Mise à l'épreuve de la continuité opérationnelle : Le paradoxe des organisations hyperconnectées

Gilles Paché

CERGAM, Aix-Marseille Université

IUT TC Aix & TC Marseille

413 Avenue Gaston Berger

13625 Aix-en-Provence Cedex

Courriel : gilles.pache@univ-amu.fr

Résumé

Les cyberattaques ayant visé, à l'automne 2026, des installations frigorifiques de la grande distribution alimentaire européenne et le prestataire de l'Établissement Français du Sang révèlent le paradoxe des organisations hyperconnectées dont l'optimisation numérique fragilise la continuité opérationnelle. La comparaison de ces incidents souligne comment la donnée, devenue agissante dans les systèmes de contrôle, transforme une intrusion informatique en dommage matériel. Trois mécanismes caractérisent cette « efficience toxique » : la convergence des technologies de l'information et des technologies opérationnelles, l'érosion des marges de manœuvre par la rationalisation, et la dissociation entre responsabilité opérationnelle et maîtrise technique. En déplaçant l'analyse des défaillances technologiques vers les choix managériaux organisant les dépendances numériques, l'article met en évidence trois leviers d'action : la désoptimisation stratégique, le management de la défiance et le pilotage amélioré de la continuité opérationnelle.

Mots-clés : Cybersécurité, chaîne du froid, continuité opérationnelle, désoptimisation stratégique, management de la défiance, résilience

Abstract

Cyberattacks targeting refrigeration systems in European food retail and the service provider of the French Blood Establishment in fall 2026 expose the paradox of hyperconnected organizations, whose digital optimization can undermine operational continuity. Comparing these incidents highlights how data, once endowed with operational agency within control systems, can turn a cyber intrusion into physical damage. Three mechanisms characterize this "toxic efficiency": the convergence of information technology and operational technology, the erosion of organizational slack through rationalization, and the disconnect between operational responsibility and technical control. By shifting the analysis from technological failures to the managerial choices that shape digital dependencies, this article identifies three avenues for action: strategic de-optimization, a management approach grounded in distrust, and enhanced operational continuity management.

Keywords: Cybersecurity, cold chain, operational continuity, strategic de-optimization, management approach grounded in distrust, resilience

Introduction

Une cyberattaque peut aujourd'hui détruire des marchandises sans toucher une palette. Il lui suffit de prendre la main à distance sur le système qui règle la température d'une chambre froide ou d'un rayon frais / surgelés de supermarché. Mi-octobre 2026, environ 700 magasins français ont ainsi vu leurs installations frigorifiques perturbées après la compromission de systèmes de supervision,[1] ainsi qu'une quinzaine de départs de feu. Le 9 novembre, le parquet de Paris a attribué l'attaque au groupe iranien « *Shahid Kaveh* », unité cyber offensive affiliée au centre électronique et cyber du Corps des Gardiens de la Révolution.[2] Des paramètres de dégivrage et de température ont été modifiés, parfois jusqu'à

[1] https://www.lemonde.fr/economie/article/2026/10/12/journee-noire-dans-les-supermarches-francais-apres-une-cyberattaque-massive_6792763_3234.html, Consulté le 10 novembre 2026.
[2] https://www.lemonde.fr/pixels/article/2026/11/09/cyberattaque-des-refrigerateurs-de-supermarche-la-justice-ouvre-une-enquete-contre-un-groupe-iranien-jean-noel-barrot-souhaite-des-sanctions-a-l-echelle-europeenne_6808673_4408996.html, Consulté le 10 novembre 2026.

retarder le déclenchement des alarmes. Des denrées ont été détruites et certaines enseignes ont suspendu temporairement leur activité. Trois semaines plus tard, une attaque visant le prestataire d'équipements frigorifiques de l'Établissement Français du Sang (EFS) a cherché à relever les seuils de température de sites conservant du plasma. Les anomalies ont cette fois été détectées à temps : aucun produit sanguin n'a été perdu et aucune conséquence sanitaire n'a été signalée.[3] Deux épisodes, deux niveaux de gravité, mais une même leçon : une intrusion numérique peut agir directement sur la matière et menacer la conservation des aliments ou des produits biologiques au cœur de l'activité économique.

