mois pour justifier de son utilité avec des données d'usage.
3. Si la justification est insuffisante, le service est archivé (accès. en lecture seule) pendant 6 mois — adapter selon les contraintes réglementaires.
4. Après la période d'archivage sans réclamation, le service est définitivement. supprimé.
5. Communiquer cette politique largement et l'appliquer sans exception.

6. Critères d'utilisation significative (à adapter) :
   (a) Moins de 5 % des utilisateurs potentiels actifs sur les 12 derniers mois.
   (b) Moins de 10 transactions/mois en moyenne.
   (c) Taux de satisfaction < 3/5.
   (d) Existence d'une alternative plus simple ou moins coûteuse.

Délai de mise en œuvre	:	2-3 mois pour la définition 12-18 mois pour le premier cycle complet
Effort estimé	:	5-10 jours x homme pour la mise en place 1-2 jours x homme par mois en maintenance
Prérequis	:	inventaire des services, métriques d'usage disponibles, validation de la direction
Critères de succès	:	– Politique formalisée et communiquée à 100 % des équipes. – Au moins 10 % des services décommissionnés après le premier cycle. – Zéro exception non justifiée à la politique.

Action 3 : adapter la production avec la méthode TELED

***Objectif** : passer d'une gestion en flux tendu à une gestion par stocks stratégiques pour les services de confort*

Méthode à adapter selon le contexte

1. Identifier les tâches de la zone verte qui sont consommatrices de ressources (calculs intensifs, traitements de données).
2. Prioriser ces tâches pour les exécuter quand les ressources sont disponibles (heures creuses, surplus de capacité).
3. Créer des stocks stratégiques de résultats (rapports pré-générés, analyses pré-calculées) plutôt que de tout générer à la demande.
4. Réduire la fréquence de mise à jour des services de confort (ex : rapport hebdomadaire le week-end au lieu de quotidien).

Délai de mise en œuvre	:	3-6 mois
Effort estimé	:	10-20 jours x homme
Prérequis	:	cartographie des tâches consommatrices, outils de planification, capacité de stockage
Critères de succès	:	– Réduction significative de la consommation en heures de pointe. – Stocks stratégiques opérationnels pour les services de confort. – Satisfaction utilisateurs maintenue malgré la réduction de fréquence.

Action 4 : communiquer le réinvestissement

Objectif *: transformer la perception de la sobriété de « privation » à « renforcement »*

Méthode à adapter selon le contexte :

1. Pour chaque service décommissionné, annoncer clairement le réinvestissement. associé
2. Utiliser une formule simple : « Nous avons décidé de décommissionner [service]. Les [montant] économisés seront immédiatement réinvestis dans [projet de renforcement] ».
3. Publier un tableau de bord public du réinvestissement avec le suivi des économies et des projets financés.
4. Célébrer les succès : « Grâce au décommissionnement de X services, nous avons pu financer Y, qui renforce notre résilience ».

Délai de mise en œuvre	:	1-2 mois
Effort estimé	:	3-5 jours x homme pour la mise en place 1 jour x homme par mois en suivi
Prérequis	:	calcul du dividende de sobriété, plan de réinvestissement validé, canaux de communication internes
Critères de succès	:	– 100 % des décommissionnements associés à un réinvestissement communiqué. – Tableau de bord du réinvestissement accessible à tous. – Perception positive de la sobriété mesurée par enquête interne.

Action 5 : pratiquer la « Sobriété offensive »

***Objectif** : transformer la sobriété en mouvement collectif et contagieux*

Méthode à adapter selon le contexte :

1. Partager publiquement la liste de services décommissionnés avec les critères d'arbitrage utilisés.
2. Créer un « GitHub de la sobriété » où sont documentées les décisions, les méthodes et les apprentissages ; exemple de contenu :
   (a) La liste des services décommissionnés et leur dividende.
   (b) Les grilles d'évaluation utilisées.
   (c) Les résistances rencontrées et les leviers efficaces.
   (d) Les templates de communication.
   (e) Les résultats obtenus (économies, ROI, impact carbone).
3. Lancer un challenge territorial : « Qui libérera le plus de ressources cette année ? ».
4. Organiser des ateliers de partage d'expérience avec d'autres organisations.
5. Publier des articles et participer à des conférences pour inspirer d'autres organisations.

Délai de mise en œuvre	:	3-6 mois pour le lancement action continue ensuite
Effort estimé	:	10-15 jours x homme pour la mise en place 2-3 jours x homme par mois en animation
Prérequis	:	résultats concrets de sobriété à partager, validation de la direction pour la communication externe, réseau de partenaires
Critères de succès	:	– Plateforme de partage opérationnelle avec au moins 10 retours d'expérience documentés. – Au moins 3 organisations partenaires engagées dans la démarche. – Participation à au moins 2 événements externes par an.

Action 6 : pour les pionniers, adopter la règle du « 1 pour 3 »

***Objectif** : inverser radicalement la tendance à l'accumulation*

Méthode à adapter selon le contexte :

1. Pour chaque nouveau service ajouté dans la zone verte, supprimer trois services existants.
2. Cette règle force une priorisation drastique et évite l'accumulation.
3. Si la règle du « 1 pour 3 » semble trop radicale, commencer par un ratio moins ambitieux (1 pour 2, ou 1 pour 1).
4. Progresser vers le ratio 1 pour 3 sur 2-3 ans.

Délai de mise en œuvre	:	1-2 mois pour la définition 2-3 ans pour atteindre le ratio cible
Effort estimé	:	2-3 jours x homme pour la mise en place suivi continu ensuite
Prérequis	:	inventaire des services de la zone verte, politique de sunset validée, engagement fort de la direction
Critères de succès	:	– Règle formalisée et intégrée au processus de demande de nouveaux services. – Ratio effectif de suppression/ajout mesuré trimestriellement. – Réduction nette du nombre de services de la zone verte sur 2 ans.

Métriques dites Oseja de la Facette 7

Le nom d'Oseja pour ces métriques est à prendre comme une typologie. d'indicateurs en relation avec ce livre blanc.

- Métrique Oseja n° 12 — Ratio de sobriété.
  - Définition : pourcentage du budget IT consacré aux zones critique. et importante par rapport au budget IT total.
  - Comment le mesurer : $\frac{Budget\ IT(zones\ rouge+orange)}{Budget\ IT\ total}$
  - Comment l'interpréter :
    - < 50 % : l'organisation est très orientée confort, risque de fragilité élevé.
    - 50-70 % : équilibre classique, marge de progression importante.
    - 70-80 % : bon alignement stratégique.
    - 80 % et plus : excellente sobriété stratégique.

ROI (conceptuel) : le dividende de sobriété

Le ROI de la sobriété stratégique ne se chiffre pas uniquement en euros économisés, mais en ressources libérées pour renforcer vos zones critique et importante. Voici la méthode d'évaluation en trois étapes que nous avons développée.

Étape 1 : Identifier les coûts actuels de la zone verte

Pour réaliser l'audit du dividende de sobriété et planifier le décommissionnement, estimer :

- Le temps nécessaire pour auditer tous les services de la zone verte (inventaire, analyse d'usage, calcul des coûts).
- Le temps de planification du décommissionnement (priorisation, planification technique, gestion des dépendances).
- Le temps de communication et d'accompagnement des équipes (formation, conduite du changement).
- L'investissement total en jours-homme pour mener cette démarche.

Étape 2 : Estimer les gains du décommissionnement

Au-delà des économies directes (licences, infrastructure), le décommissionnement génère des bénéfices indirects :

- Réduction du temps IT consacré au support et à la maintenance des services inutiles.
- Réduction de l'empreinte carbone (moins de serveurs, moins d'énergie consommée).
- Gain de clarté et de focus pour les équipes (moins de complexité à gérer).
- Libération de budget pour investir dans les zones critique et importante.

Étape 3 : Calculer le dividende net

$$Dividende\ de\ sobriété = (Économies\ annuelles\ directes + Réduction\ temps\ IT + Valeur\ gains\ indirects) - Investissement\ initial$$

Bénéfices non quantifiables

- Agilité accrue : capacité à réagir rapidement en cas de crise budgétaire.
- Résilience renforcée : ressources disponibles pour investir dans les zones critique et importante.
- Clarté stratégique : alignement de l'IT sur les priorités métier.
- Attractivité : signal fort pour les talents en quête de sens.
- Licence sociale d'opérer : reconnaissance de votre responsabilité environnementale.

M.3 Facette 8 : De la mine d'entreprise à la mine collective

Cette deuxième facette explore comment vos déchets numériques peuvent devenir une ressource collective et comment la circularité permet de construire une résilience écosystémique.

Exercice de pensée : l'audit de potentiel collectif

Au Tour 2, vous avez créé votre Digital Enterprise Mine interne. Le Tour 3 transforme cette approche individuelle en dynamique collective. Cet exercice révèle le potentiel de création d'une Digital Urban Mine territoriale.

Méthode détaillée

Cartographiez votre écosystème de mutualisation :

1. Identifier les partenaires potentiels (durée : 1 mois) :
   - Qui génère des déchets électroniques similaires aux vôtres ?
   - Quelles organisations partagent vos problématiques d'approvisionnement ?
   - Qui pourrait bénéficier de vos composants excédentaires ?
   - Qui pourrait vous fournir les composants qui vous manquent ?
   - Quelle organisation locale traite déjà ce type de problématique (recycleur, fournisseur, mainteneur) ?
2. Évaluer le potentiel de mutualisation (durée : 2 mois) :
   - Volume combiné d'équipements en fin de vie par an.
   - Diversité des composants disponibles.
   - Complémentarité des besoins (ce que vous jetez, d'autres en ont besoin).
   - Capacités mutualisables (espace de stockage, compétences de test, etc.).
3. Analyser et opérationnaliser les conditions de succès (durée : 3 mois) :
   - Niveau de confiance entre partenaires,
   - Proximité géographique,
   - Alignement des valeurs (ESG, économie circulaire),
   - Capacité d'investissement collectif,
   - Vision partagée de la gouvernance,
   - Localisation de la mine,

  - Procédures de tests et de certification,
  - Plateforme de pilotage,
  - Premier pilote.

Cet exercice révèle que vous n'êtes pas seul face au gaspillage. Ensemble, vous pouvez transformer un coût individuel en valeur collective.

Cette méthode est proposée à titre indicatif. Adapter la durée, les participants et les étapes selon vos contraintes et votre culture organisationnelle.

Modèle : grille d'évaluation du potentiel de mutualisation

Ce modèle est un exemple à adapter en ajoutant vos propres critères :

- Partenaire potentiel.
- Type (public, privé, ESN, industriel…)
- Attribuer une note entre 0 (faible) et 2 (forte) pour les trois items. suivants :
  - Volume déchets par an.
  - Complémentarité.
  - Motivation.
- Score.
- Coût de la mutualisation (logistique, gouvernance…) par rapport à la valeur marchande potentielle des pièces pondérée par le risque de rupture.

Mécanisme de fragilisation : Fragilités géopolitiques et Fragilités physiques/climatiques face à l'incertitude environnementale

Cette section ne détaille pas les mécanismes (voir annexe dédiée), mais vous aide à les utiliser pour évaluer votre propre risque.

Le traitement du matériel comme un déchet est une double fragilité qui expose aux mécanismes de fragilisation géopolitique et physique. En jetant ou en rendant des équipements encore fonctionnels pour tout ou partie, vous restez totalement dépendant des chaînes d'approvisionnement mondiales fragiles. En jetant des équipements réparables, vous contribuez à la pression sur les ressources naturelles :

Vous êtes, peut-être, une partie du problème de la fragilité physique mondiale, alors même que vous possédez, sûrement, une partie de la solution.

Comment utiliser ces mécanismes pour évaluer votre risque ?

Le mécanisme de fragilité opère sur trois dimensions. Évaluer l'exposition pour chaque dimension selon 3 niveaux de risque : faible (poids = 0), moyen (poids = 1), élevé (poids = 2) :

Dimension	Questions	Évaluation
Technique	Avez-vous diversifié les types de matériels ou de logiciels pour répondre à un même besoin ?	
Économique	Avez-vous (ou vos fournisseurs) diversifié les circuits d'approvisionnement que ce soit par les fournisseurs et les origines des matériels ?	
Organisationnel	Est-ce que vos équipes sont en capacité de réparer en autonomie les matériels ?	
Score de complexité (/ 6)	$\sum Évaluations$	

Un score total supérieur à 4 indique un fragilité forte qui nécessite une stratégie de sortie progressive. Ce seuil est indicatif et doit être adapté à votre contexte.

Scénario d'application : La rupture géopolitique

Cette section ne détaille pas le scénario (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre exposition.

