L'ART DE SURVIVRE AUX CRISES

CRISE & RÉSILIENCE MAGAZINE

NUMÉRO 15 – Septembre 2026

Pays de nos auteurs : France, Canada, Luxembourg, Belgique, Maroc, Nouvelle-Zélande, Roumanie, Suisse

LE MAGAZINE QUI VOUS PRÉPARE À L'IMPRÉVISIBLE

DOSSIER BLACKOUT FAMILIALE

Comment protéger sa famille lorsque tout s'arrête ?

FORMATION À VENIR

Construisez votre exercice de gestion de crise

4 demi-journées : 17, 19, 24 et 26 novembre 2026

CRISE & RÉSILIENCE

ANTICIPER | RÉAGIR | REBONDIR

De la planification à l'action.

FORMATION

CONSTRUISEZ VOTRE PROPRE EXERCICE DE GESTION DE CRISE

DES ÉQUIPES MIEUX PRÉPARÉES POUR UN AVENIR PLUS RÉSILIENT.

Pas un modèle générique.
Pas un exercice fictif.

Le vôtre.

VOTRE SCÉNARIO

Un scénario réaliste et adapté à votre réalité

VOS RÔLES ET RESPONSABILITÉS

Des rôles clairs et opérationnels

VOTRE CHRONOGRAMME

Une séquence réaliste et structurée

UNE MÉTHODE RÉUTILISABLE

Des outils concrets pour vos prochains exercices

INCLUS

- Rencontre préparatoire individuelle
- 1 heure de coaching après la formation
- Accès au Club Crise & Résilience

FORMAT

- 4 demi-journées : 17, 19, 24 et 26 novembre 2026
- 8 h à 12 h (Québec) 14 h à 18 h (France)
- 100 % à distance
- Places limitées pour favoriser l'accompagnement individuel

Des compétences aujourd'hui pour une organisation plus résiliente demain.

1 397 $ CA + taxes

RÉSERVEZ VOTRE PLACE DÈS MAINTENANT

INFOS : info@crise-resilience.com

CRISE-RESILIENCE.COM

Édito

La rentrée est là. Les vacances s'achèvent, les agendas se remplissent et les projets reprennent leur rythme.

Quant aux crises, elles, ne connaissent ni pause estivale ni calendrier.

Cyberattaques contre nos infrastructures essentielles, chaînes d'approvisionnement fragilisées, dépendance au numérique, blackout, accidents majeurs, surcharge informationnelle… les risques évoluent et se multiplient. Les crises surgissent parfois là où nous les anticipons, mais aussi dans ces angles morts que nous n'avions pas envisagés.

Ce nouveau numéro de Crise & Résilience Magazine explore ces vulnérabilités sous des angles très différents, avec une même ambition : mieux comprendre pour mieux se préparer.

Alexandre Fournier nous montre comment une cyberattaque peut aller jusqu'à menacer notre eau potable. Dans Résilience des chaînes d'approvisionnement : les données ne suffisent pas, Alireza Asgari nous invite à regarder au-delà des chiffres et des outils pour mieux comprendre ce qui rend réellement une organisation résiliente.

Bertrand Domeneghetti nous invite à tirer les véritables enseignements des accidents nucléaires. Hélène Charlier, quant à elle, raconte une expérience troublante : après avoir participé à nos Journées Blackout, un événement bien réel est venu rappeler que certains scénarios ne relèvent pas uniquement de la fiction.

Alexandre Fournier et karine Maréchal partagent les principaux enseignements tirés des Journées Blackout de Québec, Montréal et Paris. Une expérience qui a démontré toute la richesse de l'intelligence collective lorsque les lumières s'éteignent… et que les idées s'allument.

Mathieu Montaroux pose une autre question essentielle : comment rester informé sans se laisser aspirer par le cycle incessant et anxiogène des nouvelles ?

Pascal Nahon nous emmène au cœur de l'hôpital pour comprendre ce qui se joue lorsque le numérique n'est plus au rendez-vous.

Du côté de la recherche, Raphaël de Vittoris et Carole Bousquet explorent ce que les humains, l'intelligence artificielle et les moteurs de recherche peuvent apporter à l'anticipation des crises.

Enfin, Thomas Scorticati nous rappelle une réalité de plus en plus présente dans un monde interconnecté : nous n'avons pas besoin d'être la cible pour devenir une victime.

Autant de perspectives qui convergent vers une même conviction : dans un monde toujours plus interconnecté, les crises prennent rarement la forme que nous avions anticipée.

La bonne nouvelle ? La résilience ne dépend pas de notre capacité à tout prévoir. Elle dépend de notre capacité à nous préparer, à nous adapter et à agir lorsque l'incertitude s'invite dans nos organisations.

Les auteurs de ce numéro nous rappellent, chacun à leur manière, qu'il n'existe pas de solution unique face aux crises. Mais qu'il existe de nombreuses façons de mieux comprendre les risques, d'enrichir notre réflexion et de renforcer notre préparation.

Bonne lecture, et surtout… bonne résilience.
L'équipe éditoriale

Sommaire

Direction de la publication : K. Maréchal Richard - **Création graphique :** Alfo65 - **Crédit photo :** Magnific – Open AI
Édition : Crise&Résilience - Québec (Qc), Canada – **Nous contacter :** info@crise-resilience.com

NOTE : Les articles sont classés par ordre alphabétique des prénoms

Cyberattaques : quand l'eau potable devient une cible

Fin juillet 2026, plus de 30 réseaux d'eau du Minnesota sont visés en deux jours par une cyberattaque coordonnée[1]. Quelques jours plus tôt, au Québec, une installation de traitement de l'eau est à son tour ciblée[2].

Ces événements racontent une évolution préoccupante : la cyberattaque ne menace plus seulement les données. Elle peut désormais atteindre directement les infrastructures qui permettent à une population de boire, de se soigner ou de lutter contre un incendie.

Pour préserver la fluidité de lecture, les sources ne sont pas citées dans le corps du texte. Les chiffres en exposant renvoient à la liste complète des références, disponible en fin d'article

Alexandre Fournier

Expert en gestion et simulation de crise
Consultant, formateur et conférencier dans les domaines de la continuité des affaires et de la gestion de crise depuis 30 ans.

Longtemps, les cyberattaques visaient des données ou des rançons. Aujourd'hui, elles franchissent une frontière : celle du monde physique. En s'attaquant à l'eau, ressource vitale et symbole de confiance, les agresseurs ne cherchent plus seulement le profit. Ils cherchent à démontrer une capacité de nuisance. La cyberattaque change alors de dimension : elle devient un instrument potentiel de sabotage, de déstabilisation et de pression géopolitique.

De l'écran au robinet

Les installations de production et de traitement de l'eau reposent aujourd'hui sur une combinaison d'équipements physiques et de systèmes numériques. Pompes, vannes, capteurs, systèmes de dosage, niveaux des réservoirs ou pression du réseau sont surveillés et pilotés par des systèmes industriels. Cette transformation numérique améliore considérablement l'exploitation, mais elle crée aussi des dépendances.

Une attaque ne doit donc plus être envisagée uniquement sous l'angle de la perte de données :

elle peut affecter la capacité à surveiller, contrôler ou maintenir un processus physique essentiel.

Et c'est précisément là que la cyberattaque change de nature.

Une menace qui n'a plus rien de théorique

En février 2021, à Oldsmar, en Floride, un opérateur voit son curseur bouger seul sur son écran. Un intrus vient de prendre le contrôle à distance du système et fait grimper le taux d'hydroxyde de sodium de l'eau de 100 à 11 100 parties par million. L'opérateur réagit rapidement et rétablit le réglage. La catastrophe est évitée.

À l'époque, l'incident paraît isolé. Il ne l'est plus.

En novembre 2023, CyberAv3ngers compromet des automates Unitronics de fabrication israélienne exposés sur Internet[3]. Aux États-Unis, la Municipal Water Authority of Aliquippa, en Pennsylvanie, doit notamment basculer certains équipements en fonctionnement manuel. Parmi les faiblesses observées : l'utilisation du mot de passe par défaut « 1111 » [4].
Puis les incidents se rapprochent.