De tels événements ne racontent pas seulement l'histoire de systèmes insuffisamment protégés ; ils donnent à voir une transformation plus profonde de l'organisation des systèmes de distribution. À mesure que les équipements physiques sont hyperconnectés, supervisés à distance et intégrés à des architectures numériques de contrôle, l'information cesse d'être un simple reflet de l'activité pour devenir une ressource opératoire, susceptible de commander des processus et de produire des effets dans le monde matériel (Carreras Guzman *et al.*, 2020). Automatiser, rationaliser, réduire les coûts, supprimer les temps morts et piloter chaque opération au plus près, telle est la promesse managériale de la transformation numérique. Pourtant, la recherche d'efficience peut rendre l'activité dépendante d'infrastructures numériques que l'organisation ne maîtrise qu'en partie, voire dont elle ne sait plus se passer. Les gains de productivité et de coordination peuvent ainsi s'accompagner d'une réduction des marges de manœuvre, d'une dépendance accrue aux dispositifs de commande et d'une moindre capacité d'intervention locale. La vulnérabilité ne résulte alors pas seulement de failles techniques en étant enracinée de manière plus problématique dans les choix ordinaires de conception, d'organisation et de pilotage qui conditionnent la performance. L'enjeu consiste dès lors à examiner les dépendances produites par le modèle de management lui-même, au-delà de la seule robustesse des systèmes informatiques.

[3] https://www.lefigaro.fr/social/apres-les-supermarches-l-etablissement-francais-du-sang-victime-d-une-cyberattaque-ses-chambres-froides-prises-pour-cible-20261104, Consulté le 10 novembre 2026.

La transformation numérique peut renforcer les capacités en facilitant la coordination et l'élaboration de réponses adaptées, comme le montrent Browder *et al.* (2023) pour deux entreprises confrontées à la pandémie de Covid-19. Ceci s'accompagne toutefois de tensions, notamment lorsque les procédures formalisées s'éloignent des pratiques effectives (De Nicola *et al.*, 2023). La maîtrise du risque cyber ne saurait reposer sur les seuls dispositifs techniques dans la mesure où elle suppose une mobilisation managériale et une coordination à l'échelle systémique des chaînes logistiques (Gaudenzi et Baldi, 2024). La continuité gagne en outre à être intégrée aux pratiques de gouvernance, plutôt qu'à être conçue comme une réponse ponctuelle aux crises (Loyarte *et al.*, 2024). La mise en dialogue de ces travaux fait finalement ressortir un angle peu exploré : les conséquences des cyberattaques sur la continuité d'activités physiques reposant sur des infrastructures numériques. L'article entend éclairer un tel enjeu en examinant les effets des attaques, les mécanismes organisationnels qui les amplifient et les leviers managériaux concrets de continuité. Il s'agit de mieux comprendre dans quelle mesure les cyberattaques visant les chaînes du froid révèlent une contradiction structurelle du management contemporain, dont la recherche d'efficience par la digitalisation peut contribuer à « fabriquer » les vulnérabilités qui compromettent sa continuité.

Un réel brutalement déstabilisé

La chaîne du froid constitue une infrastructure paradoxale dans la mesure où, indispensable à la continuité de nombreuses activités, elle demeure largement invisible tant qu'elle fonctionne. Dans la grande distribution alimentaire, elle conditionne la conservation des produits, la disponibilité des marchandises et, plus largement, la capacité des enseignes à garantir la qualité et la sécurité sanitaire des aliments proposés aux consommateurs (Mustafa *et al.*, 2024). Dans le secteur sanitaire, elle participe directement à la préservation de produits biologiques dont la qualité ne peut être dissociée de leurs conditions de stockage. Une telle dépendance repose désormais sur un ensemble de dispositifs interconnectés tels que des capteurs, des logiciels de régulation, des interfaces

de supervision, ou encore des systèmes de maintenance à distance. Autrefois contrôlée par des équipements relativement autonomes, la température se présente comme une variable pilotée par des architectures numériques complexes, ce qui modifie profondément la nature du risque (Waldhans *et al.*, 2024). Une défaillance mécanique peut être localisée, observable et parfois compensée par une intervention technique. Une compromission numérique, au contraire, modifie simultanément plusieurs paramètres, affecte les mécanismes de surveillance et donne l'apparence d'un fonctionnement normal à une installation qui ne l'est plus. L'attaque ne vise donc plus seulement l'information mais atteint les conditions matérielles de production, de conservation et de distribution.