Une nouvelle crise géopolitique (conflit autour de Taïwan, embargo sur les terres rares chinoises) bloque l'importation de composants électroniques. Vous avez un besoin urgent de barrettes de RAM pour augmenter la capacité d'un serveur critique de votre zone orange. Votre fournisseur vous annonce un délai de 9 mois et un prix multiplié par 3.

Pendant ce temps, dans votre entrepôt ou celui d'une organisation partenaire, 20 serveurs mis au rebut il y a 6 mois contiennent exactement les barrettes de RAM dont vous avez besoin. Mais faute de processus pour les récupérer, les tester et les certifier, ce trésor est inaccessible.

Vous êtes en pénurie au milieu d'une abondance potentielle. C'est le paradoxe de la dépendance subie.

Checklist de préparation

1. Avant la crise (préparation)

   ☐ **Inventaire** des actifs dormants réalisé et à jour.

   ☐ **Digital Enterprise Mine** opérationnelle (Tour 2).

   ☐ **Partenariats** avec 3-5 organisations locales pour créer une Digital Urban Mine.

   ☐ **Protocole** de test et certification des composants récupérés.

   ☐ **Processus** de destruction sécurisée des données.

   ☐ **Stock stratégique** de composants critiques constitué (RAM, disques durs, alimentations).

☐ **Compétences** de démantèlement et réparation développées en interne ou via partenaires.

2. Pendant la crise (réaction)

☐ **Activation** du réseau de la Digital Urban Mine pour identifier les composants disponibles.

☐ **Récupération** des composants nécessaires dans les actifs dormants.

☐ **Test et certification** des composants selon le protocole établi.

☐ **Installation** des composants récupérés sur les équipements critiques.

☐ **Documentation** de l'opération pour capitalisation.

☐ **Communication** sur la résilience apportée par la mine collective.

3. Après la crise (capitalisation)

☐ **Mesure** du temps de réaction et des économies réalisées.

☐ **Analyse** des composants manquants dans le stock stratégique.

☐ **Ajustement** du protocole de récupération et certification.

☐ **Renforcement** des partenariats de la mine collective.

☐ **Communication** des résultats pour inspirer d'autres. organisations

Inspiration et principe de résilience : Mine urbaine

Comment sortir de ce paradoxe ? En transformant votre vision du déchet. C'est ici que la Digital Enterprise Mine, évoquée dans le Tour 2, prend une dimension de leadership.

Une organisation inspirante ne se contente pas de gérer ses propres actif, elle initie la création d'une Digital Urban Mine : une plateforme locale, en partenariat avec d'autres entreprises, des reconditionneurs et des associations, pour collecter, démanteler, certifier et redistribuer les composants et équipements.

Cette mine ne sert pas à maintenir le confort. Au contraire, elle est alimentée par les arbitrages de la zone verte. Les matériels décommissionnés des services de confort deviennent une source de pièces détachées pour garantir la durabilité des postes de travail essentiels (zone orange) ou des serveurs critiques (zone rouge).

La vraie résilience n'est pas individuelle, elle est collective. En transformant vos déchets en ressources partagées, vous créez une interdépendance choisie qui renforce tout l'écosystème. La circularité collective est le fondement de la résilience écosystémique.

Comment transposer cette inspiration à votre SI ?

Ce que la mine urbaine fait	Ce que vous pouvez faire
Déchets : valoriser les déchets pour alimenter l'économie circulaire.	**Collecter** les matériels dits « obsolètes » (fin de contrat, en panne…) pour l'organisation, afin d'identifier le réemploi de tout ou partie de leurs éléments constitutifs : disques pour stockage froid, mémoires pour environnements de test, cartes réseau pour infrastructures secondaires. **Développer** une capacité locale de récupération et réutilisation. Transformer la contrainte réglementaire (gestion des déchets) en autonomie stratégique d'approvisionnement, particulièrement critique en période de pénurie.
Gouvernance : mise en place d'une approche de gestion des biens. communs entre partenaires.	**Adopter** les principes d'Ostrom pour la gouvernance de la mine : règles cocréées, rotation des responsabilités, transparence, sanctions graduées.

Solutions : créer un bien commun numérique

Action 1 : commencer par le collectif (approche radicale)

***Objectif** : créer rapidement une Digital Urban Mine collective en plus d'une mine interne.*

Méthode à adapter selon le contexte :

1. Identifier 3-5 organisations partenaires du territoire (même secteur, clients, fournisseurs, collectivités).

2. Proposer de créer une Digital Urban Mine collective dès le jour 1.

3. Condition d'entrée : chaque partenaire apporte un nombre minimum d'équipements dormants.
   Cela crée immédiatement une masse critique et évite le problème du « passager clandestin ».

4. Mutualiser les coûts de collecte, démantèlement, test et certification.

Délai de mise en œuvre	:	6-12 mois
Effort estimé	:	20-30 jours x homme pour la coordination initiale
Prérequis	:	identification des partenaires potentiels, inventaire des équipements dormants, accord de principe des directions
Critères de succès	:	– Au moins 3 organisations partenaires engagées. – Masse critique de 500+ équipements collectés (valeur à adapter selon le contexte). – Structure de gouvernance définie et opérationnelle.

Action 2 : adopter une gouvernance de bien commun (inspirée d'Elinor Ostrom)

***Objectif** : créer une gouvernance collective qui assure la pérennité et l'équité de la mine collective.*

Les 8 principes d'Ostrom appliqués à la Digital Urban Mine :

1. Limites clairement définies : qui peut participer ? (organisations du territoire, condition d'entrée).

2. Règles adaptées au contexte local : quels composants sont collectés ? quels protocoles de test ? (co-créés par tous).

3. Participation à la prise de décision : tous les participants votent les règles et les évolutions (1 organisation = 1 voix).

4. Surveillance par les pairs : transparence totale sur les stocks, les flux et les bénéficiaires (tableau de bord public).

5. Sanctions graduées : en cas de non-respect des règles (avertissement, suspension, exclusion).

6. Résolution des conflits : mécanisme de médiation en cas de désaccord (comité de 3 membres tirés au sort).

7. Reconnaissance du droit d'auto-organisation : les autorités externes respectent l'autonomie de la mine.

8. Gouvernance multi-niveaux : si la mine s'étend, création de sous-groupes locaux avec coordination centrale.

Méthode à adapter selon le contexte :

1. Organiser un atelier de co-création des règles avec tous les partenaires. (1 journée) ; exemple de règles co-créées :

   (a) Chaque organisation apporte au moins 50 équipements par an pour rester membre.

   (b) Chaque organisation peut prélever jusqu'à 150 % de ce qu'elle a apporté (en valeur).

   (c) Les composants excédentaires sont donnés à des associations ou écoles (20 % du stock).

   (d) Les décisions stratégiques sont prises par vote à la majorité des 2/3.

   (e) Un membre qui ne respecte pas les règles reçoit un avertissement, puis est suspendu 6 mois, puis exclu.

2. Rédiger une charte de la Digital Urban Mine qui formalise les 8 principes.

3. Créer un comité de pilotage avec rotation des responsabilités (mandat de 1 an).

4. Mettre en place un tableau de bord public avec les stocks, les flux et les bénéficiaires.

5. Organiser une assemblée générale annuelle pour évaluer et ajuster les règles.

Délai de mise en œuvre	:	2-3 mois pour la mise en place initiale
Effort estimé	:	10-15 jours x homme pour la co-création des règles et la formalisation
Prérequis	:	partenaires identifiés et engagés, connaissance des principes d'Ostrom, facilitateur pour les ateliers
Critères de succès	:	– Charte de gouvernance adoptée par 100 % des partenaires. – Comité de pilotage opérationnel avec rotation effective. – Tableau de bord public accessible et mis à jour mensuellement.

Action 3 : viser l'impact sociétal, pas seulement économique

***Objectif** : transformer la mine collective en projet à impact social pour renforcer votre licence sociale d'opérer.*

Méthode à adapter selon le contexte :

1. Réservez 20 % des composants récupérés pour des associations, écoles ou structures d'insertion.
2. Proposer des formations gratuites à la réparation pour les jeunes du territoire (partenariat avec des écoles techniques).
3. Publier en open source les protocoles de test et de certification pour inspirer d'autres territoires.
4. Créer des emplois locaux de réparation et reconditionnement (partenariat avec des structures d'insertion).
5. Communiquer largement sur l'impact social de la mine collective.

Délai de mise en œuvre	:	6-12 mois pour les premiers partenariats
Effort estimé	:	5-10 jours x homme pour la coordination suivi continu ensuite
Prérequis	:	mine collective opérationnelle, identification des partenaires associatifs et éducatifs, budget pour les dons
Critères de succès	:	– 20 % des composants redistribués à des structures à impact social (valeur à adapter selon le contexte). – Au moins 2 partenariats avec des écoles ou structures d'insertion (valeur à adapter selon le contexte). – Protocoles publiés en open source.

Action 4 : l'approche progressive (pour organisations moins matures)

***Objectif** : pour les organisations qui ne sont pas prêtes à commencer par le collectif, proposer une approche progressive.*

Méthode à adapter selon le contexte :

1. Étape 1 (6 mois) : maîtriser la Digital Enterprise Mine interne (Tour 2).
2. Étape 2 (6 mois) : mutualiser avec 2-3 entreprises de confiance du. réseau
3. Étape 3 (12 mois) : élargir au secteur d'activité (5-10 organisations).
4. Étape 4 (12 mois) : ouvrir à l'ensemble du territoire (collectivités, écoles, associations).

Délai de mise en œuvre	:	2-3 ans pour le parcours complet
Effort estimé	:	5-10 jours x homme par étape
Prérequis	:	Digital Enterprise Mine interne maîtrisée (Tour 2), réseau de confiance identifié
Critères de succès	:	– Passage réussi de chaque étape avec indicateurs validés. – Nombre de partenaires croissant à chaque étape. – Gouvernance adaptée à chaque niveau d'ouverture.

Action 5 : adresser les défis pratiques

***Objectif** : lever les obstacles techniques et organisationnels à la réutilisation des composants.*

Défi 1 : responsabilité juridique et certification.

- Problème : qui certifie la qualité des composants récupérés ? qui. est responsable en cas de panne ?
- Solution : créez un protocole de test standardisé et une assurance qualité partagée. Chaque partenaire certifie ses propres équipements selon le protocole commun. Souscrivez une assurance collective pour couvrir les risques résiduels.
- Exemple de protocole : test de 100 % des composants critiques (RAM, disques), certification par un technicien formé, étiquetage avec date de test et nom du certificateur, garantie de 6 mois.

Défi 2 : confidentialité des données.

- Problème : les disques durs contiennent des données sensibles (RGPD, secret médical, secret des affaires)
- Solution : mettez en place un processus de destruction certifiée des données avant démantèlement. Investissez dans des outils de formatage sécurisé (norme DoD 5220.22-M ou mieux). Documentez chaque étape et conservez les certificats de destruction.

- Exemple : achat d'un logiciel de formatage sécurisé (Blancco, DBAN), formation de 2 techniciens, processus en 3 étapes (formatage logiciel, vérification, destruction physique si nécessaire), certificat de destruction pour chaque disque.

Défi 3 : Standardisation et compatibilité.

- Problème : tous les composants ne sont pas compatibles entre eux (RAM DDR3 vs DDR4, connecteurs propriétaires)
- Solution : commencez par les éléments les plus standardisés (RAM, disques durs SATA, alimentations ATX) avant de vous attaquer aux composants plus spécifiques. Créez un catalogue de compatibilité partagé.
- Exemple : focus initial sur RAM DDR4, disques SATA 2,5" et 3,5", alimentations ATX. Création d'une base de données de compatibilité accessible à tous les partenaires.

Délai de mise en œuvre :	3-6 mois pour les processus de base
Effort estimé :	10-15 jours x homme pour la mise en place des processus
Prérequis :	expertise technique disponible, outils de formatage sécurisé, budget pour les équipements de test
Critères de succès :	– Protocole de test et certification opérationnel. – Processus de destruction des données conforme RGPD. – Catalogue de compatibilité accessible à tous les partenaires.

Métriques Oseja de la Facette 8

- Métrique Oseja n° 13 — Impact commun.
  - Définition : ratio entre la valeur des composants donnés à la Digital. Urban Mine et la valeur des composants reçus.
  - Comment le mesurer : $Impact\ commun = \frac{Valeur\ des\ composants\ donnés}{Valeur\ des\ composants\ reçus}$
  - Comment l'interpréter :
    - Ratio > 1 : vous êtes un contributeur net au bien commun (vous donnez plus que vous ne recevez).
    - Ratio = 1 : vous êtes en équilibre (vous donnez autant que vous recevez).
    - Ratio < 1 : vous bénéficiez plus que vous ne donnez (acceptable en phase de démarrage ou pour des organisations en difficulté).