En juillet 2026, des pirates pro-russes ciblent une installation de traitement de l'eau à Saint-Noël, au Bas-Saint-Laurent, prennent le contrôle à distance d'une partie du procédé et diffusent les images de leur intrusion sur Telegram. Les mécanismes de sécurité permettent d'éviter une contamination de l'eau[2].

Quelques jours plus tard, plus de 30 réseaux d'eau du Minnesota sont visés en deux jours. Des perturbations opérationnelles, notamment des pertes de pression et des débordements, sont observées, tandis que d'autres incidents sont signalés dans plusieurs États américains[1 5].

Pris séparément, chacun de ces événements pourrait sembler anecdotique. Mis bout à bout, ils dessinent une tendance : les systèmes industriels qui permettent de produire et de distribuer l'eau potable sont désormais directement exposés aux confrontations du cyberespace.

Pourquoi l'eau est une cible de choix ?

Le secteur cumule des fragilités : des installations souvent petites et sous-financées, directement exposées à Internet, avec une mauvaise séparation entre réseaux bureautiques (TI) et réseaux industriels (OT). En France, l'ANSSI a recensé 46 entités du secteur de l'eau touchées par un incident entre janvier 2021 et août 2024, pointant des protocoles industriels vieillissants et la généralisation de la télégestion[6 7]. Ajoutez la multiplication des capteurs connectés, et la surface d'attaque explose pour des organisations qui, bien souvent, n'ont ni les moyens ni les ressources de la défendre.

L'effet domino

La véritable portée d'une attaque contre une station du traitement de l'eau ne se mesure pas à l'installation touchée, mais aux conséquences qu'elle provoque. Le jour où elle s'arrête, c'est toute la chaîne des services et des citoyens qui dépendent de l'eau qui entre en crise.

Au premier rang, le citoyen : privé d'une eau sûre au robinet, il ne peut plus boire, cuisiner ni assurer son hygiène de base. Autour de lui, tout un écosystème vacille.

Sans eau potable, un hôpital voit ses capacités de soins se dégrader rapidement : hygiène, stérilisation et dialyse deviennent impossibles à maintenir normalement. Faute d'alternative, la seule issue peut être l'évacuation des patients, comme cet hôpital texan contraint de transférer 193 personnes, dont des nouveau-nés[8] [9].

Écoles et garderies ferment, faute de respecter les normes sanitaires. Restaurants et agroalimentaire doivent cesser tout usage de l'eau pour la préparation des aliments[10].

Et si des eaux non traitées s'infiltrent dans les canalisations, c'est un avis d'ébullition qui frappe toute une population[11].

Une seule cyberattaque provoque ainsi, en cascade, une crise opérationnelle, une crise de continuité pour des dizaines d'organisations, une crise de communication et, presque toujours, une crise de confiance.

Car même lorsque la qualité de l'eau n'est pas compromise, l'incertitude suffit à déclencher l'inquiétude.

« Peut-on boire l'eau ? »

« Combien de temps ça va durer ? »

Dans une infrastructure aussi sensible, l'absence d'information laisse vite place à la rumeur.

Qui attaque, et pourquoi ?
Longtemps, la question « qui attaque ? » appelait une réponse simple : des cybercriminels en quête d'argent.

Le cybercriminel revendique lui aussi ses attaques, mais pour réclamer une rançon. Un autre type d'attaquant a émergé, dont le mobile n'est plus l'appât du gain, mais la volonté de semer la terreur, le chaos et de déstabiliser un pays, souvent par rejet de ses positions politiques.

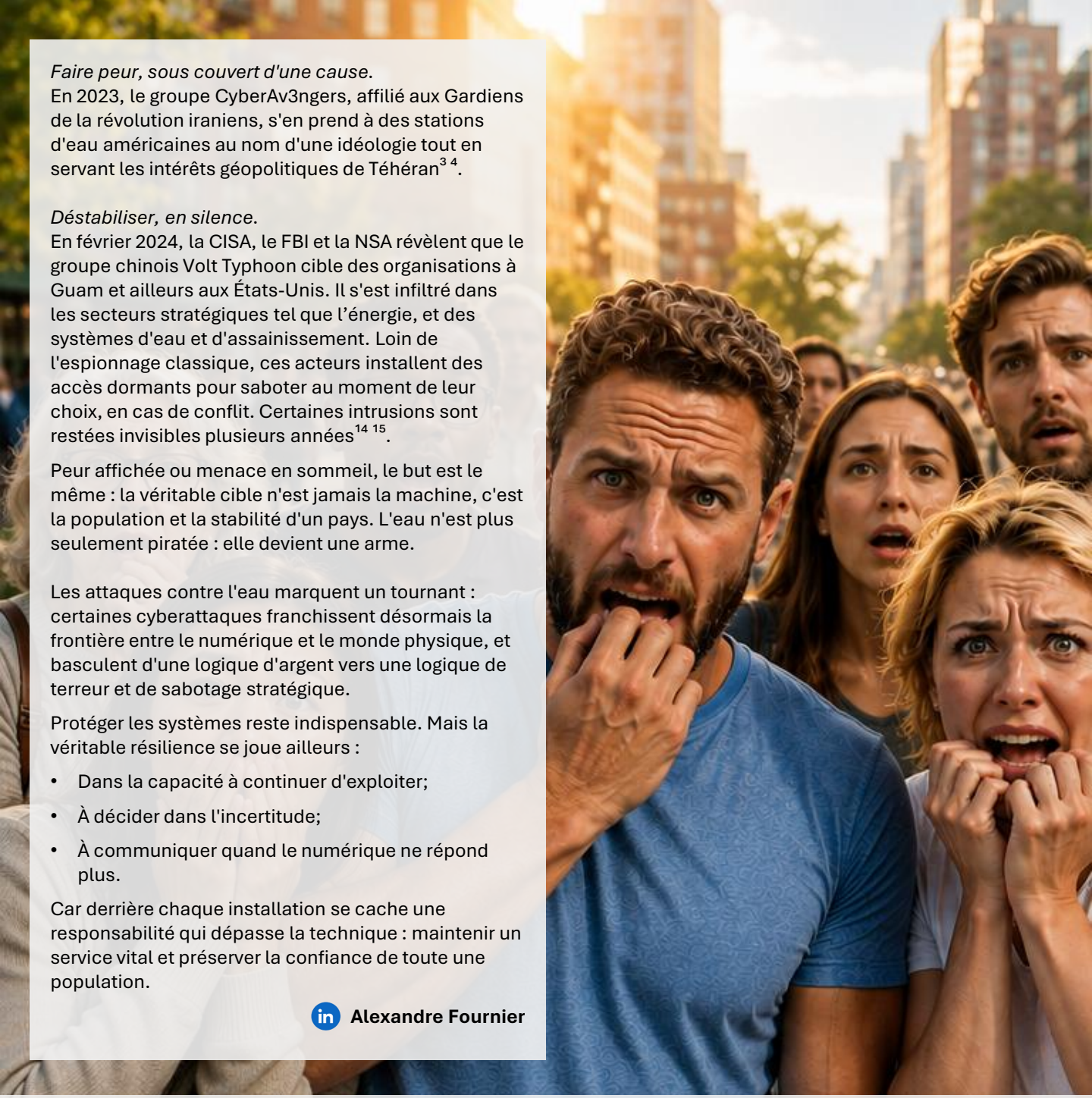
C'est ce déplacement du profit vers la terreur qui fait basculer la cyberattaque dans le cyberterrorisme.

Ce mobile se traduit de deux façons :

- Semer la peur maintenant;
- Installer une menace qui pèsera plus tard.

Trois exemples récents en dessinent toute l'étendue.

Faire peur, ouvertement.
En avril 2025, en Norvège, un groupe pro-russe ouvre à distance la vanne d'un barrage à Bremanger, libérant des millions de litres d'eau : une action que les renseignements norvégiens interpréteront comme un épisode de guerre hybride destiné à semer la peur et le chaos[12] [13].



Faire peur, sous couvert d'une cause.
En 2023, le groupe CyberAv3ngers, affilié aux Gardiens de la révolution iraniens, s'en prend à des stations d'eau américaines au nom d'une idéologie tout en servant les intérêts géopolitiques de Téhéran[3] [4].