Les travaux de Hizam (2026) sur la « myopie algorithmique » mettent en évidence les limites des dispositifs de pilotage numérique, dont les indicateurs de performance ne reflètent pas toujours les effets réels sur l'organisation. La distinction entre fonctionnement apparent et maîtrise effective est particulièrement importante dans les infrastructures fortement numérisées. Les indicateurs de disponibilité, de rendement ou de conformité technique renseignent sur l'état d'un dispositif sans garantir qu'il reste effectivement maîtrisé. Une installation frigorifique peut ainsi continuer à produire des données cohérentes et à afficher des paramètres conformes, alors même qu'une altération de ses fonctions de surveillance ou de régulation compromet progressivement la sécurité des produits conservés. Le risque tient donc autant à la défaillance technique qu'à l'incapacité de l'organisation à la détecter. La performance mesurée ne saurait, dès lors, être confondue avec une véritable maîtrise opérationnelle. Celle-ci repose sur des vérifications indépendantes, une confrontation régulière des données numériques aux observations de terrain, mais aussi sur l'implication des acteurs dans la régulation des usages, le développement de leurs compétences numériques et l'élaboration de pratiques de contrôle partagées (Thenoz, 2020).

L'épisode qui a touché la grande distribution alimentaire en octobre 2026 illustre pleinement la mutation à l'œuvre. La compromission des systèmes de régulation frigorifique a révélé qu'une intrusion pouvait agir directement sur les

paramètres garantissant la qualité des marchandises. En modifiant températures et cycles de dégivrage, et en neutralisant les mécanismes d'alerte, l'attaque a détourné des équipements de conservation de leur fonction première. Sa portée tient moins à la sophistication du procédé qu'à l'exploitation des dépendances opérationnelles : une manipulation ciblée de signaux de mesure ou de commande, éventuellement associée à une perturbation des communications, suffit à déstabiliser un processus physique et à engendrer des pertes économiques importantes (Huang *et al.*, 2009). Dans les magasins, cette défaillance s'est traduite par le retrait et la destruction de denrées devenues impropres à la commercialisation. La Figure 1 donne à voir ce passage du numérique au matériel, avec des milliers de produits frais détruits dans un magasin français, illustration tangible des dommages induits par une intrusion informatique. Le contraste est d'autant plus saisissant que les pertes surviennent dans un contexte de précarité alimentaire (en 2024, les Banques Alimentaires ont aidé 2,4 millions de personnes en France, soit 50 % de plus qu'en 2019).

Figure 1 : Produits frais détruits dans un supermarché français suite à la cyberattaque d'octobre 2026



Source : france • tv (2026).

Le cas de l'EFS ajoute une dimension plus sensible encore, dans la mesure où l'attaque visant les installations frigorifiques d'un prestataire sur plusieurs sites a exposé la conservation de produits sanguins à un risque dramatique de dégradation. La détection des anomalies et les mesures prises ont toutefois permis de préserver les stocks. Cette différence est essentielle : la résilience ne se mesure pas seulement à l'absence d'incident, mais à la capacité de détecter une anomalie avant qu'elle ne devienne irréversible. Les deux épisodes révèlent ainsi une même propriété des infrastructures connectées. Elles peuvent être attaquées à distance, tandis que leurs vulnérabilités se matérialisent localement, dans les magasins, les entrepôts et les établissements sanitaires. Ils soulignent également que les conséquences d'une compromission dépendent étroitement de la nature des produits concernés, des dispositifs de surveillance disponibles et de la capacité des organisations à intervenir dans des délais compatibles avec les exigences de conservation. Le Tableau 1 présente une analyse comparative des deux incidents, en mettant en évidence les processus de cyberattaque, leurs conséquences et les mécanismes de détection et de résilience mobilisés.

Trois registres d'une « efficience toxique »

La première vulnérabilité tient à la convergence croissante entre technologies de l'information et technologies opérationnelles. Longtemps relativement distincts, ces univers sont désormais imbriqués dans des architectures où les données ne servent plus seulement à observer l'activité mais à commander directement les équipements qui la rendent possible. Les systèmes frigorifiques connectés illustrent une telle évolution : l'association de capteurs, de microcontrôleurs et de plateformes logicielles permet de surveiller et de contrôler à distance des installations physiques, d'ajuster leurs paramètres de température et d'humidité et de suivre le fonctionnement de leurs différents équipements, notamment les unités de réfrigération et de dégivrage (Mohammed *et al.*, 2022). Si cette intégration améliore la réactivité opérationnelle et l'efficacité énergétique, elle introduit parallèlement une propriété nouvelle : la compromission d'une interface numérique peut se traduire immédiatement par une altération matérielle. Le problème

dépasse donc la confidentialité ou l'intégrité des données au sens traditionnel en concernant l'intégrité des actions produites par les systèmes numériques. Nous assistons ainsi à l'émergence d'une économie de la donnée agissante dans laquelle la frontière entre information et intervention physique tend à disparaître. La cybersécurité devient, par conséquent, une question de maîtrise des processus réels, et non plus seulement de protection des systèmes informatiques.