ROI (conceptuel) : le dividende de circularité

Le ROI de la circularité ne se chiffre pas uniquement en euros économisés, mais en résilience collective créée. Voici la méthode d'évaluation en trois étapes que nous avons développée.

Étape 1 : Identifier les coûts actuels du gaspillage de ressources

Pour chaque équipement mis au rebut dans les 12 derniers mois, estimez :

- Le coût d'achat initial de l'équipement.
- La valeur résiduelle des composants réutilisables (RAM, disques, alimentations, écrans).
- Le coût de remplacement de ces composants s'ils devaient être achetés neufs.
- Les délais d'approvisionnement en cas de pénurie (coût d'opportunité).

Étape 2 : Estimer les gains de la circularité

Au-delà des économies directes, la création d'une Digital Urban Mine génère des bénéfices indirects :

- Réduction de la dépendance aux chaînes d'approvisionnement mondiales.
- Accélération des réparations (composants disponibles immédiatement).
- Résilience collective face aux pénuries (effet de réseau).
- Impact social et environnemental (création d'emplois locaux, réduction. de l'empreinte carbone)

Étape 3 : Calculer le dividende net

$$Dividende\ de\ circularité\ =\ (Valeur\ des\ composants\ récupérés\ +\ Valeur\ des\ gains\ indirects)\ -\ Coût\ de\ mise\ en\ place\ de\ la\ mine$$

M.4 Facette 9 : Le donut de Raworth et le courage du « Non »

Cette troisième facette explore comment le modèle du donut peut devenir une boussole pour prospérer dans un espace juste et sûr, entre un plancher social et un plafond écologique.

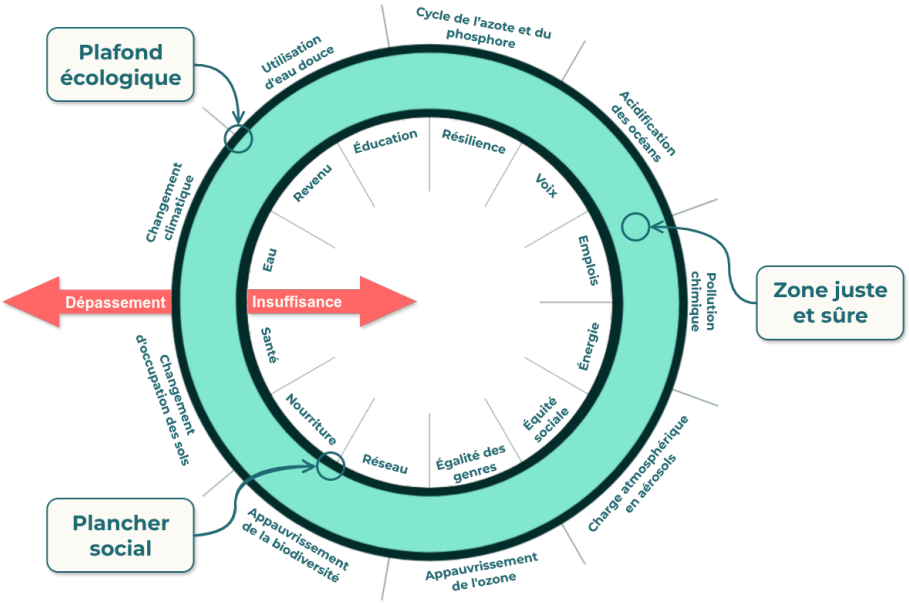


FIG. M.4.1 : Le donut de Kate Raworth

Exercice de pensée : votre position dans le donut

L'exercice consiste à évaluer la position de vos services de la zone verte dans le donut de Kate Raworth pour identifier ceux qui dépassent le plafond écologique sans satisfaire le plancher social (le pire des deux mondes).

Méthode détaillée (durée suggérée : 3 heures)

Cette méthode est proposée à titre indicatif. Adapter la durée, les participants et les étapes selon vos contraintes et votre culture organisationnelle.

Cette méthode est simplifiée pour être facilement intégrée dans une démarche. Pour avoir une méthode plus rigoureuse, il est nécessaire de mettre en place des évaluations fines pour pouvoir comparer les dimensions du donut entre elles afin de les arbitrer, et de tenir compte pour les impacts négatifs de la phase projet en plus de la phase d'utilisation. Cela ne fait pas l'objet de ce document.

1. Participants : réunissez le CODIR, les directeurs métiers, le DSI, le responsable RSE et idéalement un expert du donut.

2. Présentation du modèle du donut (30 min) : expliquer le concept de Kate Raworth :

   (a) Plancher social : besoins humains fondamentaux (santé, éducation, équité, emploi, justice sociale).

(b) Plafond écologique : limites planétaires (climat, biodiversité, eau douce, azote, phosphore).

(c) Espace juste et sûr : entre le plancher et le plafond, où l'humanité peut prospérer durablement.

3. Sélection des services (15 min) : choisir 5 à 10 services représentatifs de votre zone verte.

4. Créer la méthode du « Test du donut » :

(a) Pour chaque service et chaque dimension du donut concernée, évaluer sa contribution positive sur une échelle de 0 (nulle) à 2 (forte) (60 minutes).
Permet-il d'éviter ou de réduire une insuffisance du plancher social ou un dépassement du plafond écologique ?

(b) Pour chaque service et chaque dimension du donut concernée, évaluer son impact négatif sur une échelle de 0 (nulle) à 2 (fort) (60 minutes).
Augmente-t-il ou génère-t-il une insuffisance du plancher social ou un dépassement du plafond écologique ?

(c) Visualisation dans le donut (45 min) :

i. Placer chaque service sur un graphique à deux axes (contribution positive en ordonnée, impact négatif en abscisse).

ii. Identifier les services en bas à droite (faible contribution, fort impact) : ce sont les premiers candidats au décommissionnement.

Mécanisme de fragilisation : Impacts sociétaux dans un contexte d'incertitude croissante

Cette section ne détaille pas le mécanisme (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre risque.

Pourquoi continuer à maintenir des services qui ne créent ni valeur sociale ni durabilité environnementale ? Le numérique n'est plus un simple outil, il façonne la société. Les conséquences de nos technologies — surcharge informationnelle, surveillance, dépendance aux algorithmes, fracture numérique, désinformation — créent un climat de méfiance et d'incertitude qui affecte directement votre entreprise.

Cette érosion de la confiance se traduit par une perte de votre « licence sociale d'opérer » : le droit implicite de mener vos activités, accordé par la société en échange de votre contribution au bien commun.

Comment utiliser ce mécanisme pour évaluer votre risque ?

La méthode « Test du donut » proposée ci-dessus est l'outil pour réaliser cette évaluation.

Scénario d'application : La crise de confiance généralisée

Cette section ne détaille pas le scénario (voir annexe dédiée), mais vous aide à l'utiliser pour évaluer votre propre exposition.

À force de proposer des services qui ne répondent plus aux besoins réels, qui sont trop complexes ou perçus comme intrusifs, les organisations créent une rupture de confiance qui peut se manifester sur deux fronts indépendants mais fortement corrélés :

Crise de confiance externe : vos clients, partenaires et la société se détournent de tout ou partie de vos services numériques, remettant en cause votre « licence sociale d'opérer ».

Crise de confiance interne : vos propres équipes ne croient plus à la pertinence de tout ou partie de vos outils et développent massivement du shadow IT.

Ces deux crises peuvent apparaître indépendamment, mais la présence de l'une est un signal d'alarme fort pour l'autre. Si vous subissez les deux simultanément, la crise est systémique et peut paralyser votre organisation.

Il est possible de se référer à l'annexe du Tour 2 pour identifier si l'organisation peut subir une crise de conscience : Votre organisation pourrait-elle subir une crise de confiance ?. En tout état de cause, il est important de se préparer même si l'organisation est dans une bonne situation vis-à-vis de cette crise de confiance, dans un objectif d'amélioration continue.

Checklist de préparation

1. Avant la crise (préparation)

   ☐ **Audit** de la position donut de tous les services de la zone verte réalisé.

   ☐ **Identification** des services hors du donut (bas-droite : faible contribution sociale, fort impact écologique).

   ☐ **Plan de décommissionnement** des services hors du donut.

   ☐ **Création** d'un « Tableau de bord donut » public avec vos métriques et vos objectifs.

   ☐ **Publication** d'un « Manifeste donut » expliquant votre engagement.

   ☐ **Intégration** du « Test du donut » dans le processus. de validation des nouveaux projets.

   ☐ **Formation** du CODIR et des équipes aux enjeux du donut.

2. Pendant la crise (réaction)

   ☐ **Communication** transparente sur votre position donut et vos actions.

   ☐ **Accélération** du décommissionnement des services hors du donut.

   ☐ **Réinvestissement** du dividende de sobriété dans des projets qui vous ramènent dans le donut.

   ☐ **Dialogue** avec les parties prenantes (clients, employés, citoyens, régulateurs).

☐ **Publication** de vos résultats (économies, réduction CO2, contribution sociale).

3. Après la crise (capitalisation)

☐ **Mesure** de l'évolution de votre position donut.

☐ **Analyse** de l'impact sur votre réputation et votre attractivité.

☐ **Documentation** des apprentissages.

☐ **Renforcement** de votre engagement donut.

☐ **Partage** de votre expérience pour inspirer d'autres. organisations

Inspiration et principe de résilience : Amsterdam, ville donut

Comment contrer cette fragilité ? En adoptant le donut comme boussole stratégique, outil de navigation et de gouvernance, comme l'ont fait, par exemple, certaines villes, dont Amsterdam.

Le donut n'est pas seulement un outil de sensibilisation, mais un outil de navigation. Il vous aide à dire « non » aux projets qui vous font sortir de l'espace juste et sûr, et « oui » aux projets qui vous y maintiennent ou vous y ramènent. C'est un acte de courage et de lucidité.

Le donut vous permet de transformer votre zone verte : au lieu de maintenir des services de confort qui transgressent le plafond écologique ou le plancher social sans créer de réelle contribution positive, vous allez concentrer vos ressources sur des services qui créent de la valeur sociale tout en respectant les limites planétaires.

Une organisation inspirante n'est pas celle qui suit les tendances, mais celle qui anticipe les besoins profonds de la société et qui a le courage d'y adapter son modèle d'affaires. Elle utilise le donut pour dire « non » à une croissance qui détruit, afin de pouvoir dire « oui » à une prospérité qui régénère.

Comment transposer cette inspiration à votre SI ?

Ce que fait Amsterdam	Ce que vous pouvez faire
Donut : définition d'un espace juste et sûr dans lequel l'humanité. peut prospérer.	**Pérenniser** l'organisation en intégrant les limites planétaires et sociales afin de ne pas dégrader l'environnement dans lequel elle opére.
Amsterdam : la ville a mis en place une gouvernance participative qui permet d'impliquer toutes les parties prenantes dans les décisions et de les faire collaborer autour d'objectifs communs.	**Adopter** une gouvernance élargie, associant la clientèle, les fournisseurs, les associations pour arbitrer certaines décisions au-delà d'une simple vision comptable. **Publier** un manifeste donut avec des objectifs mesurables. Créer un tableau de bord accessible montrant la position de chaque service dans le donut. Communiquer régulièrement les progrès et les arbitrages.

Solutions : devenir votre propre Oseja numérique

Action 1 : publier le « Tableau de bord du donut »

***Objectif** : montrer aux parties prenantes la position de tous vos services dans le donut pour identifier les priorités.*

Méthode à adapter selon le contexte :

1. Appliquer la méthode du « Test du donut » sur chaque service de. la zone verte
2. Définir le plan d'action associé pour réduire les impacts négatifs ou augmenter les contributions positives.
3. Publier ce tableau de bord en interne et, si possible, en externe.

Délai de mise en œuvre	:	2-3 mois
Effort estimé	:	5-10 jours x homme
Prérequis	:	cartographie des services de la zone verte, grille du test du donut définie, validation de la direction pour la publication
Critères de succès	:	– 100 % des services de la zone verte évalués selon le test du donut. – Tableau de bord publié et accessible. – Plan d'action défini pour chaque service hors du donut.

Action 2 : institutionnaliser le « Test du donut »

***Objectif** : intégrer le donut dans le processus de validation de tous les nouveaux projets numériques.*

Méthode à adapter selon le contexte :

1. Ajouter une condition plus ou moins contraignante (idéalement rédhibitoire) selon le contexte avec l'évaluation du « Test du donut » au processus de Go/NoGo des nouveaux services.