Déstabiliser, en silence.
En février 2024, la CISA, le FBI et la NSA révèlent que le groupe chinois Volt Typhoon cible des organisations à Guam et ailleurs aux États-Unis. Il s'est infiltré dans les secteurs stratégiques tel que l'énergie, et des systèmes d'eau et d'assainissement. Loin de l'espionnage classique, ces acteurs installent des accès dormants pour saboter au moment de leur choix, en cas de conflit. Certaines intrusions sont restées invisibles plusieurs années[14] [15].

Peur affichée ou menace en sommeil, le but est le même : la véritable cible n'est jamais la machine, c'est la population et la stabilité d'un pays. L'eau n'est plus seulement piratée : elle devient une arme.

Les attaques contre l'eau marquent un tournant : certaines cyberattaques franchissent désormais la frontière entre le numérique et le monde physique, et basculent d'une logique d'argent vers une logique de terreur et de sabotage stratégique.

Protéger les systèmes reste indispensable. Mais la véritable résilience se joue ailleurs :

- Dans la capacité à continuer d'exploiter;
- À décider dans l'incertitude;
- À communiquer quand le numérique ne répond plus.

Car derrière chaque installation se cache une responsabilité qui dépasse la technique : maintenir un service vital et préserver la confiance de toute une population.

Alexandre Fournier

Sources
Les numéros ci-dessous correspondent aux appels de notes (chiffres en exposant) figurant dans l'article. Une même source peut être citée à plusieurs reprises et conserve alors le même numéro.

1. The Guardian — US cyber attacks on water (Minnesota) : https://www.theguardian.com/technology/2026/aug/04/us-cyber-attacks-water-minnesota-iran
2. CBC — Hacking water treatment plants, cyberattack (Québec / Saint-Noël) : https://www.cbc.ca/news/canada/montreal/hacking-water-treatment-plants-cyberattack-quebec-9.7294526
3. The Hacker News — Iranian hackers exploit PLCs (CyberAv3ngers / Unitronics) : https://thehackernews.com/2023/11/iranian-hackers-exploit-plcs-in-attack.html
4. CISA — Avis AA23-335A (Aliquippa, mot de passe « 1111 ») : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
5. FBI — Alerte 2026, secteur eau et eaux usées (automates exposés) : https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet--facing-programmable-logic-controllers-causing-operational-disruptions
6. Banque des Territoires — Services d'eau et d'assainissement très vulnérables (ANSSI) : https://www.banquedesterritoires.fr/des-services-deau-et-dassainissement-tres-vulnerables-face-aux-cyberattaques
7. GuideIT — Cybersécurité dans le secteur de l'eau : un état des lieux inquiétant : https://www.guideit.fr/cybersecurite-dans-le-secteur-de-leau-un-etat-des-lieux-inquietant/
8. CDC — Water Emergency Toolkit (établissements de santé) : https://www.cdc.gov/water-emergency/hcp/toolkit/index.html
9. MECO — Health Care Water Crisis (évacuation hospitalière) : https://www.meco.com/fr/health-care-water-crisis/
10. Québec.ca — Avis sur l'eau potable, établissements alimentaires : https://www.quebec.ca/sante/alimentation/salubrite-aliments-prevention-risques/etablissements-alimentaires/avis-eau-potable
11. Québec.ca — Avis d'ébullition / avis de non-consommation : https://www.quebec.ca/agriculture-environnement-et-ressources-naturelles/eau-potable/qualite-eau-potable/avis-ebullition-avis-non-consommation
12. Daily Security Review — Norway attributes dam cyberattack to Russian hackers : https://dailysecurityreview.com/cyber-security/norway-attributes-dam-cyberattack-to-russian-hackers/
13. Cybernews — Norway blames Russian hackers, dam cyberattack (Bremanger) : https://cybernews.com/cybercrime/norway-blames-russian-hackers-dam-cyberattack-bremanger/
14. Cyberwarzone — Volt Typhoon : China's critical infrastructure pre-positioning campaign : https://cyberwarzone.com/2026/03/09/volt-typhoon-chinas-critical-infrastructure-pre-positioning-campaign/
15. CISA — *Avis AA24-038A, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure* (7 février 2024) : https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

5 réflexes pour garder le contrôle quand l’eau est attaquée

Cartographier la dépendance à l'eau, pas seulement les systèmes qui la contrôlent

Identifiez toutes les activités qui s'arrêtent sans eau potable pas uniquement l'usine elle-même, mais l'hôpital, l'école, le service d'incendie, le restaurant du coin. Cette cartographie révèle qui doit être alerté en priorité et dans quel délai, avant même qu'une attaque ne survienne.

Préparer un mode dégradé manuel et l'exercer réellement

Les incidents qui ont été maîtrisés (Oldsmar, Saint-Noël) l'ont été grâce à un opérateur humain capable de reprendre le contrôle ou à un mécanisme physique de sécurité indépendant du numérique. Un plan qui suppose que les systèmes automatisés fonctionneront toujours n'est pas un plan de continuité, il faut savoir opérer en manuel, et le pratiquer en exercice, pas seulement sur papier.

Préparer la communication avant la question « peut-on boire l'eau ? »

Le doute se propage plus vite que la contamination elle-même. Ayez des messages-clés pré-rédigés pour la population, les médias et les organisations partenaires (hôpitaux, écoles, services d'urgence), et un porte-parole identifié capable de parler dans l'heure suivant la détection d'un incident, même pour dire « nous enquêtons encore ».

Segmenter et surveiller la frontière TI/OT

La majorité des incidents recensés exploitent une mauvaise séparation entre réseaux bureautiques et réseaux industriels, ou des accès laissés par défaut (mots de passe, télégestion non protégée). Un audit de cette frontière et la suppression des accès à distance non essentiels reste la mesure la plus simple avec le meilleur rapport impact/coût.

Activer une cellule de crise inter organisationnelle, pas seulement technique

Une attaque sur l'eau n'est pas qu'un incident informatique : c'est simultanément une crise opérationnelle, sanitaire, de continuité et de confiance. La cellule de crise doit donc réunir dès le départ les TI, les opérations, les communications et les partenaires externes concernés (santé publique, sécurité incendie) pas seulement l'équipe cyber.

Résilience des chaînes d'approvisionnement: les données ne suffisent pas.

Les outils prédictifs peuvent aider les entreprises à anticiper les perturbations, mais la résilience ne se résume pas à l'utilisation de tableaux de bord.

Nos recherches montrent qu'elle se développe lorsque des données fiables, des processus décisionnels éprouvés et un jugement éclairé se conjuguent avant, pendant et après une crise

Alireza Asgari

Docteur en Sciences de Gestion et assistant professor en supply chain et systèmes d'information à Clermont School of Business.

ÉTUDE SCIENTIFIQUE

Les chaînes d'approvisionnement évoluent désormais dans un contexte de turbulence permanente : chocs de la demande, défaillances de fournisseurs, goulets d'étranglement logistiques, événements climatiques et tensions géopolitiques.

Dans ce contexte, l'attrait des données est indéniable. Pourtant, nos recherches incitent les gestionnaires de risques à la prudence :

les données sont importantes, mais elles ne suffisent pas à elles seules à garantir la résilience.

Pour de nombreuses organisations, la première réaction face à l'incertitude est d'investir dans la technologie. De nouvelles plateformes sont acquises, des tableaux de bord sont déployés et des outils prédictifs sont mis en place pour mieux appréhender les risques. Cette réaction est compréhensible. Lorsque l'environnement devient instable, les responsables ont besoin de signaux d'alerte plus précoces et d'une vision plus claire de la situation chez les fournisseurs, au niveau des stocks, des flux de transport et de la demande client.

Les travaux antérieurs sur la résilience de la chaîne d'approvisionnement ont systématiquement démontré que

la visibilité, l'agilité, la flexibilité, la collaboration et la gestion des risques sont essentielles en cas de perturbations.

Les données peuvent contribuer à développer toutes ces capacités.

Toutefois, le principal enseignement de notre recherche est que la résilience ne découle pas de la maîtrise des technologies ni des ressources dont disposent les entreprises.