Tableau 1 : Analyse comparative de deux cyberattaques visant des infrastructures de chaîne du froid en France (automne 2026)

Critères d'analyse	Incident 1 Grande distribution alimentaire	Incident 2 Établissement Français du Sang (EFS)
Date, secteur et description	*11-12 octobre 2026* – Grande distribution alimentaire. Cyberattaque touchant plusieurs centaines de magasins, ciblant leurs systèmes de régulation frigorifique.	*1-2 novembre 2026* – Secteur sanitaire. Cyberattaque visant un prestataire d'équipements frigorifiques de l'EFS, affectant les installations de trois sites de l'établissement.
Systèmes ciblés et processus de cyberattaque	Compromission du logiciel de contrôle frigorifique. Modification à distance des paramètres de température et de dégivrage : température portée à 50 °C et durée du dégivrage prolongée de une à huit heures, retardant le déclenchement des alertes. Des équipements obsolètes ont été concernés.	Perturbation des systèmes de gestion des installations frigorifiques du prestataire externe, par l'intermédiaire d'un logiciel fourni par un tiers. Modification des seuils de température et de dégivrage à des valeurs très élevées. Des températures de 110 °C ont été rapportées par la presse.
Conséquences	Surchauffe des chambres froides et congélateurs, destruction de volumes importants de produits frais et surgelés, pertes économiques et perturbations de l'approvisionnement de plusieurs magasins.	Risque de dégradation des poches de plasma destinées à la transfusion et à la fabrication de médicaments, ainsi que des échantillons biologiques. Aucune perte de produits sanguins n'a été déclarée.
Détection et gestion de crise	Détection des anomalies de température, intervention des équipes techniques, déconnexion des équipements concernés et contrôle des marchandises. Dans certains magasins, les alertes tardives ont contribué à l'ampleur des pertes.	Détection rapide grâce aux systèmes indépendants de contrôle et de supervision des températures mis en place par l'EFS. Neutralisation des équipements concernés et transfert préventif ou sécurisation des produits sanguins.
Enseignements en matière de cybersécurité et de résilience	Nécessité de sécuriser les accès distants aux systèmes industriels, de maintenir les logiciels et équipements à jour et de garantir des mécanismes d'alerte fiables pour limiter les conséquences physiques et économiques d'une cyberattaque.	Importance de la sécurisation des prestataires et des composants logiciels tiers, mais aussi de dispositifs indépendants de supervision permettant de détecter une anomalie et de préserver les produits sensibles.

Source : Élaboration personnelle.

La deuxième vulnérabilité est plus dérangeante, car elle renvoie aux fondements mêmes du management contemporain : l'optimisation peut devenir une « fabrique » de la fragilité. Depuis plusieurs décennies, les organisations poursuivent une rationalisation systématique de leurs ressources à travers une réduction des stocks, une automatisation des tâches, une mutualisation des infrastructures, et une suppression des capacités jugées improductives. Loin d'être irrationnelles, ces orientations répondent à des impératifs économiques réels. Leur accumulation peut néanmoins produire une dépendance excessive à des dispositifs techniques centralisés et interconnectés. La moindre défaillance prend alors une dimension disproportionnée, faute de solutions alternatives immédiatement mobilisables. L'ouvrage de Scott (1998) traitant la simplification des systèmes complexes éclaire la contradiction sous-jacente. En privilégiant une représentation rationalisée et standardisée de la réalité, les organisations risquent de négliger les connaissances locales et les capacités d'adaptation qui assurent leur robustesse. La recherche d'efficience élimine ainsi parfois les marges qui permettent d'absorber l'imprévu. La redondance devient un coût, l'autonomie une duplication et l'intervention humaine une inefficacité. Pourtant, dans un environnement instable, ces prétendues imperfections constituent précisément des « ressources de continuité », en quelque sorte un *slack* organisationnel à la Cyert et March (1963).