2. Appliquer cette nouvelle condition au processus de validation des nouveaux services en zone verte.

Délai de mise en œuvre	:	1-2 mois
Effort estimé	:	3-5 jours x homme
Prérequis	:	processus de validation des projets existant, grille du test du donut validée, formation des équipes projet
Critères de succès	:	– Test du donut intégré au processus Go/NoGo de tous les nouveaux projets. – 100 % des nouveaux services évalués avant validation. – Aucun projet validé sans évaluation donut positive.

Action 3 : communiquer votre vision donut

***Objectif** : transformer votre engagement donut en signal fort pour toutes vos parties prenantes.*

Méthode à adapter selon le contexte :

1. Rédiger un « Manifeste donut » qui explique l'engagement à prospérer dans l'espace juste et sûr.

2. Publier sur le site web, les réseaux sociaux, les rapports annuels.

3. Partager les métriques, les arbitrages, les échecs et les succès de manière transparente.

4. Organiser des événements de partage d'expérience avec d'autres organisations.

5. Devenir « Ambassadeur » du donut dans l'écosystème.

Délai de mise en œuvre	:	2-4 mois
Effort estimé	:	5-10 jours x homme pour la rédaction et publication puis effort continu de communication
Prérequis	:	engagement de la direction validé, résultats concrets du test du donut, canaux de communication définis
Critères de succès	:	– Manifeste donut publié et accessible. – Communication régulière sur les métriques et arbitrages. – Au moins 2 événements de partage organisés par an.

Action 4 : réinvestir le dividende de sobriété dans le donut

***Objectif** : créer un cercle vertueux entre sobriété (Facette 7) et vision donut (Facette 9).*

Méthode à adapter selon le contexte :

1. Utiliser les ressources libérées par le décommissionnement des services hors du donut (Facette 7) pour financer des projets qui ramènent dans l'espace juste et sûr.

2. Prioriser les projets en fonction de leurs contributions positives sans excès sur leurs impacts négatifs.

3. Communiquer clairement le lien entre sobriété et donut.

Délai de mise en œuvre	:	3-6 mois
Effort estimé	:	3-5 jours x homme pour la mise en place du processus
Prérequis	:	dividende de sobriété calculé (Facette 7), tableau de bord du donut opérationnel, processus de priorisation des projets
Critères de succès	:	– 100 % du dividende de sobriété réinvesti dans des projets donut. – Lien sobriété-donut communiqué et compris par les équipes. – Amélioration mesurable du positionnement dans le donut.

Action 5 : publier la « Déclaration d'Interdépendance numérique »

Objectif : formaliser votre engagement envers le bien commun et inspirer d'autres organisations

Méthode :

1. Rédiger une « Déclaration d'Interdépendance numérique » inspirée de la Déclaration d'Interdépendance de l'Agile Manifesto [116, 117], mais pour le bien commun.

2. Inclure des principes concrets qui guident les décisions.

3. Publier et inviter d'autres organisations à la signer.

4. Créer un mouvement collectif autour de cette déclaration.

Exemple de Déclaration d'Interdépendance numérique :

> Nous reconnaissons que notre résilience dépend de celle de notre écosystème. Nous nous engageons à :
> **Mesurer** notre succès à notre contribution au bien commun, pas seulement à notre profit individuel.
> **Ne jamais optimiser** notre organisation au détriment du collectif, mais chercher des solutions vertueuses.
> **Partager** nos ressources inutilisées (matériel, composants, connaissances) avec notre écosystème.
> **Prospérer** dans l'espace juste et sûr du donut, entre un plancher social et un plafond écologique.
> **Dire « non »** au confort qui détruit, pour dire « oui » à la robustesse qui régénère.
> **Inspirer** par l'exemple, en partageant nos apprentissages et nos échecs.
> **Construire** une résilience collective, car sans fournisseurs, clients et compétences pérennes, nous ne le sommes pas.
> Cette déclaration est notre boussole stratégique. Elle guide toutes nos décisions.
> Signataires : [Liste des organisations]

Délai de mise en œuvre	:	2-3 mois pour la rédaction 6-12 mois pour créer le mouvement
Effort estimé	:	5-10 jours x homme pour la rédaction puis effort continu d animation
Prérequis	:	vision donut mature, réseau de partenaires engagés, validation de la direction
Critères de succès	:	– Déclaration publiée et signée par l'organisation. – Au moins 5 organisations signataires la première année. – Mouvement collectif visible et actif.

ROI (conceptuel) : le dividende de sens

Le ROI de la vision donut ne se chiffre pas uniquement en euros économisés, mais en licence sociale d'opérer renforcée. Voici la méthode d'évaluation en trois étapes que nous avons développée.

Étape 1 : Identifier les coûts actuels des services hors du donut

Pour chaque service de votre zone verte, évaluez :

- Sa contribution au plancher social (satisfait-il un besoin humain fondamental ?).
- Son impact sur le plafond écologique (respecte-t-il les limites planétaires ?).
- Le coût total de possession (licences, infrastructure, maintenance, énergie).
- Les risques réputationnels et réglementaires associés.

Étape 2 : Estimer les gains de l'alignement sur le donut

Au-delà des économies directes, l'adoption de la vision donut génère des bénéfices indirects :

- Amélioration de la licence sociale d'opérer (droit de mener vos activités accordé par la société).
- Renforcement de l'attractivité employeur (réduction du turnover, attraction des talents).
- Anticipation des évolutions réglementaires (réduction des risques de sanctions).
- Amélioration de la réputation (nouveaux clients, partenariats).

Étape 3 : Calculer le dividende net

$$Dividende\ de\ sens = (Économies\ directes + Valeur\ des\ gains\ indirects) - Coût\ de\ mise\ en\ place\ de\ la\ vision\ donut$$

M.5 Conclusion : de la résilience individuelle à l'inspiration de la collectivité

Ce voyage à travers les trois facettes du Tour 3 vous a transformé. Vous ne faites plus que consommer simplement du numérique, vous en êtes devenu l'architecte conscient et une organisation inspirante.

Tableau de synthèse des trois facettes

Facette	7	8	9
Mécanisme	Verrouillages socio-techniques et Dépendance au sentier (Path Dependency)	Fragilités géopolitiques Fragilités physiques/climatiques face à l'incertitude environnementale	Impacts sociétaux dans un contexte d'incertitude croissante
Scénario	La crise de confiance généralisée	La rupture géopolitique	La crise de confiance généralisée
Principe	Sobriété stratégique	Circularité collective	Vision donut
Métriques	nº 12 — Ratio de sobriété	nº 13 — Impact commun	
Actions	Instaurer la « Matrice d'arbitrage » Adopter des « Politiques de désengagement » (Sunset Policies) Adapter la production avec la méthode TELED Communiquer le réinvestissement Pratiquer la « Sobriété offensive » Adopter la règle du « 1 pour 3 »	Création de la Digital Urban Mine collective Adopter une gouvernance de bien commun Viser l'impact sociétal, pas seulement économique Adresser les défis pratiques	Publier le « Tableau de bord du donut » Institutionnaliser le « Test du donut » Communiquer votre vision donut Réinvestir le dividende de sobriété dans le donut Publier la « Déclaration d'Interdépendance numérique »

Vous êtes devenu votre propre Oseja numérique

Comme Oseja de Sajambre a choisi l'autonomie énergétique pour garantir sa résilience et partager son électricité avec les villages voisins, vous avez choisi l'autonomie numérique pour garantir votre robustesse et partager vos ressources avec votre écosystème.

Vous avez appris à :

Choisir l'essentiel plutôt que d'accumuler le superflu.

Partager vos ressources plutôt que de les gaspiller.

Inspirer par l'exemple plutôt que de subir les crises.

Vous êtes devenu une source d'inspiration qui ne se contente pas de gérer ses propres actifs, mais qui comprend que la vraie résilience est collective. Vous avez créé une interdépendance choisie qui renforce tout l'écosystème.

Le chemin du leadership ne fait que commencer

Mais le chemin ne fait que commencer. Il est exigeant, car il demande du courage, de la lucidité et de la persévérance. C'est le seul qui soit véritablement porteur de sens et de pérennité.

Montrez au monde qu'un autre numérique est possible : plus sobre, plus robuste, plus solidaire, plus juste. Un numérique qui ne sert pas la technologie, mais qui sert l'humanité.

Comme Oseja éclaire la voie vers l'autonomie énergétique, vous éclairez maintenant la voie vers l'autonomie numérique. D'autres villages vous regardent et s'inspirent de votre exemple. À vous de continuer à montrer le chemin.

Vous êtes devenu votre propre Oseja numérique. Et ce n'est que le début. Le Tour 4 vous attend pour aller plus loin.

---

[116] Kent Beck et al. *Manifeste pour le développement Agile de logiciels*. 2001. URL : https://agilemanifesto.org/iso/fr/manifesto.html.

[117] Kent Beck et al. *Déclaration d'interdépendance*. 2005. URL : https://fr.wikipedia.org/wiki/D%C3%A9claration_d%27interd%C3%A9pendance.

Annexe N

Tour 4 détaillé : intégrer et approfondir

N.1 Introduction : de la compétence à la maîtrise et l'approfondissement

Vous avez parcouru un chemin remarquable. La zone rouge (Tour 1 — Sécuriser) est sécurisée, la zone orange (Tour 2 — Optimiser) optimisée, et la zone verte (Tour 3 — Expérimenter) concentrée sur l'essentiel. Vous avez acquis des outils puissants : les 3U, les 5R, le Donut, la sobriété offensive, la gouvernance des biens communs. Vous pensez peut-être avoir terminé. Mais il reste une étape cruciale : l'approfondissement.

L'approfondissement ne consiste pas à apprendre de nouveaux outils, mais à savoir quand et où appliquer les outils déjà disponibles. L'expertise n'est pas de connaître le plus d'outils, mais de savoir choisir le bon au bon moment, même hors de son contexte d'origine. C'est cette capacité d'orchestration et de contextualisation qui transforme la compétence en maîtrise.

Ce quatrième tour invite à revisiter les trois zones avec un regard neuf, armé de tous les acquis des tours précédents. Vous allez découvrir que les outils appris dans une zone peuvent transformer les autres zones. Vous allez vérifier, approfondir et intégrer.

Important : ce tour est obligatoire pour atteindre la maîtrise, mais ses parties sont flexibles. Chaque organisation choisit son niveau d'ambition. Certaines suggestions sont pragmatiques et accessibles, d'autres sont radicales et réservées aux pionniers. À vous de choisir jusqu'où vous voulez aller.

N.2 Zone verte : contrôle de conformité

Objectif : vérifier que les acquis du Tour 2 ont bien été appliqués

Lors du Tour 3, vous avez rationalisé votre zone verte avec la sobriété stratégique, la Digital Urban Mine et le Donut. Mais avez-vous bien intégré les outils fondamentaux du Tour 2 ? Les 3U (Utile, Utilisable, Utilisé) et les 5R (Refuser, Réduire, Réemployer, Réparer, Recycler) sont des outils puissants qui auraient dû être appliqués dès le Tour 3. Si vous l'avez fait, cette section sera un simple contrôle de conformité. Si vous ne l'avez pas fait, c'est le moment de corriger et d'améliorer.

Checklist rapide : avez-vous appliqué les acquis du Tour 2 ?

Reprenez la liste des services de confort (zone verte) et posez-vous ces questions :

- Les 3U (Audit d'utilité) — avez-vous :
  - mesuré le taux d'utilisation réel de chaque service de confort ?
  - évalué l'utilité métier de chaque service avec un score 3U ?
  - vérifié l'utilisabilité (complexité, formation nécessaire) ?
  - décommissionné les services avec un score 3U trop faible ?
- Les 5R (Circularité) — avez-vous :
  - refusé de nouveaux services de confort non essentiels ?
  - réduit les fonctionnalités superflues des services existants ?
  - réemployé des composants issus de services décommissionnés ?
  - réparé plutôt que remplacé le matériel de la zone verte ?
  - recyclé (via la mine) les équipements obsolètes ?
- Le Dividende de Sobriété — avez-vous :
  - calculé les économies réalisées en décommissionnant les services inutiles ?
  - réinvesti ce dividende dans les zones rouge et orange ?

Résultat attendu

Si vous avez répondu positivement à la majorité des questions, c'est parfait. Votre zone verte est bien rationalisée avec les outils du Tour 2. Vous pouvez passer à la zone orange avec confiance, tout en n'oubliant pas de continuer le travail de rationalisation de votre zone verte.

Si vous avez répondu à moins de la moitié, vous avez probablement fait le Tour 3 de manière trop philosophique, sans pragmatiquement appliquer les outils du Tour 2. Avant de passer à la zone suivante, il serait bien de mener l'audit 3U et les 5R de manière systématique. Référez-vous à l'annexe du Tour 2 pour les méthodes détaillées.