Dans notre étude menée auprès d'entreprises françaises, l'incertitude et une stratégie axée sur les données ont incité ces dernières à adopter les ressources du Big Data. Ceci confirme une réalité concrète : face à un environnement commercial moins prévisible, les entreprises recherchent davantage d'éléments probants, de signaux et de prévisions plus fiables.

La possession de systèmes, de plateformes et de capacités techniques ne s'est pas traduite automatiquement par de meilleures capacités de prédiction.

En situation de crise, des données de mauvaise qualité peuvent être pires que l'absence de données : elles engendrent une confiance illusoire.

Un tableau de bord peut présenter un fournisseur comme présentant un faible risque car la dernière mise à jour remonte à trois mois. Un retard de transport peut paraître gérable car les équipes locales utilisent des définitions différentes du délai de livraison. Une prévision de la demande peut être ignorée car les services des ventes, des opérations et des achats divergent sur les chiffres.

Dans chaque cas, le problème n'est pas l'absence de technologie, mais l'absence de données fiables, partagées et exploitables.

Nous constatons que les organisations les plus résilientes ne sont ni celles qui s'appuient uniquement sur des algorithmes, ni celles qui se fient uniquement à leur instinct. Elles combinent :

des données fiables, des procédures rigoureuses et un jugement éclairé.

Concernant les données fiables, nos conclusions soulignent donc l'importance de la qualité des données pour la résilience.

Des données fiables permettent aux entreprises de détecter plus tôt les signaux faibles : augmentation des retards des fournisseurs, variations anormales de la demande, tensions sur les stocks, écarts de qualité ou dégradation des performances de livraison.

Cependant, la détection n'est que la première étape. Un signal doit être interprété, analysé et donner lieu à des actions concrètes. C'est là que de nombreuses organisations échouent. Elles produisent des rapports, mais ces rapports n'influent pas sur les décisions. Elles génèrent des alertes, mais celles-ci ne sont pas clairement attribuées à des responsables.

Elles prévoient des perturbations, mais ces prévisions ne déclenchent aucune décision d'approvisionnement, aucun ajustement logistique, aucun échange avec les fournisseurs ni aucun plan de communication client.

Concernant les procédures rigoureuses, la résilience s'améliore lorsque les données s'intègrent aux pratiques de gestion courantes. Les outils prédictifs doivent être intégrés à la planification des ventes et des opérations, aux évaluations des fournisseurs, aux réunions sur les risques liés aux achats, aux décisions en matière de stocks et aux simulations de crise.

Les équipes doivent savoir quels indicateurs sont pertinents, à quelle fréquence ils sont analysés, qui est responsable des actions à entreprendre et quelles options sont disponibles lorsque des seuils sont franchis. Concrètement, l'analyse prédictive ne doit pas être considérée comme un outil réservé aux experts et utilisé ponctuellement par les analystes. Elle doit devenir un langage commun pour anticiper les tensions et coordonner les réponses.

Concernant le jugement éclairé, notre étude souligne que le jugement humain demeure essentiel. Les outils prédictifs peuvent identifier des tendances, estimer des probabilités et signaler des anomalies, mais ils ne peuvent appréhender pleinement le contexte. Les crises impliquent souvent ambiguïté, compromis politiques, informations incomplètes et situations sans équivalent historique précis. Les gestionnaires expérimentés apportent une connaissance approfondie des fournisseurs, des marchés, des contraintes internes et des signaux informels, autant d'éléments difficiles à modéliser. Leur intuition ne remplace pas les données ; elle contribue à leur interprétation.

La résilience de la chaîne d'approvisionnement ne saurait se réduire à un simple projet technologique. Les données et les outils prédictifs sont certes puissants, mais uniquement lorsqu'ils reposent sur des informations fiables, sont intégrés aux pratiques quotidiennes et interprétés par des personnes qui comprennent l'activité. La leçon pour les gestionnaires de risques est claire : privilégiez la qualité des données aux tableaux de bord, les processus décisionnels à l'automatisation et le jugement managérial à la confiance aveugle dans les algorithmes. La résilience ne se construit pas en prédisant l'avenir avec exactitude. Elle se construit en anticipant les risques, en en comprenant la signification et en agissant avec rapidité, coordination et expérience lorsque l'incertitude se concrétise.

Asgari, A., Alaeddini, M., & Reaidy, P. (2025). The Role of Big Data and Predictive Analytics in Developing Resilient Supply Chains: A Resource-based Perspective. IFAC-PapersOnLine, 59(10), 2874-2879.

https://doi.org/10.1016/j.ifacol.2025.09.483

https://www.sciencedirect.com/science/article/pii/S2405896325012467

Alireza Asgari

Docteur en Sciences de Gestion et assistant professor en supply chain et systèmes d'information à Clermont School of Business. Ses travaux se situent à la croisée de la gestion de la chaîne d'approvisionnement, de l'analytique big data et de la résilience, avec un intérêt particulier pour le secteur agroalimentaire.

À lire aussi sur

Le MAGAZINE par Crise et Résilience

6 min

CONTINUITÉ D'ACTIVITÉ MAI 2026

Crise au Moyen-Orient : réexaminer les leviers de résilience des chaînes d'approvisionnement agroalimentaires

Dans le secteur agroalimentaire, les crises géopolitiques ne s'arrêtent pas aux frontières du conflit : elles déstabilisent l'ensemble de la chaîne d'approvisionnement et propagent...

6 clés pour transformer les données en résilience

Pour appliquer immédiatement ces enseignements, les gestionnaires doivent partir d'un principe simple : se concentrer sur les décisions, et non sur la technologie.

1-Identifier trois à cinq perturbations critiques susceptibles d'impacter gravement les opérations, telles que la défaillance d'un fournisseur, des retards de livraison, des pics de demande, des ruptures de stock ou des problèmes de qualité.

2-Définir des indicateurs clés de performance (KPI) pour chaque risque identifié afin de détecter rapidement les signaux précurseurs d'une perturbation : retards de livraison, variations anormales des commandes, baisse du niveau de service, tensions sur les stocks ou incidents récurrents chez les fournisseurs.

3-Vérifier la fiabilité de ces KPI. Les données doivent être récentes, cohérentes entre les services et validées par les équipes qui les utilisent. Un tableau de bord sophistiqué est inutile si les informations sous-jacentes sont obsolètes ou contestées.

4-Intégrer les données aux processus habituels. Les KPI doivent être examinés régulièrement lors des réunions avec les fournisseurs, de la planification des ventes et des opérations, des analyses de la chaîne d'approvisionnement et des exercices de gestion de crise. L'objectif n'est pas de multiplier les rapports, mais d'intégrer les KPI liés aux risques au processus décisionnel continu.

5-Attribuer clairement les responsabilités. Chaque alerte doit répondre à trois questions : qui la reçoit, qui l'interprète et qui décide des mesures à prendre ? Sans attribution de responsabilité, les alertes précoces se perdent dans le bruit de fond.

6-Préserver le jugement humain. Si les outils prédictifs peuvent certes mettre en évidence des signaux faibles, les gestionnaires

Ce que les accidents nucléaires nous, enseignent vraiment !

Alors que « l'effet ciseaux » entre des besoins énergétiques grandissants et la nécessité de décarboner conduit à la reprise du nucléaire,

les crises passées rappellent une exigence essentielle : comprendre la complexité des risques nucléaires.

Cette complexité pèse lourdement sur la communication de crise et altère durablement la confiance.

Bertrand Domeneghetti

Président fondateur de RISKOVER.
Auteur conférencier. Inspecteur général de sapeurs-pompiers.
Gestion des risques et des crises. Le risque nucléaire.

Depuis les années 1950, l'énergie nucléaire a connu plusieurs inflexions majeures, notamment avec les accidents de Three Mile Island, Tchernobyl et Fukushima. Les contraintes énergétiques et climatiques la replacent aujourd'hui au cœur des stratégies de décarbonation, mais sa relance repose sur la confiance publique qu'un accident majeur pourrait fragiliser.

Pour mieux s'y préparer, que nous enseignent vraiment Three Mile Island, Tchernobyl et Fukushima ?

Cet article en propose une lecture resserrée à partir de leurs principaux enseignements.