La réflexion sur les marges de manœuvre organisationnelles prolonge notre analyse sur la survivabilité des chaînes logistiques, où nous proposons de dépasser l'analyse du « fonctionnement ordinaire » pour s'intéresser à la capacité d'un système à poursuivre ses activités après la perte d'une ressource ou d'une infrastructure essentielle (Paché, 2026). Une telle perspective prend une résonance particulière dans les organisations dont les équipements physiques dépendent désormais de dispositifs numériques de commande et de supervision. La question ne porte plus seulement sur la disponibilité des infrastructures mais également sur la possibilité de maintenir une capacité d'action indépendante de leur fonctionnement. Une installation frigorifique peut ainsi rester matériellement intacte tout en devenant inutilisable, voire dangereuse, si ses fonctions de

régulation ou de contrôle sont compromises. La continuité suppose alors de préserver des possibilités concrètes de reprise, telles que la commande locale, la vérification autonome des paramètres, l'intervention humaine ou le fonctionnement en mode dégradé. L'enjeu clé consiste à identifier les fonctions qui doivent demeurer maîtrisables, y compris lorsque les systèmes numériques qui les pilotent ne peuvent plus être considérés comme fiables. Appliquée aux organisations hyperconnectées, la survivabilité conduit ainsi à préserver non seulement les ressources nécessaires à l'activité, mais aussi la faculté collective de décider et d'agir lorsque les infrastructures numériques perdent leur fiabilité.

Une troisième vulnérabilité réside dans la dissociation entre responsabilité et maîtrise. La digitalisation repose sur une multiplication des interdépendances car fabricants, prestataires informatiques, exploitants et utilisateurs interviennent sur des infrastructures dont aucun acteur ne maîtrise nécessairement l'ensemble. Les incidents frigorifiques illustrent la fragmentation dont il est question puisque l'organisation qui subit les conséquences n'est pas forcément celle qui administre les équipements, configure les accès ou décide des mises à jour. Le CERT-FR a d'ailleurs documenté en octobre 2026 des compromissions de contrôleurs frigorifiques accessibles à distance, en soulignant notamment les risques liés aux équipements exposés sur Internet et arrivés en fin de vie.[4] La responsabilité opérationnelle demeure localisée tandis que les capacités de contrôle sont distribuées dans un écosystème de fournisseurs et de technologies. Si le dirigeant reste comptable de la continuité, il ne dispose pas toujours des moyens de vérifier directement les conditions techniques qui la garantissent. Il en résulte une illusion de maîtrise avec des tableaux de bord et des indicateurs donnant le sentiment d'un contrôle organisé, sans garantir la compréhension effective des dépendances. L'organisation devient alors responsable d'un système qu'elle ne gouverne qu'imparfaitement. Les trois registres permettent de synthétiser les principales vulnérabilités générées par la recherche d'efficience (voir le Tableau 2).

[4] https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012, Consulté le 10 novembre 2026.

Tableau 2 : Les trois registres d'une « efficience toxique »

Registres de vulnérabilité	Fragilités induites	Enjeux managériaux
Convergence technologies de l'information / technologies opérationnelles	Compromission d'une interface numérique pouvant provoquer une altération directe des processus physiques (température, humidité, dégivrage)	Garantir l'intégrité des commandes et sécuriser les systèmes industriels et logistiques au-delà de la seule protection des données
Optimisation et rationalisation	Diminution des marges de sécurité, des capacités de substitution et des possibilités d'adaptation face aux défaillances	Préserver des redondances, des ressources de secours et des capacités d'intervention humaine pour garantir la continuité
Dissociation entre responsabilité et maîtrise	Dépendance envers des acteurs tiers, perte de visibilité sur les systèmes et décalage entre responsabilité opérationnelle et maîtrise technique	Renforcer la gouvernance des prestataires externes, la traçabilité totale des responsabilités et la maîtrise des dépendances technologiques

Source : Élaboration personnelle.

Implications managériales

La première implication managériale consiste à réhabiliter ce que la recherche de performance a progressivement disqualifié, à savoir la redondance, les marges de manœuvre et les capacités inutilisées. Une organisation qui fonctionne sans réserve, sans solution alternative et sans possibilité de reprise manuelle n'est pas nécessairement performante ; elle est peut-être simplement performante tant que rien ne vient perturber son fonctionnement nominal. Dans une chaîne du froid, disposer d'un dispositif de contrôle indépendant, conserver une possibilité de régulation locale ou maintenir une procédure manuelle peut sembler économiquement irrationnel au quotidien. Pourtant, ces ressources deviennent décisives lorsque le système central est compromis. Il ne s'agit évidemment pas de promouvoir le gaspillage ni de renoncer aux gains de productivité, mais de reconnaître une valeur économique à certaines capacités qui ne produisent aucun rendement immédiat. Nous proposons ainsi le concept de *désoptimisation stratégique*, c'est-à-dire accepter délibérément une part d'inefficience apparente afin de préserver les conditions de continuité de l'activité. L'enjeu est de conserver suffisamment de degrés de liberté pour absorber une perturbation majeure.