Temps estimé pour ce contrôle : quelques heures (l'audit est rapide, et ne nécessite pas de nouvelles actions si le travail a déjà été fait)

N.3 Zone orange : approfondissement radical

Objectif : aller plus loin que le Tour 2 avec les acquis du Tour 3

Lors du Tour 2, vous avez optimisé votre zone orange avec les 3U, les 5R, la Digital Enterprise Mine et l'antifragilité. C'était déjà un travail considérable. Mais le Tour 3 a apporté des notions encore plus puissantes : la sobriété offensive, la gouvernance des biens communs (Ostrom), et le Donut. Ces notions ont été introduites dans le Tour 3 pour la zone verte, mais certaines, issues du Tour 2, ont aussi été renforcées, poussées et expérimentées dans des contextes plus larges.

Il est maintenant temps de les appliquer à votre zone orange. Vous allez découvrir que ces notions radicales peuvent transformer vos projets d'optimisation en projets de transformation sociétale et écologique.

Les notions du Tour 3 à appliquer à la zone orange

La sobriété offensive : partagez vos optimisations

Dans le Tour 3, vous avez appris que la sobriété devient contagieuse et désirable quand elle est partagée. Appliquez ce principe à votre zone orange.

Question : vos optimisations bénéficient-elles seulement à votre organisation, ou à tout votre écosystème ?

Action : créez un « GitHub de l'optimisation » où vous partagez publiquement vos meilleures pratiques :

Protocoles de test pour la réutilisation de composants.

Scripts d'automatisation pour réduire la charge cognitive.

Configurations low-tech pour prolonger la durée de vie du matériel.

Méthodes d'évaluation de l'impact écologique de vos projets.

Lancez un challenge territorial : « Qui peut réduire de 20 % la consommation énergétique de sa zone orange en 6 mois ? » Partagez vos résultats, vos échecs, vos apprentissages. Rendez la sobriété désirable en montrant qu'elle est source de performance, et non de privation.

Résultat : vous transformez votre optimisation individuelle en mouvement collectif. Votre direction inspire et prouve que la sobriété est contagieuse.

La gouvernance des biens communs (Ostrom) : transformez vos projets en communs

Dans le Tour 3, vous avez appris à créer une Digital Urban Mine collective avec une gouvernance inspirée d'Elinor Ostrom. Appliquez ce principe à d'autres projets de votre zone orange.

Question : quels projets de votre zone orange pourraient devenir des biens communs numériques ?

Exemple : vous développez une solution de gestion de stock plus résiliente. Au lieu de la garder pour vous, proposez-la en open source à d'autres acteurs de votre secteur. Créez une gouvernance collective inspirée des 8 principes d'Ostrom :

Frontières clairement définies : qui peut utiliser la solution ? Qui peut contribuer ?

Règles adaptées aux conditions locales : chaque organisation peut adapter la solution à ses besoins.

Arrangements de choix collectif : les utilisateurs participent à la définition des évolutions.

Surveillance : transparence totale sur l'utilisation et les contributions.

Sanctions graduées : les passagers clandestins (qui utilisent sans contribuer) sont identifiés et encouragés à contribuer ; toujours agir dans la bienveillance pour inspirer.

Mécanismes de résolution des conflits : processus clair pour arbitrer les désaccords.

Reconnaissance du droit d'organisation : les autorités externes respectent l'autonomie du commun.

Entreprises imbriquées : le commun s'intègre dans un écosystème plus large de communs.

Résultat : vous renforcez la résilience de toute votre chaîne de valeur, pas seulement de votre organisation. Vous créez un écosystème d'interdépendance choisie ; elle n'est plus subie et donc renforce votre robustesse.

Le donut de Kate Raworth : une boussole pour chaque projet

Dans le Tour 3, vous avez appris à utiliser le Donut pour questionner les services de confort. Maintenant, appliquez-le à chaque projet de votre zone orange.

Question : ce projet d'optimisation respecte-t-il le Donut ?

Plancher social : ce projet contribue-t-il à satisfaire un besoin humain fondamental (accès, éducation, santé, équité) ? Ou vise-t-il seulement l'efficacité opérationnelle ?

Plafond écologique : ce projet respecte-t-il les limites planétaires (énergie, eau, matériaux, déchets) ? Ou optimise-t-il au prix d'une augmentation de l'empreinte écologique ?

Exemple : vous optimisez votre CRM pour traiter plus de données plus vite. Appliquez le Donut :

Plancher social : ce CRM améliore-t-il l'expérience client (satisfaction, accessibilité) pour réduire la fracture numérique ? Ou sert-il seulement à vendre plus ? Si tel est le cas, est-ce que les produits vendus préviennent ou combattent les insuffisances ou les dépassements ?

Plafond écologique : cette optimisation consomme-t-elle plus d'énergie (paradoxe de Jevons) ? Ou réduit-elle l'empreinte par transaction ? Crée-t-elle une opportunité pour limiter les dépassements ?

Action : Créez un « Dashboard Donut » pour vos 5 principaux projets de la zone orange. Pour chaque projet, évaluez :

Contribution au plancher social ou au plafond écologique : impact positif sur les besoins humains fondamentaux ou les limites planétaires

Impact sur le plafond écologique ou le plancher social : accroissement des dépassement de limites planétaires ou des insuffisances du plancher social

Grille de décision :

- Si les contributions dépassent les impacts → Continuez et amplifiez.
- Sinon → Repensez ou abandonnez.

Les projets à faible contribution sociale et fort impact écologique doivent faire l'objet d'un arbitrage pour être repensés ou abandonnés, ou arbitrés en pleine conscience.

Résultat attendu

Après cet approfondissement, votre zone orange n'est plus seulement optimisée (Tour 2), elle est aussi alignée avec vos convictions profondes (Tour 3). Vos projets d'optimisation deviennent des projets de transformation sociétale et écologique. Vous ne cherchez plus seulement la performance, mais à préserver, à restaurer, voire à régénérer.

Temps estimé pour l'analyse : quelques semaines (selon le nombre de projets à questionner et transformer)

N.4 Zone rouge : simplification pragmatique et aspiration radicale

Objectif : simplifier d'abord, questionner ensuite

Votre zone rouge est votre cœur de métier, vos services critiques. Lors du Tour 1, vous l'avez sécurisée avec la résilience organisée, la redondance, technique ou géographique et la non-régression. C'était nécessaire et précieux. Mais maintenant que vous avez acquis les outils du Tour 2 (3U, 5R, antifragilité) et les convictions du Tour 3 (Donut, sobriété), vous pouvez aller plus loin.

Cette section se divise en deux parties :

Partie recommandée : simplifier la zone rouge avec les outils pragmatiques du Tour 2

Partie optionnelle : questionner la zone rouge avec les convictions radicales du Tour 3 (pour les pionniers)

Important : la zone rouge est sacrée (elle touche à votre cœur de métier, avec une numérisation forte), mais elle ne devrait pas être intouchable. Toutefois, si vous ne vous sentez pas suffisamment mature pour la revisiter, patientez, la maturité viendra plus tard. Ne forcez pas cette étape.

Partie 1 : simplification avec les 3U et les 5R

Le test de l'utilité : même dans le critique, tout n'est pas vital

Vous avez sécurisé votre zone rouge, mais l'avez-vous simplifiée ? Un service critique comme un ERP peut contenir des centaines de fonctionnalités. Sont-elles toutes réellement vitales ?

Question : même dans la zone rouge, toutes les fonctionnalités sont-elles Utiles, Utilisables, Utilisées ?

Exercice : appliquez la grille 3U à 2 principaux services critiques (ERP, CRM, infrastructure réseau…). Pour chaque fonctionnalité :

Utilisé : quel est le taux d'utilisation réel ? (logs, analytics)

Utile : quelle est la contribution métier ? (impact sur le CA, la satisfaction client, la productivité)

Utilisable : quelle est la complexité ? (formation nécessaire, taux d'erreur, charge cognitive)

Résultat : vous découvrirez probablement que 20 à 30 % des fonctionnalités des services critiques ont un score 3U faible. Elles sont candidates à la simplification.

Action : désactivez les fonctionnalités inutiles (ou créez des profils simplifiés). Vous réduirez la surface d'attaque, la charge cognitive et les coûts de maintenance. Votre zone rouge devient plus robuste parce que plus simple.

Le test de la circularité : appliquer les 5R à la zone rouge

Vous avez appliqué les 5R aux zones orange et verte. Pourquoi pas à la zone rouge ?

Question : peut-on appliquer les 5R à la zone rouge sans compromettre la criticité ?

Exemples :

Refuser :

- refusez les évolutions non critiques qui ajoutent de la complexité sans valeur. Questionnez chaque nouvelle fonctionnalité : est-elle vraiment indispensable ? Est-ce que le principe de non-régression peut s'appliquer à cette fonctionnalité ?

Réduire :

- réduisez le nombre de serveurs en consolidant (virtualisation, conteneurisation), en substituant avec des alternatives low-tech, tout en maintenant la redondance nécessaire.

- lors des évolutions, réduisez le nombre de fonctionnalités proposées en vous aidant des 3U, réduisez les au bon public cible…

Résultat : votre zone rouge devient plus sobre et plus autonome. Votre dépendance aux chaînes d'approvisionnement mondiales se réduit, ce qui renforce la résilience face aux ruptures géopolitiques.

Le test de l'antifragilité : entraînez votre zone rouge

Vous avez appliqué l'antifragilité à votre zone orange (Tour 2, Facette 6) ; vous avez découvert ses bénéfices et mesurez l'apport important pour la sérénité de vos équipes et de vous-même. Appliquez-la maintenant à votre zone rouge, à la seule condition d'être en pleine confiance pour faire suite à votre apprentissage en zone orange. Si ce n'est pas le cas, patientez et continuez d'acquérir de la maturité sur ce sujet.

Question : avez-vous rendu la panne si banale que vos équipes n'en ont plus peur ?

Action : mettez en place des « Chaos Monkey » sur les services critiques, provoquez des pannes contrôlées régulièrement, organisez des post-mortems constructifs, mesurez votre MTTR (temps de récupération moyen) et cherchez à le réduire.

Protocole de Chaos Engineering pour la zone rouge :

- Définir l'état stable : quels indicateurs montrent que le système fonctionne normalement ?

- Hypothèse : « Le système restera stable même si [tel événement] se produit »

- Injection de chaos : provoquez l'événement (panne d'un serveur, latence réseau, corruption de données)

- Observation : le système est-il resté stable ? Quel a été le MTTR ?

- Apprentissage : qu'avons-nous appris ? Comment améliorer ?

- Automatisation : intégrez ce test dans votre pipeline CI/CD (Continuous Integration/Continuous Delivery)

Résultat : votre zone rouge n'est plus un sanctuaire intouchable que l'on protège avec anxiété. Elle devient un muscle que l'on entraîne en permanence. La robustesse de la zone rouge n'est plus passive, elle est active et dynamique.

Partie 2 : questionnement radical avec le donut

Avertissement : cette partie est réservée aux organisations les plus avancées. Les questions posées sont radicales et peuvent remettre en question des choix critiques. Si la vôtre n'est pas prête, concentrez-vous sur la Partie 1 (simplification pragmatique) ; cette partie 2 viendra naturellement quand vous aurez acquis toute la maturité nécessaire pour la dérouler.

Le donut appliqué à la zone rouge : une question de sens

Vous avez appliqué le Donut aux zones verte et orange. Osez maintenant l'invoquer pour votre zone rouge.

Questions radicales :

Plancher social : votre ERP, votre CRM, votre infrastructure critique contribuent-ils réellement à satisfaire un besoin humain fondamental ? Ou servent-ils seulement à maximiser le profit ?

Plafond écologique : votre infrastructure critique respecte-t-elle les limites planétaires ? Ou consomme-t-elle des ressources de manière insoutenable ?

Résultat : si vous allez jusque-là, vous transformez votre zone rouge en un modèle de sobriété et de responsabilité. Vous prouvez que même le critique peut être sobre. Votre organisation devient une source d'inspiration pour tout votre secteur.

Temps estimé pour la Partie 1 : 2-3 semaines (simplification pragmatique)

Temps estimé pour la Partie 2 : variable (questionnement radical, selon votre ambition)

N.5 Conclusion : la spirale intégrée pour atteindre la maîtrise

Vous avez terminé le quatrième tour. Vous avez vérifié que les acquis du Tour 2 ont bien été appliqués dans votre zone verte. Vous avez approfondi votre zone orange avec les notions radicales du Tour 3. Vous avez simplifié votre zone rouge avec les outils pragmatiques du Tour 2, et peut-être même questionné avec les convictions du Tour 3.