L'accident de Three Mile Island 1979

Malgré la fusion partielle du cœur du réacteur et le relâchement de radioactivité dans l'enceinte de confinement, il est admis que les conséquences radiologiques[1] dans l'environnement ont été minimes.

Les populations proches de la centrale ont toutefois été plongées dans une inquiétude profonde, amplifiée par des difficultés de communication qui ont entamé leur confiance envers les institutions. L'accident a marqué un tournant dans la perception de la filière, le mouvement antinucléaire est renforcé. La contestation gagne de nombreux pays.

Three Mile Island montre déjà que les conséquences d'un accident nucléaire ne se mesurent pas seulement en doses reçues, mais aussi en confiance perdue.

Pourtant, l'industrie américaine s'impose de nouvelles normes de sécurité, reprises ensuite à l'échelle mondiale. Curieusement, l'accident de Three Mile Island a sans doute contribué à rendre l'industrie nucléaire techniquement plus sûre.

L'accident de Tchernobyl 1986

Les enfants et adolescents biélorusses et ukrainiens de moins de dix-huit ans au moment de l'accident sont les plus sérieusement affectés[2] par les dépôts radioactifs.

1-Nombreuses publications regroupées dans https://www.fnac.com/a23086982/Bertrand-Domeneghetti-Crises-nucleaires-mythes-et-realites

2- Même source et datas directement disponibles auprès des publications du Comité scientifique des Nations unies pour l'étude des effets des rayonnements ionisants (UNSCEAR)

À ÉCOUTER

*Sur notre chaine **YouTube***

L'accident est en grande partie imputable à la conception ancienne du réacteur soviétique, sans enceinte de confinement notamment. Il serait donc imprudent d'établir des parallèles trop directs avec les réacteurs occidentaux.

Tchernobyl aide néanmoins à comprendre la difficulté à communiquer en situation de crise nucléaire.

En cas d'accident nucléaire, à la question, y a-t-il un risque OUI ou NON ? Les populations, les médias et les décideurs attendent une réponse aussi binaire que la question. Or une telle réponse n'est pas toujours possible. On parle de risque « stochastique », c'est-à-dire d'une augmentation de la probabilité d'apparition de cancers, notion complexe qui complique considérablement la parole publique.

Qualifier la dispersion des rejets et évaluer un danger sanitaire probabiliste restent des exercices particulièrement difficiles. Même préparés, les acteurs ne peuvent disposer d'informations complètes en début de crise.

L'accident de Fukushima 2011

Dans le cas de l'accident japonais, le fossé entre la réalité des expositions et la perception qu'en ont encore aujourd'hui les populations demeure considérable plus de quinze ans après l'accident et treize ans après les premiers rapports.

« Aucune augmentation perceptible de l'incidence des effets liés aux rayonnements ionisants sur la santé des populations exposées n'est attendue »

précisent pourtant depuis 2013 les experts internationaux, indépendants.

Pour autant, les effets psychologiques liés à l'impréparation de l'évacuation ou à l'éloignement durable des populations de leur lieu de vie ne peuvent être méconnus.

Comment apprécier sa sécurité face à un risque radiologique insidieux, imperceptible, invisible et persistant, qui se disperse avec le vent, se concentre localement et produit des effets sanitaires différés rendant difficile l'établissement d'une causalité directe ?

Autant de questions restées sans réponse surtout en début de crise. Pourtant *« On n'a qu'une fois l'occasion de faire une première bonne impression »*.

Les premières heures des crises alimentent directement les peurs et pèsent durablement sur la confiance accordée aux autorités.

Le choc systémique provoqué sur la chaîne d'approvisionnement mondiale, notamment dans les industries automobiles et électroniques, rappelle enfin qu'un accident nucléaire peut produire des effets bien au-delà de son périmètre sanitaire immédiat.

Les études épidémiologiques robustes montrent que les conséquences sanitaires radiologiques ne sont pas les plus inquiétantes, ni à TMI bien sûr, ni à Fukushima.

Les détresses psychologiques sont une constante des trois grands accidents nucléaires. Ce constat n'est pas sans lien avec le suivant.

La parole publique joue alors un rôle crucial. Pourtant, décideurs, exploitants, médias et populations peinent à apprécier la situation en temps réel. Disons-le, la communication de crise a été jugée défaillante lors des trois grandes crises nucléaires. En cas de nouvel accident, les complexités inhérentes au risque nucléaire pourraient encore empêcher la communication attendue.

L'impact serait alors immense, et l'avenir de la filière nucléaire à nouveau fragilisé. Comment s'y préparer ? Comment vous informer et vous protéger efficacement en situation d'accident nucléaire ? C'est tout l'objet de notre prochain article.

Bertrand Domeneghetti

Consultant en gestion des risques notamment nucléaires, Bertrand Domeneghetti est Inspecteur général de sapeurs-pompiers (er), membre associé de l'Académie nationale des sciences, belles-lettres et arts de Bordeaux, administrateur de société et auteur de *Crises nucléaires. Mythes et réalités*.

Riskover
RISQUES & CRISES

Tel : + (0) 7 83 61 59 58

Site web : https://riskover-crise.com/

À LIRE *DU MÊME AUTEUR ...*

COMMENT VOUS INFORMER EN CAS DE CRISE NUCLÉAIRE ?

En toute situation conserver votre téléphone avec vous.

AVANT

- Identifiez les principales sources d'information officielles
- Renseignez-vous auprès de votre mairie
- Si vous habitez à proximité d'une installation nucléaire, prenez contact avec la CLI compétente.

PENDANT

- Écoutez le préfet (L'État)
- Veillez les médias (radio, télévision, internet)
- Pour comprendre le niveau du risque radiologique auquel vous êtes exposé, c'est l'ASNR qu'il faut écouter et consulter.

APRÈS

- Suivez les conseils de la colonne centrale « PENDANT »
- Renseignez-vous dans les centres d'accueil et d'information (CAI) ou dans les cellules d'information des centres d'accueil et de regroupement (CARE).

De la formation au réel : quand le scénario déraille

Une journée consacrée à la gestion de crise.

Quelques heures plus tard, la théorie confrontée au réel : 900 passagers immobilisés, des informations fragmentaires et une coordination sous tension.

Cette expérience interroge notre capacité à gérer l'imprévisible, à mobiliser la résilience collective et, surtout, à transformer le chaos en opportunité d'apprentissage.

Hélène Charlier

Crisis Management Coordinator – Direction Operations – Safe.brussels

Contribuer au développement du programme BRU response de la Région de Bruxelles-Capitale.

La crise constitue un révélateur puissant des organisations. Elle met à l'épreuve les procédures, la coordination, la circulation de l'information, mais aussi la capacité des individus à s'adapter.

Mon vécu raconté ici offre une occasion concrète d'interroger l'écart entre la crise préparée et la crise vécue.

Quand le scénario quitte la voie de la réalité

La gestion de crise repose sur la préparation : identifier les risques, élaborer des scénarios, définir les responsabilités et entraîner les acteurs.

Mais que se passe-t-il lorsque la situation réelle s'écarte rapidement du scénario prévu ?

C'est précisément l'expérience que j'ai vécue entre Paris et Bruxelles le 24 juin dernier, quelques heures après une journée de formation consacrée au Blackout, organisée d'une main de maître par Crise & Résilience que je remercie vivement.

18h50 : départ gare de Paris nord par une température avoisinant les 41°C. Le TGV peine à atteindre sa vitesse habituelle.

19h30 : arrêt total du TGV peu avant Compiègne. La climatisation cesse de fonctionner, ma voisine fait un malaise. Puis l'attente s'installe, tandis que les informations demeurent rares, incertaines et que la température augmente à l'intérieur du wagon. Les deux contrôleurs font des allers-retours incessants.
Une détection d'incendie au niveau du moteur est finalement évoquée. L'évacuation ne peut être immédiatement organisée. Les malaises se multiplient, le wagon bar est dépouillé pour palier à la déshydratation.

20h37 : Les deux contrôleurs décident finalement d'ouvrir les portes. Les voyageurs commencent spontanément à s'organiser.

Le scénario initial vient de basculer dans une situation dont personne ne maîtrise plus complètement l'évolution.