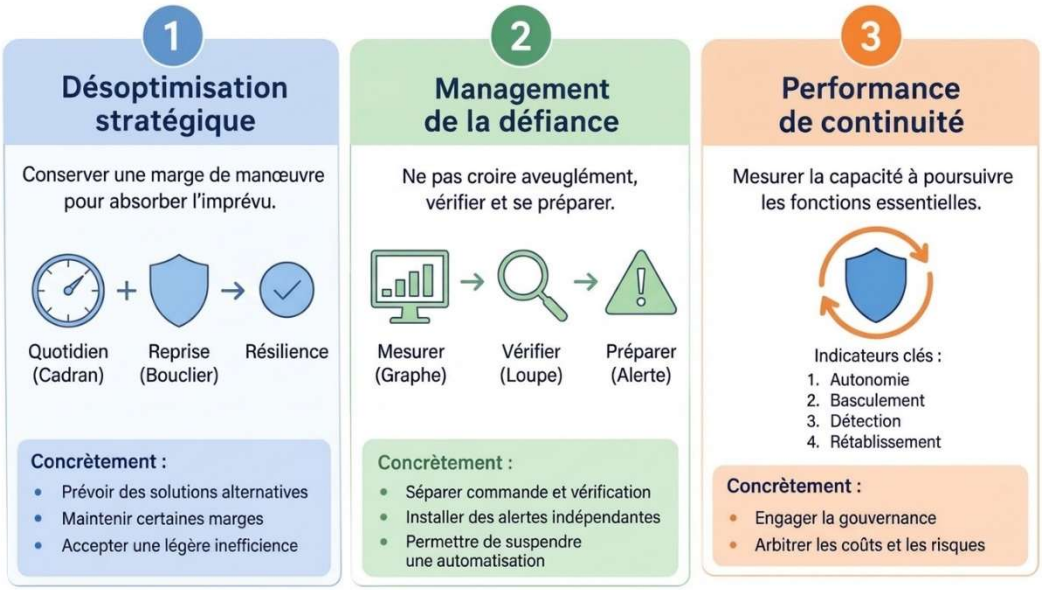
La deuxième implication consiste à substituer au management de la confiance un véritable management de la défiance. Les organisations ont progressivement construit leurs dispositifs de pilotage sur une présomption de fiabilité avec des capteurs qui mesurent, des logiciels qui calculent, des tableaux de bord qui restituent et des systèmes automatisés qui exécutent. Or, une information cohérente n'est pas nécessairement authentique, pas davantage qu'une commande techniquement valide n'est nécessairement légitime. La confiance accordée aux infrastructures numériques ne peut donc plus constituer un présupposé de fonctionnement en devenant une hypothèse régulièrement testée. Cela suppose notamment de dissocier les dispositifs de commande et de vérification, de prévoir des alertes indépendantes, de contrôler physiquement certaines mesures critiques et de permettre aux opérateurs de suspendre une automatisation suspecte. Les recommandations du National Institute of Standards & Technology relatives à la sécurité des technologies opérationnelles soulignent précisément l'importance de considérer simultanément les exigences de sécurité, de disponibilité et de sûreté physique (Stouffer *et al.*, 2023). Il s'agit en dernier ressort d'institutionnaliser le doute dans les processus décisionnels, une organisation intelligente n'étant pas celle qui croit toutes les données dont elle dispose mais qui est capable de les contester. Le doute devient ainsi une compétence organisationnelle à part entière, et non un dysfonctionnement managérial.

La troisième implication concerne la définition même de la performance, sachant que les indicateurs traditionnels mesurent la productivité, les coûts, les délais, les taux d'utilisation ou la disponibilité des équipements. De fait, ils renseignent sur l'efficacité d'une organisation lorsque ses infrastructures fonctionnent normalement, mais beaucoup moins sur sa capacité à poursuivre son activité lorsque celles-ci deviennent indisponibles ou suspectes. Nous proposons donc d'introduire la notion de *performance de continuité* entendue comme la capacité à préserver les fonctions essentielles malgré la défaillance, la compromission ou l'indisponibilité des systèmes numériques. Elle pourra être appréciée à travers plusieurs indicateurs tels que la durée de fonctionnement