Vous n'êtes plus en phase d'apprentissage à découvrir et à apprendre les outils. Vous avez dépassé la pratique qui applique les outils dans leur contexte d'origine. Vous avez approfondi votre maîtrise : vous savez quand et où appliquer les bons outils, même hors de leur contexte. Vous savez choisir entre pragmatisme et radicalité selon votre maturité et votre ambition.

La spirale est intégrée

La spirale n'est plus un guide externe que vous suivez. Elle est devenue votre boussole intérieure. Face à toute nouvelle technologie, à toute nouvelle crise, à toute nouvelle opportunité, vous avez les réflexes pour l'analyser à travers les trois filtres :

1. Le filtre du critique (zone rouge) : est-ce que cela touche à mon cœur de métier ? Comment le sécuriser et le simplifier sans le fragiliser ?

2. Le filtre de l'important (zone orange) : est-ce que cela améliore ma production de manière durable et responsable ?

3. Le filtre du confort (zone verte) : est-ce que cela en vaut vraiment le coût ? Quelles ressources puis-je libérer en y renonçant ?

Ces trois filtres ne sont pas séquentiels, ils sont simultanés. Vous les appliquez en parallèle, vous les faites dialoguer. C'est cela, la maîtrise.

Maturité, pragmatisme et inspiration

Vous avez parcouru les quatre tours de la spirale. Vous avez acquis la compétence (Tours 1-3) et approfondi votre maîtrise (Tour 4). Vous êtes maintenant capable de :

Protéger ce qui est vital (Tour 1),

Optimiser ce qui est important (Tour 2),

Transformer ce qui procure du confort (Tour 3),

Intégrer tous ces acquis de manière fluide et contextuelle (Tour 4).

Vous ne subissez plus seulement les contraintes. Vous ne résistez plus seulement aux chocs. Vous transformez les contraintes en opportunités, et inspirez son écosystème, prouvant que performance et responsabilité ne sont pas contradictoires. La spirale ne s'arrête jamais. Elle est le moteur de votre amélioration continue et de votre pertinence dans un monde en perpétuel changement. Votre organisation est devenu l'Oseja numérique : un modèle de résilience, de sobriété et de leadership pour votre secteur.

Félicitations. Vous avez approfondi votre maîtrise de la robustesse numérique. Continuez !

Partie IV

INDEX

Annexe O

Glossaire

Glossaire

Backdoor (Porte dérobée) Accès secret et dissimulé à un système informatique, installé par un attaquant. Une backdoor lui permet de revenir plus tard, de voler des données ou de prendre le contrôle du système, même si le point d'entrée initial a été corrigé. Enjeu pour la direction : même après avoir contenu une cyberattaque, votre système peut rester compromis et sous la menace d'une récidive si toutes les portes dérobées n'ont pas été découvertes et éliminées. 133

Deepfake (Hypertrucage) Contenu média (vidéo, audio) généré ou modifié par une intelligence artificielle pour faire dire ou faire à une personne quelque chose qu'elle n'a jamais dit ou fait. Les deepfakes modernes sont si réalistes qu'ils sont presque impossibles à distinguer de la réalité à l'œil nu. Enjeu pour la direction : risque majeur de désinformation, d'usurpation d'identité (de vous-même ou de vos employés), de fraude ("fraude au président") et d'atteinte dévastatrice à la réputation de votre entreprise. 146

Dépendance au sentier (Path Dependency) Principe selon lequel les décisions prises dans le passé limitent fortement les options disponibles aujourd'hui, même si ces décisions ne sont plus optimales. Une fois qu'une technologie ou un fournisseur est adopté à grande échelle, il devient extrêmement coûteux et complexe d'en changer. Enjeu pour la direction : votre entreprise peut être « prisonnière » d'un fournisseur ou d'une technologie (ex : un seul fournisseur de cloud), vous rendant vulnérable à ses hausses de prix, à ses failles de sécurité ou à ses changements de stratégie. 29, 43, 51, 63, 130, 134, 137, 142, 144, 147, 195, 204, 212, 240, 247, 276

Licence sociale d'opérer Elle désigne un processus par lequel une entreprise ou une organisation se donne les moyens d'obtenir l'accord tacite le plus large possible des parties prenantes et populations concernées pour le développement ou la réalisation d'un projet ou d'une activité économique. (https ://youmatter.world/fr/definition/licence-to-operate-definition-enjeux-methode/). 52, 63, 67, 70, 73, 130

Mine urbaine (urban mine) La mine urbaine désigne la récupération de matières premières à partir de déchets urbains, tels que les appareils électroménagers ou les bâtiments, pour les réutiliser ou les recycler. Cette approche contribue directement à la réduction de l'empreinte carbone en évitant l'exploitation de nouvelles ressources naturelles et en minimisant les déchets.. 55

MTTR (Mean Time To Recovery) Le temps moyen jusqu'à la réparation (MTTR) est le temps moyen nécessaire à la réparation d'un système, généralement technique ou mécanique, incluant les contrôles de bon fonctionnement.. 206, 229

Point de défaillance unique (Single Point of Failure / SPOF) Composant d'un système dont la défaillance entraîne l'arrêt de l'ensemble du système. Il peut s'agir d'un serveur critique, d'un fournisseur unique, ou même d'une seule personne détenant une compétence clé. Enjeu pour la direction : identifier et réduire les SPOF est un objectif stratégique majeur pour garantir la continuité de votre activité. Un SPOF non identifié est une bombe à retardement pour votre résilience. 42, 48, 57, 100, 130, 187, 188, 191, 229

Ransomware (Rançongiciel) Type de logiciel malveillant qui chiffre les fichiers d'un système informatique, les rendant inutilisables. Les attaquants exigent ensuite le paiement d'une rançon, généralement en cryptomonnaie, en échange de la clé de déchiffrement. Enjeu pour la direction : risque de paralysie totale de l'activité, de perte de données critiques et d'extorsion financière, avec le dilemme de payer la rançon (sans garantie de résultat) ou de faire face à une reconstruction longue et coûteuse. 27, 132, 133

Sideloading (Chargement latéral) Installation d'une application sur un appareil (comme un smartphone) en contournant le magasin d'applications officiel (ex : l'App Store d'Apple ou le Google Play Store). Le Digital Markets Act (DMA) en Europe force, par exemple Apple à autoriser cette pratique. Enjeu pour la direction : peut représenter une opportunité (plus de liberté pour distribuer vos applications d'entreprise) mais également un risque de sécurité (les applications non vérifiées peuvent contenir des malwares). 142

VUCA Acronyme de Volatility, Uncertainty, Complexity and Ambiguity. Il est utilisé pour décrire un environnement en perpétuelle évolution, totalement imprévisible, fortement complexe et toujours ambigu. 13, 126

Wiper (Logiciel effaceur) Logiciel malveillant particulièrement destructeur dont le seul but est d'effacer ("to wipe") de manière irréversible les données des systèmes qu'il infecte. Contrairement à un ransomware, il n'y a aucune intention de rendre les données en échange d'une rançon. Enjeu pour la direction : c'est le scénario du pire. Un wiper ne vise pas le gain financier mais la destruction pure et simple, pouvant anéantir des années de données. 132, 133

Annexe P

Bibliographie complète

[1] HPE. *What is IT resilience ?* URL : https://www.hpe.com/us/en/what-is/it-resilience.html.

[2] Olivier Hamant. *Pourquoi parler de robustesse et non de résilience ?* larobustesse.org. URL : https://larobustesse.org/?PourquoiParlerDeRobustesseEtNonDeResilie.

[3] ENTSO-E. *Factual Report : 28 April 2025 Iberian Blackout*. European Network of Transmission System Operators for Electricity, 2025. URL : https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/.

[4] Nicolás Boullosa. *The Asterix village in the dark : resilience in a blacked-out world*. Avr. 2025. URL : https://faircompanies.com/articles/the-asterix-village-in-the-dark-resilience-in-a-blacked-out-world/.

[5] One Media. *Le village autonome qui a échappé au blackout électrique*. 2025. URL : https://onemedia.fr/actualite/le-village-autonome-qui-a-echappe-au-grand-blackout-electrique/.

[6] James Nelson et al. "Statistical development of microgrid resilience during islanding operations". In : *Applied Energy* 279 (2020), p. 115733. URL : https://www.sciencedirect.com/science/article/pii/S0306261920312150.

[7] Mehdi Khamassi et al. "Behavioral regulation and the modulation of information coding in the lateral prefrontal and cingulate cortex". In : *Cerebral Cortex* 25.9 (2015), p. 3197-3218. DOI : 10.1093/cercor/bhu114. URL : https://doi.org/10.1093/cercor/bhu114.

[8] Opteamis. *La dette technique : le passif invisible du numérique*. 2025. URL : https://www.opteamis.com/la-dette-technique-le-passif-invisible-du-numerique/.

[9] McKinsey and Company. *Building Resilience : The CEO's new imperative*. Rapp. tech. McKinsey et Company, 2023.

[10] Boston Consulting Group. *Leading Through Permacrisis*. Rapp. tech. Boston Consulting Group, 2023.

[11] Gartner. *Cloud Computing Trends and Future Direction*. Rapp. tech. Gartner, 2024.

[12] Reuters. *Kaseya Ransomware Attack : Impact Assessment*. 2021.

[13] Okta. *Business at Work Report*. Rapp. tech. Okta, 2023.

[14] Salesforce. *State of the Connected Customer*. Rapp. tech. Salesforce, 2024.

[15] SWIFT. *Annual Traffic Report*. Rapp. tech. SWIFT, 2023.

[16] Parametrix. *CrowdStrike's Impact on the Fortune 500*. Analyse économique estimant les pertes directes à 5,4 milliards de dollars pour les entreprises du Fortune 500 (hors Microsoft). 24 juill. 2024. URL : https://www.parametrixinsurance.com/reports-white-papers/crowdstrikes-impact-on-the-fortune-500.

[17] Z2Data. *Quartz Mine Disruption in Spruce Pine, NC, Threatens Semiconductor Manufacturing*. Rapp. tech. Z2Data, 2024.

[18] Le Monde. *Aux Etats-Unis, l'IA bouleverse déjà le marché du travail et les prédictions de jobs apocalypse se multiplient*. 2025.

[19] IDC. *Worldwide Digital Transformation Spending Guide*. Rapp. tech. IDC, 2024.

[20] Evgeny Morozov. *To Save Everything, Click Here*. PublicAffairs, 2013. URL : https://academic.oup.com/jdh/article-abstract/27/1/111/474220?login=false.

[21] Les Échos. *Comment Google utilise l'intelligence artificielle pour faire baisser sa facture d'électricité*. 2018. URL : https://www.lesechos.fr/2016/07/comment-google-

utilise-lintelligence-artificielle-pour-faire-baisser-sa-facture-delectricite-218671.

[22] NATURE. “Accurate structure prediction of biomolecular interactions with AlphaFold 3”. In : *Nature* (2024). URL : https://www.nature.com/articles/s41586-024-07487-w.

[23] David GRAEBER. *The Utopia of Rules*. 2015. URL : https://files.libcom.org/files/David_Graeber-The_Utopia_of_Rules_On_Technology_St.pdf.

[24] RESILIENT CITIES NETWORK. *Building Wellington’s Resilient Community Water Access*. 2020. URL : https://resilientcitiesnetwork.org/wellington-water-security/.

[25] BBC. *Floating bamboo houses keep this indigenous tribe safe*. 2024. URL : https://www.bbc.com/future/article/20240531-the-floating-houses-built-to-withstand-typhoons-and-flooding-in-the-philippines.

[26] UNITED NATIONS DEVELOPMENT PROGRAM. *Learning from local ingenuity – how simple reed fencing has unlocked a solution to rising sea levels in Egypt*. 2022. URL : https://www.undp.org/arab-states/blog/learning-local-ingenuity-how-simple-reed-fencing-has-unlocked-solution-rising-sea-levels-egypt/.

[27] LEMAGIT. *L’affaire Broadcom VMware : le guide pour comprendre*. 2025. URL : https://www.lemagit.fr/essentialguide/Laffaire-Broadcom-VMware.

[28] INSTITUTE FOR SUSTAINABLE IT. *La règle des 3U*. URL : https://fr.wiki.isit-europe.org/nr/Utile_Utilisable_Utilis%C3%A9.

[29] RACE FOR WATER. *La règle des 5R*. 2024. URL : https://www.raceforwater.org/fr/nous-soutenir/eco-gestes/.

[30] LE WEB VERT. *La loi d’erooM, de Tristan Nitot*. 2024. URL : https://www.lewebvert.fr/blog/2024-06-20-interview-tristan-nitot/.

[31] BOAVIZTA. *Le diagnostic rapide EROOM*. 2024. URL : https://www.boavizta.org/eroom/diagnostic-rapide.