L'information : une ressource essentielle et opérationnelle

21h20 : l'évacuation en urgence est demandée. Il est annoncé deux heures d'attente avant que le TGV de secours n'arrive, la destination est inconnue.

En situation de crise, l'incertitude est inévitable. Le silence, lui, ne devrait pas l'être.

Au fil des heures, les passagers cherchent à comprendre : Que va-t-il se passer ? Où allons-nous ? Quand ? Et surtout, qui sait réellement ?

22h52 : la Gendarmerie arrive, des agents SNCF, des sapeurs-pompiers. 30 minutes plus tard, la Protection Civile arrive avec 800L d'eau, pas de nourriture. Nous les voyons défiler mais aucune communication ne nous est faite. Mes nouveaux compagnons de survie et moi les alpaguons pour tenter d'en savoir davantage. Les réponses obtenues sont souvent fragmentaires :

« ça ce n'est pas nous,
faut demander à la SNCF,
ça ce n'est pas moi,
faut demander au pompier,
ça je ne sais pas ».

Je finis par harponner un sapeur-pompier sur l'absence de coordination opérationnelle et du manque cruel de communication. Ce dernier me somme platement de retourner à ma place en me rétorquant que « c'est votre ressenti Madame ».

Ce même ressenti m'a poussé toute la soirée à m'interroger sur une combinaison de facteurs qui auraient pu être explosifs :

- Et s'il y avait bel et bien eu un incendie ?
- Et si l'orage attendu avait fracassé le ciel durant cette soirée ?
- Et s'il y avait eu plus de personnes vulnérables (bébés, enfants, personnes âgées…) ?
- Et si les passagers s'étaient davantage rebellés ?
- Quid de ceux qui sont partis en pleine nature ?
- Quid d'un comptage officiel ?

Ce constat ne remet pas en cause l'engagement des professionnels présents. Il souligne une difficulté des situations complexes : plusieurs acteurs peuvent être mobilisés sans pour autant disposer d'une représentation partagée de la situation. Or l'information n'est pas simplement un outil de communication.

En situation de crise, elle devient une ressource opérationnelle. Une information tardive ou contradictoire ne fait pas qu'alimenter l'impatience. Elle peut également encourager les initiatives individuelles, parfois difficiles à coordonner.

Dans notre cas, certains voyageurs commencent ainsi à partir à pied ou à organiser leur propre solution de sortie. À partir du moment où chacun construit sa propre représentation de la situation, le pilotage collectif devient forcément plus délicat.

La résilience ne se décrète pas : elle s'observe

00h15 : le TGV de secours arrive. Il serait pourtant réducteur de ne retenir que les difficultés. Car au milieu de cette situation dégradée et suffocante, une magnifique dynamique s'installe : celle de l'entraide. Des passagers accompagnent les personnes vulnérables, partagent de l'eau, cherchent des informations et rassurent leurs voisins. Des rencontres se font, des morceaux de vie se partagent.

Aucune cellule de crise n'avait besoin de les convoquer. Ils étaient déjà là.

Cette dynamique rappelle que le citoyen ne doit pas être considéré uniquement comme le destinataire d'une réponse de crise. Il peut et doit en être un acteur.

La question devient alors : comment intégrer cette capacité d'initiative dans les dispositifs de préparation ? Des projets dans plusieurs pays ont vu le jour pour rencontrer cette réalité.

En Région bruxelloise, le programme BRU response permet d'augmenter la résilience communautaire et de renforcer la capacité individuelle et collective à surmonter les crises au travers notamment de Réserves Citoyennes Communales de Sécurité Civile.

Le protocole : indispensable, mais pas toujours suffisant

1h50 : je suis enfin à bord du TGV. L'expérience met également en lumière la tension entre procédure et adaptation.

Les procédures sont indispensables. Elles sécurisent l'action, clarifient les responsabilités et évitent que chacun improvise dans son coin. Mais aucune procédure ne peut prévoir l'exhaustivité des combinaisons.

Dans le train, les deux contrôleurs ont ainsi dû composer avec une situation qui évoluait rapidement. Alors que leur protocole leur interdisait d'ouvrir les portes, ils ont pris une décision et adapté leur comportement. Dans un environnement dégradé, ils ont cherché à répondre aux besoins des passagers et à communiquer avec les moyens dont ils disposaient.

De la résilience à l'antifragilité

3h45 : arrivée à Bruxelles-midi. C'est ainsi que cette expérience donne, et c'est ce que je retiens le plus, un relief particulier à une notion abordée quelques heures auparavant : l'antifragilité.

La résilience permet d'absorber un choc et de continuer à fonctionner. L'antifragilité invite à aller plus loin : se nourrir du désordre et du hasard pour s'améliorer face à l'adversité. Et tenir bon.

Cultiver les options dans le chaos, c'est aussi savoir adapter ses décisions et ses modes d'action lorsque les circonstances évoluent, sans perdre de vue le cadre de sécurité et les responsabilités de chacun. C'est accepter l'incertitude et apprendre des écarts observés pour éviter, demain, des défaillances aux conséquences plus graves.

Conclusion

5h : enfin chez moi. Cette expérience n'est ni une critique des professionnels mobilisés, ni un jugement sur leur engagement. Elle constitue avant tout un retour d'expérience.

Elle rappelle qu'en situation de crise, les organisations sont confrontées à une réalité mouvante, où les procédures, les moyens, les informations et les comportements humains interagissent de manière difficilement prévisible.

Elle rappelle aussi que la préparation ne peut pas se limiter à construire des plans. Il faut les tester, les confronter à des scénarios dégradés, entraîner les acteurs à décider dans l'incertitude et associer davantage les citoyens à cette préparation. Surtout, il faut accepter qu'un bon dispositif de crise ne soit pas celui qui élimine toute incertitude, mais celui qui permet de continuer à agir malgré elle.

Quelques heures après avoir réfléchi à la résilience et l'antifragilité en formation, j'en ai fait l'expérience dans un train immobilisé.

Le scénario avait déraillé.

L'apprentissage, lui, ne faisait que commencer.

Hélène Charlier

Passionnée par la résilience communautaire, Hélène Charlier travaille pour le Gouverneur pour la gestion de crise en Région de Bruxelles-Capitale au sein de safe.brussels depuis 2023. Titulaire d'un master en criminologie, elle contribue notamment au développement du programme BRU response aux côtés des différents partenaires impliqués dans ce projet. Elle a travaillé auparavant dans le domaine de l'asile et migration puis dans les violences conjugales et intrafamiliales.

safe.brussels tps://safe.brussels/fr

BRU response ps://safe.brussels/fr/bru-response

Principe de communication de crise de réflexe : Processus Opérationnel en Communication de crise

Aiguillage de crise : mode d'emploi pour garder le cap

1- Préparer l'imprévisible, pas seulement le scénario idéal

Les plans sont indispensables, mais ils ne suffisent pas. Tester régulièrement les situations dégradées : perte de communication, absence d'un acteur clé, afflux de personnes vulnérables, changement soudain de situation… permet de révéler les véritables points de fragilité.

2- Faire de l'information une priorité opérationnelle

En situation de crise, ne pas avoir d'information est déjà une information. Même lorsqu'aucune réponse définitive n'est disponible, communiquer ce que l'on sait, ce que l'on ignore et dans la mesure du possible quand aura lieu la prochaine mise à jour permet de réduire l'incertitude, l'angoisse potentielle et d'éviter les rumeurs ou les initiatives désordonnées. Le principe de communication de crise de réflexe adoptée en Belgique : « We know – We do – We care – We'll back » aurait par exemple pu être utilisé (voir lien ci-après).

3- Partager une représentation commune de la situation : mettre en place une coordination opérationnelle et stratégique

Chaque intervenant peut disposer d'une information différente. La priorité est donc de construire rapidement une vision partagée : que s'est-il passé ? Quels sont les risques ? Qui fait quoi ? Quelles décisions ont été prises ? Quelles informations doivent circuler ? L'importance d'un PC-OPS (Poste de Commandement Opérationnel) n'est plus à démontrer.