autonome, le délai de basculement en mode dégradé, la capacité de détection indépendante, ou le temps de restauration d'une fonction critique. La continuité ne peut dès lors être abandonnée aux seuls spécialistes informatiques, car elle engage des arbitrages économiques, industriels, humains et organisationnels. Le conseil d'administration et la direction générale doivent ainsi assumer explicitement leur responsabilité dans la gouvernance du risque cyber et dans les choix organisationnels qui déterminent le niveau de protection et de continuité de l'activité (Slapničar *et al.*, 2023). Il leur revient notamment d'arbitrer entre les coûts des protections, les dépendances technologiques acceptées et les conséquences potentielles d'une interruption d'activité.

Les trois implications relèvent d'une même *logique systémique*, comme le synthétise la Figure 2. La résilience organisationnelle émerge des interactions entre ressources disponibles, mécanismes de contrôle et capacités de réponse dont les interdépendances conditionnent l'exposition aux perturbations et leurs effets potentiels. Son analyse suppose notamment de prendre en compte les phénomènes de propagation susceptibles de transformer une défaillance locale en perturbation globale, mais également les capacités de maintien des fonctions critiques et les possibilités de reconfiguration du système. L'enjeu consiste à dépasser une évaluation exclusivement fondée sur les performances en régime nominal pour intégrer différentes configurations de dégradation, de basculement et de récupération. Une telle approche permet de mieux caractériser les relations entre vulnérabilités, dépendances technologiques et capacités d'adaptation tout en prenant en considération les arbitrages qui déterminent le niveau de robustesse de l'ensemble organisationnel. Les trois dimensions identifiées forment ainsi un cadre analytique complémentaire dans lequel les choix structurels, les mécanismes de surveillance et les critères d'évaluation contribuent conjointement à la maîtrise des perturbations. À cet égard, la résilience cyber s'apprécie à travers la capacité de l'organisation à préserver ses fonctions essentielles et à maintenir son activité malgré l'altération de ses conditions de fonctionnement (Dupont, 2022).

Figure 2 : Leviers managériaux de la résilience cyber



Source : Élaboration personnelle.

Conclusion

Les cyberattaques contre les chaînes du froid invitent à reconsidérer une croyance profondément ancrée dans le management contemporain : davantage d'optimisation, d'automatisation et de données produirait nécessairement davantage de performance. Les événements de l'automne 2026 suggèrent au contraire que la sophistication technologique masque une fragilité organisationnelle croissante, particulièrement lorsque les capacités de contrôle, de décision et d'intervention sont externalisées ou concentrées dans des infrastructures interconnectées. La question n'est donc pas de ralentir la transformation numérique mais de sortir de son interprétation exclusivement productiviste. La désoptimisation stratégique, le management de la défiance et la performance de continuité esquissent les contours d'un autre paradigme : une organisation véritablement performante doit conserver des marges de manœuvre, savoir contester ses propres données et poursuivre ses fonctions essentielles lorsque ses dispositifs numériques deviennent indisponibles. Une telle perspective suppose de réhabiliter des ressources longtemps considérées

comme improductives (redondance, autonomie, intervention humaine et capacité d'improvisation). La robustesse devient alors une composante constitutive de la performance, et non une assurance accessoire contre ses accidents.

La réflexion prend une dimension supplémentaire avec la généralisation de l'IA et l'automatisation croissante des décisions. Si les organisations confient progressivement à des systèmes algorithmiques la surveillance, l'interprétation et le pilotage de leurs opérations, elles risquent de reproduire, à une échelle supérieure, les contradictions observées dans les infrastructures frigorifiques : concentration du pouvoir d'action, dépendance technologique et affaiblissement des capacités humaines de contestation. Le paradoxe serait alors de construire des organisations toujours plus intelligentes du point de vue computationnel, mais toujours moins autonomes dans leur capacité à faire face à l'imprévu. Peut-être faut-il finalement renverser la question fondatrice du management de la transformation numérique, et plutôt que de demander jusqu'où nous pouvons automatiser et optimiser les organisations, demandons-nous ce qu'elles doivent impérativement conserver dans la capacité de faire sans leurs systèmes numériques. À force de vouloir supprimer les degrés de liberté qui entravent la performance, nous avons peut-être supprimé dans le même temps ceux qui permettent aux organisations de survivre. Le véritable progrès managérial ne consisterait-il pas, de manière paradoxale, à réapprendre à ne pas tout optimiser ?