[32] INTERNATIONAL COPPER ASSOCIATION. *Mines urbaines*. URL : https://internationalcopper.org/fr/policy-focus/climate-environment/urban-mining/.

[33] CENTRE DE L’HORMÈSE. *Qu’est-ce que l’Hormèse ?* 2024. URL : https://www.hormese.com/a-propos/hormese.

[34] 37SIGNALS. *Getting Real : The smarter, faster, easier way to build a successful web application*. URL : https://basecamp.com/gettingreal.

[35] Elinor OSTROM. *Governing the Commons*. Cambridge University Press, 1990.

[36] Kate RAWORTH. *Doughnut Economics : Seven Ways to Think Like a 21st-Century Economist*. Chelsea Green, 2017.

[37] *Amsterdam, ville donut*. URL : https://amsterdamdonutcoalitie.nl/.

[38] ALLIANZ. *Risk Barometer 2025*. Allianz Global Corporate and Specialty, division assurance des grandes entreprises. Enquête annuelle auprès de 3 778 experts en gestion des risques dans 106 pays identifiant les principaux risques commerciaux mondiaux (cyber-incidents, interruptions d’activité, catastrophes naturelles). 2025. URL : https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf.

[39] AXA. *Future Risks Report 2024*. AXA, groupe d’assurance mondial, en partenariat avec Ipsos. Enquête auprès de 3 000 experts et 20 000 citoyens explorant les risques émergents et leur interconnexion dans un contexte de polycrisis (pollution, cybersécurité, changement climatique, éthique technologique). 2024. URL : https://www-axa-com.cdn.axa-contento-118412.eu/www-axa-com/dad8b74b-e921-4b2d-bea8-2f7dabe369aa_axa_futurerisksreport_2024_va.pdf.

[40] CENTER FOR CREATIVE LEADERSHIP. *Leading Beyond Barriers : Creating Impact in an Age of Polycrisis*. Center for Creative Leadership, organisation à but non lucratif leader mondial du développement du leadership depuis 50+ ans. Identifie les capacités de leadership critiques pour naviguer dans les crises interconnectées et les barrières psychologiques bloquant le progrès sur les défis globaux. 2025. URL : https://cclinnovation.org/wp-content/uploads/2025/02/leadingbeyondbarriers.pdf.

[41] Cigref. *4 Archétypes de la fonction numérique pour 2040*. Cigref, réseau de 150 grandes entreprises et administrations publiques françaises créé en 1970. Rapport d'orientation stratégique proposant 4 archétypes prospectifs de la fonction numérique à l'horizon 2040 (innovation, résilience, responsabilité, transversalité). 2025. URL : https://www.cigref.fr/rapport-dorientation-strategique-2025-du-cigref-4-archetypes-de-la-fonction-numerique-pour-2040.

[42] European Research Council. *Transformative change for a sustainable future*. European Research Council, organisme de financement de la recherche d'excellence de l'UE créé en 2007. Synthèse de 300+ projets explorant les stratégies innovantes pour un changement transformatif vers la durabilité et l'équité. 2024. URL : https://erc.europa.eu/sites/default/files/2024-12/Transformative-change-for-a-sustainable-future.pdf.

[43] Huan Liu et Ortwin Renn. "Polycrisis and Systemic Risk : Assessment, Governance, and Communication". In : *International Journal of Disaster Risk Science* (2025). Huan Liu (Kyoto University) et Ortwin Renn (Research Institute for Sustainability, expert mondial de la gouvernance des risques). Article de synthèse examinant polycrisis et risque systémique, leurs différences et implications pour la gouvernance et la communication des crises. URL : https://link.springer.com/article/10.1007/s13753-025-00636-3.

[44] Nature. "A systemic risk assessment methodological framework for the global polycrisis". In : *Nature Communications* (2025). Ajay Gambhir (ASRA) et 27 co-auteurs (Stockholm Resilience Centre, Oxford, Edinburgh, PIK). Cadre méthodologique d'évaluation des risques systémiques pour la polycrisis, appliqué aux crises alimentaire et énergétique. Méthodologie disponible via STEER (outil open-access). URL : https://www.nature.com/articles/s41467-025-62029-w.pdf.

[45] OCDE. *États de fragilité 2025*. OCDE, organisation internationale de 38 pays membres. Rapport analysant la fragilité dans 61 pays via un cadre multidimensionnel de 56 indicateurs couvrant 6 dimensions (politique, sociétale, sécuritaire, environnementale, économique, humaine). 25 ans d'expertise sur la fragilité. 2025. URL : https://www.oecd.org/content/dam/oecd/fr/publications/reports/2025/02/states-of-fragility-2025_c9080496/3797ea0f-fr.pdf.

[46] Oxford Poverty and Human Development Initiative. *Resilient Human Development*. Oxford Poverty and Human Development Initiative (OPHI), centre de recherche de l'Université d'Oxford dirigé par Sabina Alkire. Cadre conceptuel sur le développement humain résilient face aux chocs et crises, appliquant une approche multidimensionnelle de la pauvreté et du bien-être. 2025. URL : https://ophi.org.uk/sites/default/files/2025-09/OPHIRP_68a_2025_Resilient_%28Alkire%29.pdf.

[47] PolyCIVIS. *From Polycrisis to Polysolutions*. PolyCIVIS, réseau Jean Monnet de l'alliance universitaire CIVIS (11 universités euro-africaines). Approche interdisciplinaire explorant la polycrisis et proposant des solutions durables via une compréhension systémique de la gouvernance, des systèmes économiques et de la dimension humaine. 2025. URL : https://civis.eu/storage/files/1foundational-brief-polycrisis-and-policy-series-formatted-version2-schreiber-etal-mar-2025.pdf.

[48] Jürgen Scheffran. "Systemic risks and governance of the global polycrisis in the Anthropocene". In : *Global Sustainability* (2025). Jürgen Scheffran (Université de Hambourg, IFSH), expert en sécurité climatique et conflits environnementaux (500+ citations). Analyse la stabilité du nexus climat-conflit-migration-pandémie et les cascades de basculement dans la polycrisis de l'Anthropocène. Intègre recherche sur climat-conflit et risques systémiques. URL : https://www.cambridge.org/core/services/aop-cambridge-core/content/view/95EF7C378D08AD2806659BBACFABBAF5/S2059479825100264a.pdf/systemic_risks_and_governance_of_the_global_polycrisis_in_the_anthropocene_stability_of_the_climateconflictmigrationpandemic_nexus.pdf.

[49] Swiss Re. *SONAR 2024*. Swiss Re Institute, centre de recherche du réassureur mondial. Rapport annuel SONAR identifiant 16 risques émergents via crowdsourcing interne

(résilience des chaînes d'approvisionnement, climat, cyber, isolement social, chaleur extrême). Outil de dialogue avec le secteur pour la gestion proactive des risques. 2024. URL : https://www.swissre.com/institute/research/sonar/sonar2024.html.

[50] Bishoy L. Zaki, Valérie Pattyn et Ellen Wayenberg. "Policymaking in an age of polycrises : emerging perspectives". In : *Policy Design and Practice* (2024). Bishoy L. Zaki, Valérie Pattyn et Ellen Wayenberg (Université de Gand). Collection spéciale développant l'utilité analytique du concept de polycrisis pour la conception des politiques publiques et l'apprentissage politique en temps de crises interconnectées. DOI : 10.1080/25741292.2024.2432048. URL : https://doi.org/10.1080/25741292.2024.2432048.

[51] Henry Farrell et Abraham L. Newman. "Weaponized Interdependence : How Global Economic Networks Shape State Coercion". In : *International Security* 44.1 (2019), p. 42-79. URL : https://direct.mit.edu/isec/article/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic.

[52] Chaire Digital, Gouvernance et Souveraineté. *Souveraineté numérique et crise géopolitique*. 2022. URL : https://www.sciencespo.fr/public/chaire-numerique/2022/12/09/compte-rendu-retour-sur-la-conference-annuelle-2022-souverainete-numerique-et-crise-geopolitique/.

[53] Groupe d'experts intergouvernemental sur l'évolution du climat (GIEC). *Climate Change 2022 : Mitigation of Climate Change*. AR6 Working Group III. 2022. URL : https://www.ipcc.ch/report/ar6/wg3/downloads/report/IPCC_AR6_WGIII_SummaryVolume.pdf.

[54] The Shift Project. *Rapport intermédiaire sur les consommations énergétiques et impacts climatiques des infrastructures numériques*. 2025. URL : https://theshiftproject.org/app/uploads/2025/04/2025_03_06-TSP-Rapport-intermediaire-IA-quelles-infra-num-monde-decarbone.pdf.

[55] The Shift Project. *Intelligence artificielle, données, calculs : quelles infrastructures dans un monde décarboné ?* 2025. URL : https://theshiftproject.org/publications/intelligence-artificielle-centres-de-donnees-rapport-final/.

[56] Steven M. Rinaldi, James P. Peerenboom et Terrence K. Kelly. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". In : *IEEE Control Systems Magazine* 21.6 (2001), p. 11-25. DOI : 10.1109/37.969131. URL : https://doi.org/10.1109/37.969131.

[57] Sobhan Sean Arisian et al. "Cyber risk mitigation in critical supply chains". In : (2025). URL : https://www.researchgate.net/publication/396455676_Cyber_risk_mitigation_in_critical_supply_chains.

[58] Dirk Helbing. "Globally networked risks and how to respond". In : *Nature* 497 (2013), p. 51-59. URL : https://www.nature.com/articles/nature12047.

[59] *S'inspirer de l'épidémiologie pour lutter contre les cybermenaces*. URL : https://www.polytechnique-insights.com/tribunes/digital/sinspirer-de-lepidemiologie-pour-lutter-contre-les-cybermenaces/.

[60] Everett M. Rogers. *Diffusion of Innovations*. 5e éd. Free Press, 2003. URL : https://teddykw2.wordpress.com/wp-content/uploads/2012/07/everett-m-rogers-diffusion-of-innovations.pdf.

[61] Laure Lahaye. *Femmes et vulnérabilité numérique : causes et conséquences*. Soralia, 2022. URL : https://www.soralia.be/accueil/etude-2022-femmes-et-vulnerabilite-numerique-quelles-causes-pour-quelles-consequences/.

[62] Shoshana Zuboff. *The Age of Surveillance Capitalism*. PublicAffairs, 2019. URL : https://www.hbs.edu/faculty/Pages/item.aspx?num=56791.

[63] Peter M. Senge. *The Fifth Discipline : The Art and Practice of the Learning Organization*. Doubleday, 1990.

[64] David A. Kolb. *Experiential Learning : Experience as the Source of Learning and Development*. Prentice Hall, 1984.

[65] Benjamin S. Bloom. *Taxonomy of Educational Objectives : The Classification of Educational Goals*. Longmans, Green, 1956.