4- Préparer les acteurs à sortir potentiellement du cadre

Les procédures donnent un cadre sécurisant, mais elles ne peuvent couvrir toutes les configurations. Les exercices devraient permettre aux équipes de s'entraîner à adapter une procédure lorsque les circonstances l'exigent, tout en maintenant la sécurité et la traçabilité des décisions.

5- Considérer le citoyen comme une ressource

Une population confrontée à une crise ne reste pas nécessairement passive ni individualiste. Elle s'organise, s'entraide et produit spontanément des solutions. Les dispositifs de préparation gagnent à intégrer cette capacité d'initiative pour autant qu'elle soit balisée et structurée plutôt qu'à la considérer uniquement comme un facteur de perturbation Un citoyen SPOC de référence par wagon aurait par exemple pu être identifié afin d'aider les contrôleurs à diffuser l'information au sein de leur wagon, à donner les recommandations ou encore à faire remonter les difficultés.

6- Transformer chaque crise en opportunité d'apprentissage

Le retour d'expérience ne doit pas chercher uniquement à déterminer « ce qui n'a pas fonctionné ». Il doit surtout permettre de répondre à d'autres questions : qu'avons-nous appris ? Que devons-nous changer ? Que devons-nous tester maintenant ?

Quand les lumières s'éteignent, les idées s'allument.

Trois villes. Une même expérience.

Et si, demain matin, l’électricité disparaissait ?

Plus de courant. Plus de réseau. Les communications deviennent difficiles. Les informations se font rares.

C'est cette réalité que des participants de Québec, Montréal et Paris ont choisi de vivre pendant une journée.

Venus chercher des réponses, ils sont surtout repartis avec une meilleure compréhension de ce qu'est réellement un blackout, de ses conséquences et de l'importance de s'y préparer bien avant que les lumières ne s'éteignent.

Karine Maréchal-Richard

Experte en continuité des affaires et en gestion de crise. Consultante, formatrice et conférencière dans les domaines de la continuité des affaires et de la gestion de crise.

Alexandre Fournier

Expert en gestion et simulation de crise
Consultant, formateur et conférencier dans les domaines de la continuité des affaires et de la gestion de crise depuis 30 ans.

Il existe des événements dont on se souvient pour les conférences. Et puis il y a ceux dont on se souvient pour les conversations. Celles qui commencent autour d'une table, se poursuivent pendant la pause-café et continuent longtemps après le retour au bureau.

Les Journées Blackout ont été de ceux-là. Elles ont réuni des professionnels venus d'univers très différents : responsables de sécurité civile, gestionnaires, dirigeants, spécialistes des technologies de l'information, représentants municipaux, intervenants du réseau de la santé, organisations publiques et entreprises privées.

Tous partageaient une même question :

sommes-nous réellement prêts lorsqu'une crise dépasse nos scénarios habituels ?

À travers les trois éditions de Québec, Montréal et Paris, les réponses ont été nombreuses. Mais elles n'ont pas toujours été celles que l'on attendait.

L'objectif des Journées Blackout était de sensibiliser les participants à la réalité d'un blackout majeur, qu'il touche leur organisation ou leur vie familiale. Car se préparer à un tel événement ne consiste pas seulement à disposer de plans et de procédures.

C'est aussi développer les bons réflexes, réfléchir aux décisions qui devront être prises et amorcer les conversations qui permettront d'être mieux préparés lorsque l'imprévu surviendra.

Une expérience plutôt qu'une formation

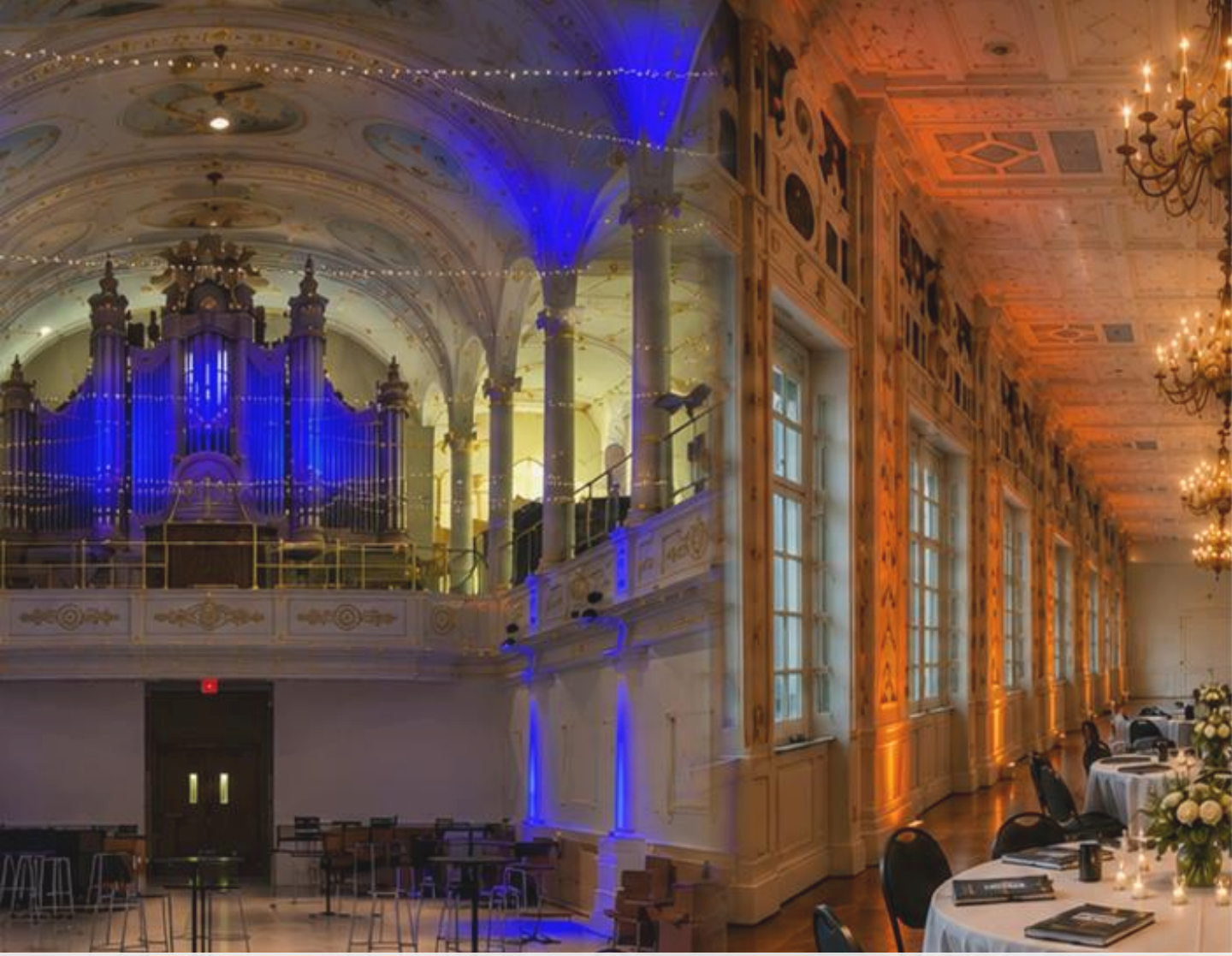
Dès les premières minutes, les participants comprennent qu'ils ne sont pas venus assister à une formation comme les autres. Ils sont là pour vivre une expérience.

Car un blackout ne se résume pas à une panne d'électricité. Il fait progressivement disparaître les repères habituels.

Les communications deviennent plus difficiles. Les informations arrivent au compte-gouttes. Les priorités évoluent. Pourtant, les décisions, elles, ne peuvent pas attendre.

Tout au long de la journée, les participants sont confrontés à des situations inspirées de cas réels. Ils doivent :

analyser rapidement, faire des choix avec une information imparfaite, débattre et adapter leur stratégie à mesure que la situation évolue.



L’objectif n’est pas de trouver une réponse unique. Il est de se confronter à la complexité d’un blackout, d’en mesurer les conséquences et de comprendre les défis qu’il impose aux organisations comme aux familles. Ce qui paraît simple sur papier devient souvent beaucoup plus difficile lorsque l’information manque, que les priorités se multiplient et que les décisions ne peuvent être reportées.