Références bibliographiques

Browder, R., Dwyer, S., & Koch, H. (2024). Upgrading adaptation: How digital transformation promotes organizational resilience. *Strategic Entrepreneurship Journal*, Vol. 18, n° 1, pp. 128–164. https://doi.org/10.1002/sej.1483

Carreras Guzman, N., Wied, M., Kozine, I., & Lundteigen, M.-A. (2020). Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Systems Engineering*, Vol. 23, n° 1, pp. 1–17. https://doi.org/10.1002/sys.21509

Cyert, R., & March, J. (1963). *A behavioral theory of the firm*. New York: Prentice-Hall.

De Nicola, A., Villani, M.-L., Sujan, M., Watt, J., Costantino, F., Falegnami, A., & Patriarca, R. (2023). Development and measurement of a resilience indicator for cyber-socio-technical systems: The allostatic load. *Journal of Industrial Information Integration*, Vol. 35, Article 100489. https://doi.org/10.1016/j.jii.2023.100489

Dupont, B. (2022). La cyber-résilience en pratiques : Sensemaking, préparation et adaptation. *Management & Data Science*, Vol. 7, n° 1, Article 21908. https://doi.org/10.36863/mds.a.21908

Galaitsi, S.-E., Pinigina, E., Keisler, J., Pescaroli, G., Keenan, J., & Linkov, I. (2023). Business continuity management, operational resilience, and organizational resilience: Commonalities, distinctions, and synthesis. *International Journal of Disaster Risk Science*, Vol. 14, n° 5, pp. 713–721. https://doi.org/10.1007/s13753-023-00494-x

Gaudenzi, B., & Baldi, B. (2024). Cyber resilience in organisations and supply chains: from perceptions to actions. *The International Journal of Logistics Management*, Vol. 35, n° 7, pp. 99–122. https://doi.org/10.1108/IJLM-09-2023-0372

Hizam, M. (2026). IA en entreprise : Sortir de la myopie algorithmique. *Management & Data Science*, Vol. 10, n° 2, Article 80419. https://management-datascience.org/articles/80419/

Huang, Y.-L., Cárdenas, A., Amin, S., Lin, Z.-S., Tsai, H.-Y., & Sastry, S. (2009). Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure Protection*, Vol. 2, n° 3, pp. 73–83. https://doi.org/10.1016/j.ijcip.2009.06.001

Loyarte, E., Gurrutxaga, N., & Funcia, J. (2024). Continuity governance model: A new process stage in the BCM system that underpins organizational resilience. *Cogent Business & Management*, Vol. 11, n° 1, Article 2434731. https://doi.org/10.1080/23311975.2024.2434731

Mohammed, M., Riad, K., & Alqahtani, N. (2022). Design of a smart IoT-based control system for remotely managing cold storage facilities. *Sensors*, Vol. 22, n° 13, Article 4680. https://doi.org/10.3390/s22134680

Mustafa, M., Navaranjan, N., & Demirovic, A. (2024). Food cold chain logistics and management: A review of current development and emerging trends. *Journal of Agriculture & Food Research*, Vol. 18, Article 101343. https://doi.org/10.1016/j.jafr.2024.101343

Paché, G. (2026). Entre performance et survivabilité : Repenser le management des chaînes logistiques face aux géocrises. *Revue de Management et de Stratégie*, octobre, Article a452. https://www.revue-rms.fr/entre-performance-et-survivabilite-repenser-le-management-des-chaines-logistiques-face-aux-geocrises/

Scott, J. (1998). *Seeing like a State: How certain schemes to improve the human condition have failed*. New Haven (CT): Yale University Press.

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems*, Vol. 51, Article 100642. https://doi.org/10.1016/j.accinf.2023.100642

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to operational technology (OT) security*. Gaithersburg (MD): National Institute of Standards & Technology.

Thenoz, É. (2020). Gestion des usages des technologies numériques dans les organisations : Une approche qualitative par le contrôle organisationnel et les chartes informatiques. *Systèmes d'Information & Management*, Vol. 25, n° 3, pp. 51–86. https://doi.org/10.3917/sim.203.0051

Waldhans, C., Albrecht, A., Ibald, R., Wollenweber, D., Sy, S.-J., & Kreyenschmidt, J. (2024). Temperature control and data exchange in food supply chains: Current situation and the applicability of a digitalized system of time–temperature-indicators to optimize temperature monitoring in different cold chains. *Journal of Packaging Technology & Research*, Vol. 8, n° 1, pp. 79–93. https://doi.org/10.1007/s41783-024-00165-2