[66] Chris Argyris et Donald A. Schön. *Organizational Learning : A Theory of Action Perspective*. Addison-Wesley, 1978.
[67] Stéphane Crozat. *Vers une ataraxie numérique : low-technicisation et convivialité*. 2021. URL : https://aswemay.fr/co/040011.html.
[68] Erik Hollnagel, David D. Woods et Nancy Leveson. *Resilience Engineering : Concepts and Precepts*. Ashgate Publishing, 2006.
[69] Sidney Dekker. *Drift into Failure : From Hunting Broken Components to Understanding Complex Systems*. Ashgate Publishing, 2011.
[70] Nassim Nicholas Taleb. *Antifragile : Things That Gain from Disorder*. Random House, 2012.
[71] Donella H. Meadows. *Thinking in Systems : A Primer*. Chelsea Green Publishing, 2008.
[72] Edgar Morin et Anne Brigitte Kern. *Homeland Earth : A Manifesto for the New Millennium*. Hampton Press, 1999. URL : https://archive.org/details/homelandearthman0000mori.
[73] Adam Tooze. *This is why 'polycrisis' is a useful way of looking at the world right now*. World Economic Forum, 2023. URL : https://www.weforum.org/stories/2023/03/polycrisis-adam-tooze-historian-explains/.
[74] Jean-Claude Juncker. *Speech by President Jean-Claude Juncker at the Annual General Meeting of the Hellenic Federation of Enterprises*. 2016. URL : https://europa.eu/rapid/press-release_SPEECH-16-2293_fr.htm.
[75] Cascade Institute. *What Is a Global Polycrisis ?* Rapp. tech. Cascade Institute, 2022. URL : https://cascadeinstitute.org/wp-content/uploads/2022/04/What-is-a-global-polycrisis-v2.pdf.
[76] F. Schreiber et al. *From Polycrisis to Polysolutions : An Interdisciplinary Approach to Complex Global Challenges*. Foundational Brief. PolyCIVIS, mars 2025. URL : https://civis.eu/storage/files/1foundational-brief-polycrisis-and-policy-series-formatted-version2-schreiber-etal-mar-2025.pdf.
[77] Jürgen Scheffran. "Systemic Risks and Governance of the Global Polycrisis in the Anthropocene". In : *Global Sustainability* (2023). URL : https://www.cambridge.org/core/journals/global-sustainability/article/systemic-risks-and-governance-of-the-global-polycrisis-in-the-anthropocene-stability-of-the-climateconflictmigrationpandemic-nexus/95EF7C378D08AD2806659BBACFABBAF5.
[78] Thomas Homer-Dixon et al. "Global polycrisis : the causal mechanisms of crisis entanglement". In : *Global Sustainability* (2023). URL : https://www.cambridge.org/core/journals/global-sustainability/article/global-polycrisis-the-causal-mechanisms-of-crisis-entanglement/06F0F8F3B993A221971151E3CB054B5E.
[79] World Economic Forum. *Global Risks Report 2024*. Rapp. tech. World Economic Forum, 2024. URL : https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.
[80] IPCC. *Climate Change 2023 : Synthesis Report – Sixth Assessment Report*. Rapp. tech. Intergovernmental Panel on Climate Change, 2023. URL : https://www.ipcc.ch/report/ar6/syr/.
[81] Santa Fe Institute. *Complex Systems and Tipping Points*. 2023. URL : https://www.santafe.edu/events/critical-transitions-in-complex-systems-are-t.
[82] A. Gambhir et al. "A Systemic Risk Assessment Methodological Framework for the Global Polycrisis". In : *Nature Communications* (2024). URL : https://www.nature.com/articles/s41467-025-62029-w.
[83] Nassim Nicholas Taleb. *The Black Swan : The Impact of the Highly Improbable*. Ouvrage de référence sur les événements rares et imprévisibles aux conséquences catastrophiques (cygnes noirs). Random House, 2007.
[84] Lloyd's List. *Ever Given : Suez Canal blockage economic impact*. 2021. URL : https://www.lloydslist.com/LL1137492/The-lessons-and-the-aftermath-of-the-Ever-Given-incident.

[85] Synergy Research Group. *Cloud Market Share Q2 2024*. Rapp. tech. Synergy Research Group, 2024. URL : https://www.srgresearch.com/articles/cloud-market-growth-stays-strong-in-q2-while-amazon-google-and-oracle-nudge-higher.

[86] AWS. *Post-Incident Analysis December 2021*. Rapp. tech. Amazon Web Services, 2021. URL : https://aws.amazon.com/premiumsupport/technology/pes/.

[87] SIA. *Global Semiconductor Industry Report*. Rapp. tech. Semiconductor Industry Association, 2024. URL : https://www.semiconductors.org/wp-content/uploads/2024/05/SIA-2024-Factbook.pdf.

[88] ASTERèS. *La dépendance technologique aux softwares et services cloud américains : une estimation des conséquences économiques en Europe*. Rapp. tech. ASTERèS, 2025. URL : https://www.cigref.fr/wp/wp-content/uploads/2025/04/Etude-Asteres-La-dependance-technologique-aux-services-de-cloud-et-logiciels-americains-avril-2025.pdf.

[89] Les Échos. *Sous pression géopolitique, la Cour pénale internationale tourne la page Microsoft*. Nov. 2025. URL : https://www.lesechos.fr/tech-medias/hightech/sous-pression-geopolitique-la-cour-penale-internationale-tourne-la-page-microsoft-2199143.

[90] TeleGeography. *Submarine Cable Map*. 2024. URL : https://www.submarinecablemap.com/.

[91] Reuters. *Baltic Sea Cable Cuts : Investigation Reports*. Rapports d'enquête couvrant la période 2023-2025. 2023. URL : https://www.reuters.com/world/europe/estonia-probe-sweden-cable-damage-part-baltic-sea-incident-investigation-2023-10-19/.

[92] CISQ. *The Cost of Poor Software Quality in the US*. Rapp. tech. Consortium for Information et Software Quality, 2024. URL : https://www.it-cisq.org/wp-content/uploads/sites/6/2022/11/CPSQ-Report-Nov-22-2.pdf.

[93] Center for Creative Leadership. *Leading Beyond Barriers : Creating Impact in an Age of Polycrisis*. Rapp. tech. Center for Creative Leadership, 2024. URL : https://cclinnovation.org/wp-content/uploads/2025/02/leadingbeyondbarriers.pdf.

[94] S. Alkire. *Resilient Human Development*. Rapp. tech. OPHIRP_68a_2025. Oxford Poverty et Human Development Initiative, 2025. URL : https://ophi.org.uk/sites/default/files/2025-09/OPHIRP_68a_2025_Resilient_%28Alkire%29.pdf.

[95] ICJ. *Principle of Non-Regression in Environmental Law*. 2018. URL : https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/an-international-law-principle-of-nonregression-from-environmental-protections/DFB6236C0504491E00B4174EE6D13186.

[96] IMO. *STCW Convention Requirements*. Rapp. tech. International Maritime Organization, 2023. URL : https://www.imo.org/en/ourwork/humanelement/pages/stcw-conv-link.aspx.

[97] INRAE. *Agriculture Numérique et Résilience*. Rapp. tech. 2024. URL : https://hal.inrae.fr/hal-05290456v1/file/LActu-newsletter-2024.pdf.

[98] IEEE Spectrum. "How IBM Watson Overpromised and Underdelivered on AI Health Care". In : *IEEE Spectrum* (2019). URL : https://spectrum.ieee.org/how-ibm-watson-overpromised-and-underdelivered-on-ai-health-care.

[99] EASA. *Certification Specifications for Large Aeroplanes*. Rapp. tech. European Union Aviation Safety Agency, 2023. URL : https://www.easa.europa.eu/en/document-library/certification-specifications.

[100] Netflix Tech Blog. *Multi-Region Resilience*. 2023. URL : https://netflixtechblog.com/.

[101] Basel Committee. *Principles for Operational Resilience*. Rapp. tech. Bank for International Settlements, 2023. URL : https://www.bis.org/bcbs/publ/d516.htm.

[102] Facebook Engineering. *More details about the October 4 outage*. 2021. URL : https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/.

[103] Netflix. *Chaos Engineering Principles*. 2023. URL : https://www.gremlin.com/community/tutorials/chaos-engineering-the-history-principles-and-practice.

[104] Défenseur des droits. *Rapport sur la dématérialisation des services publics*. Rapp. tech. 2024. URL : https://www.defenseurdesdroits.fr/rapport-dematerialisation-et-inegalites-dacces-aux-services-publics-266.

[105] Signal Blog. *Maintaining Service During the Facebook Outage*. 2021. URL : https://signal.org/blog/.

[106] Queue-it. *Roland Garros Virtual Queue Case Study*. 2024. URL : https://queue-it.com/.

[107] EU Commission. *Streaming Platforms Bandwidth Reduction Agreement*. Rapp. tech. European Commission, 2020. URL : https://commission.europa.eu/strategy-and-policy/coronavirus-response/digital-solutions-during-pandemic_en.

[108] SEC. *Market Circuit Breakers Rules*. Rapp. tech. U.S. Securities et Exchange Commission, 2023. URL : https://www.sec.gov/rules-regulations.

[109] CrowdStrike. *Post-Incident Analysis Report*. Rapp. tech. Rapport officiel post-incident détaillant la mise à jour défectueuse du 19 juillet 2024 qui a affecté 8,5 millions de machines Windows. 2024. URL : https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

[110] Toyota. *Supply Chain Resilience Strategy*. Integrated Report 2023. 2023. URL : https://global.toyota/pages/global_toyota/ir/library/annual/2023_001_integrated_en.pdf.

[111] ERCOT. *Texas Grid Failure Analysis*. Rapp. tech. 2021. URL : https://energy.utexas.edu/research/ercot-blackout-2021.

[112] ANSSI. *Panorama de la cybermenace 2024*. Rapp. tech. Agence nationale de la sécurité des systèmes d'information, 2024. URL : https://cyber.gouv.fr/publications/panorama-de-la-cybermenace-2024.

[113] European Energy Agency. *Datacenter Energy Resilience Report*. Rapp. tech. 2024. URL : https://www.eea.europa.eu/.

[114] Patagonia. *Don't Buy This Jacket*. 2011. URL : https://eu.patagonia.com/fr/fr/stories/planete/activisme/dont-buy-this-jacket-black-friday-and-the-new-york-times/story-18615.html.

[115] e-Estonia. *We have built a digital society and so can you*. URL : https://e-estonia.com/.

[116] Kent Beck et al. *Manifeste pour le développement Agile de logiciels*. 2001. URL : https://agilemanifesto.org/iso/fr/manifesto.html.

[117] Kent Beck et al. *Déclaration d'interdépendance*. 2005. URL : https://fr.wikipedia.org/wiki/D%C3%A9claration_d%27interd%C3%A9pendance.

[118] Celia Paulsen et al. *Criticality Analysis Process Model : Prioritizing Systems and Components*. Rapp. tech. NIST Interagency Report 8179. National Institute of Standards et Technology, 2018. DOI : 10.6028/NIST.IR.8179. URL : https://doi.org/10.6028/NIST.IR.8179.

[119] International Organization for Standardization. *Security and resilience — Business continuity management systems — Requirements*. Rapp. tech. ISO 22301 :2019. ISO, 2019.

[120] National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. Rapp. tech. Special Publication 800-53 Revision 5. NIST, 2020.

[121] Delta Air Lines. *Delta Air Lines Announces September Quarter 2024 Financial Results*. Rapport financier Q3 2024 documentant l'impact de la panne CrowdStrike : plus de 6 000 vols annulés, 500 000 passagers affectés, 500 millions dollars de pertes. 10 oct. 2024. URL : https://ir.delta.com/news/news-details/2024/Delta-Air-Lines-Announces-September-Quarter-2024-Financial-Results/default.aspx.

[122] BBC News. *CrowdStrike : NHS services disrupted by global IT outage*. Documentation médiatique de l'impact sur le système de santé britannique NHS, avec report de milliers d'interventions chirurgicales. 19 juill. 2024.

[123] Sources médias australiennes. *Impact de la panne CrowdStrike sur Woolworths et Coles*. Documentation de la fermeture des caisses automatiques dans les supermarchés australiens suite à la panne. 2024.

[124] NPR. *Spruce Pine just got hit by Helene. The fallout on the tech industry could be huge*. Article documentant le rôle critique de Spruce Pine (80-90% du quartz ultra-pur mondial) et l'impact de l'ouragan Helene. 30 sept. 2024. URL : https://www.npr.org/2024/09/30/nx-s1-5133462/hurricane-helene-quartz-microchips-solar-panels-spruce-pine.

[125] Wired. *Hurricane Helene Will Send Shockwaves Through the Semiconductor Industry*. Analyse approfondie de l'impact de l'ouragan Helene sur les mines de quartz de Spruce Pine et les répercussions sur l'industrie des semiconducteurs. 1er oct. 2024. URL : https://www.wired.com/story/hurricane-helene-shockwaves-semiconductor-industry-microchips-spruce-pine-north-carolina-sand-high-quality-quartz/.

[126] CNN. *Devastation from Hurricane Helene could bring semiconductor supply chain to its knees*. Analyse des experts estimant que les stocks mondiaux de quartz haute pureté seraient épuisés au-delà de trois mois d'arrêt de production. 2 oct. 2024. URL : https://www.cnn.com/2024/10/02/tech/semiconductor-supply-chain-north-carolina-helene.

[127] Defense Logistics Agency. *Supply Chain Illumination in the Department of Defense*. Rapp. tech. Rapport du département de la Défense mentionnant Spruce Pine comme point critique de la chaîne d'approvisionnement en matériaux stratégiques. 13 jan. 2025. URL : https://dbb.defense.gov/Portals/35/Documents/Reports/2025/DBB%20Supply%20Chain%20Illumination%20Report%20CLEARED.pdf.

[128] U.S. Department of Energy. *2023 Critical Materials Assessment*. Rapp. tech. Évaluation des matériaux critiques pour l'énergie et la sécurité nationale, incluant les matériaux nécessaires à la fabrication de semiconducteurs. 27 mai 2023. URL : https://www.energy.gov/sites/default/files/2023-05/2023-critical-materials-assessment.pdf.

[129] White House. *2021–2024 Quadrennial Supply Chain Review*. Rapp. tech. Revue quadriennale des chaînes d'approvisionnement critiques, soulignant que "le marché seul ne peut pas résoudre les vulnérabilités". Déc. 2024. URL : https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/12/20212024-Quadrennial-Supply-Chain-Review.pdf.

Annexe Q

Figures