Trois villes, trois atmosphères

Les Journées Blackout ont pris vie dans trois lieux aussi différents qu'inspirants : une ancienne église à Québec, la salle Toundra à Montréal et le Salon des Lumières à Paris.

Trois décors chargés d'histoire, trois ambiances bien distinctes, mais une même volonté : créer les conditions propices à la réflexion, aux échanges et à l'apprentissage collectif.

À Québec, l'ancienne église permettait de recréer une véritable ambiance de blackout. Les rideaux tirés plongeaient progressivement la salle dans la pénombre. Les lampes rechargeables devenaient les seules sources de lumière. Sans artifices, l'environnement obligeait chacun à sortir de son quotidien et à se projeter dans un contexte où les repères habituels avaient disparu.

À Montréal, la salle Toundra vibrait d'une énergie différente. Les ateliers prenaient rapidement vie, les idées circulaient d'une table à l'autre et les discussions se poursuivaient bien au-delà des exercices. Les participants confrontaient leurs réalités, partageaient leurs expériences et enrichissaient mutuellement leurs réflexions.

À Paris, le Salon des Lumières offrait un contraste saisissant. En pleine canicule, la chaleur rappelait que les crises prennent toujours une couleur particulière selon le contexte dans lequel elles surviennent. Dans ce lieu chargé d'histoire, les échanges demeuraient tout aussi riches, portés par la curiosité, la diversité des parcours et une même envie de mieux se préparer.

Les décors étaient différents. Les conditions aussi. Pourtant, une constante s'est retrouvée dans les trois villes : la qualité des échanges, la générosité des participants et cette impression que chacun apprenait autant des autres que du scénario proposé.

Ce sont ces trois atmosphères, chacune avec sa personnalité, qui ont donné aux Journées Blackout leur caractère si particulier.

Les véritables experts étaient aussi dans la salle

En relisant les questionnaires d'évaluation, un constat s'impose rapidement. Les conférences ont été très appréciées, mais ce qui revient le plus souvent dans les commentaires, ce sont les échanges entre les participants. Les ateliers, les discussions autour des tables, les regards croisés et les expériences partagées ont profondément marqué les esprits.

À plusieurs reprises, les mêmes idées reviennent.

« Les ateliers ont permis d'échanger notre réalité avec celles des autres participants. Les trois conférences étaient excellentes. »

« Les échanges avec les personnes autour de la table et les exemples concrets des conférenciers ont été les moments les plus marquants. »

« Les ateliers étaient bien structurés et il y avait suffisamment de temps pour échanger avec les autres participants. »

Pendant une journée, les silos disparaissent. Une municipalité découvre les préoccupations d'une entreprise privée. Un spécialiste des technologies de l'information nourrit la réflexion d'un gestionnaire RH. Un responsable de la sécurité civile échange avec un dirigeant de PME.

Mais certains apportaient aussi un vécu que l'on ne retrouve dans aucun manuel. Quelques participants avaient déjà traversé un blackout majeur. D'autres venaient de régions où les cyclones, les tempêtes ou les interruptions prolongées de services essentiels font partie de la réalité. Certaines organisations avaient développé, au fil des ans, une véritable culture de préparation, tandis que d'autres amorçaient tout juste leur réflexion.

Très vite, ces expériences prennent autant de valeur que le scénario lui-même. On ne parle plus seulement de ce qu'il faudrait faire :

on partage ce qui a réellement fonctionné, les erreurs commises, les difficultés rencontrées et les solutions trouvées sur le terrain.
C'est là que réside la véritable richesse de ces journées.
Elle ne vient pas uniquement des conférences ou des intervenants, mais de la diversité des personnes réunies autour de la même table et de l'intelligence collective qui naît de leurs échanges.

Lorsqu'un professionnel partage une expérience vécue, il ne transmet pas seulement des connaissances : il permet aux autres d'imaginer plus concrètement ce que signifie traverser une crise. En situation de crise, aucune organisation ne détient seule toutes les réponses.

Une journée qui fait réfléchir… et surtout agir

Les Journées Blackout n'avaient pas pour objectif de faire peur. Elles visaient à faire réfléchir. Et surtout, à donner envie d'agir.

Les réponses recueillies montrent que les participants repartent rarement avec une simple idée. Les actions envisagées sont très concrètes :

- Préparer une trousse d'urgence,
- Revoir un plan de continuité,
- Identifier les clients prioritaires,
- Tester un scénario avec son équipe,
- Sensibiliser sa famille
- Ou encore partager les apprentissages avec ses collègues.

Les témoignages parlent d'eux-mêmes.

« Je rentre avec de nombreuses idées concrètes à mettre en pratique avec ma famille. »

« Je repars avec de nouvelles idées et moins de zones d'ombre pour affiner nos plans. »

« Je réalise que je n'étais pas aussi préparé que je le croyais. »

« Ce n'est pas une question de si, mais de quand cela va arriver. »

Ces phrases racontent peut-être mieux que tout le reste ce qu'ont produit les Journées Blackout. Plus qu'un transfert de connaissances, elles ont provoqué une prise de conscience. Elles ont amené les participants à regarder autrement leur propre niveau de préparation, autant dans leur organisation que dans leur vie personnelle.

Avant de quitter les lieux, chaque participant repart avec une mini trousse de survie préparée par Crise & Résilience contenant :

- Une lampe rechargeable
- Couverture de survie
- Pastilles pour purifier l'eau
- Biscuits
- Crayons et carte réflexe

Une ambiance qui donne envie de revenir

Les chiffres témoignent d'un haut niveau de satisfaction. Les évaluations sont excellentes. La très grande majorité des participants recommanderaient la journée à leurs collègues et nombreux sont ceux qui souhaitent déjà participer à une prochaine édition. Mais les statistiques racontent seulement une partie de l'histoire. Ce qui marque davantage, ce sont les mots utilisés par les participants.

Enrichissante, inspirante, pertinente, concrète, productive, conscientisation.

Ces mots reviennent sans cesse. Ils décrivent une journée où l'on apprend, mais surtout où l'on échange.

Une journée où chacun apporte son expérience et repart enrichi de celle des autres.

Ce que nous retenons

En organisant ces trois éditions, nous voulions ouvrir un espace de réflexion autour d'un scénario encore peu exploré : le blackout de grande ampleur. Au fil des rencontres, une conviction s'est imposée. La résilience ne se construit pas uniquement à travers des plans, des procédures ou des exercices. Elle se construit aussi dans les conversations, les retours d'expérience et la capacité d'écouter ceux qui vivent les mêmes défis sous un angle différent.

Une autre leçon nous a tout autant marqués. Les participants ne sont pas seulement venus apprendre : ils sont aussi venus partager. Au fil des ateliers, des idées ingénieuses ont émergé des échanges. Certaines étaient d'une simplicité désarmante. D'autres remettaient en question des façons de faire que l'on croyait bien établies. Chaque groupe apportait sa réalité, ses contraintes et ses solutions. Très souvent, une idée lancée par un participant faisait évoluer la réflexion de toute la salle.

C'est sans doute la plus belle démonstration de l'intelligence collective. Lorsque des professionnels issus d'univers différents confrontent leurs expériences, leurs expertises et leurs points de vue, les réponses deviennent plus riches, plus nuancées et souvent plus concrètes que celles qu'une organisation pourrait construire seule.

Au fond, les Journées Blackout n'ont pas seulement permis de mieux comprendre le risque de blackout. Elles ont créé un espace où chacun pouvait remettre certaines certitudes en question, enrichir sa réflexion et repartir avec des idées concrètes à mettre en œuvre.

Les Journées Blackout nous auront rappelé une chose essentielle : lorsque les lumières s'éteignent, les meilleures idées naissent rarement d'une seule personne. Elles prennent forme lorsque les expériences se rencontrent, que les perspectives se croisent et que l'intelligence devient véritablement collective.

À toutes celles et ceux qui ont participé aux Journées Blackout de Québec, Montréal et Paris, merci. Vous avez fait bien plus que prendre part à un événement. Vous avez contribué à faire vivre une réflexion collective qui, nous l'espérons, continuera bien au-delà de cette tournée. Car, face aux crises, nous sommes toujours plus forts lorsque nous apprenons ensemble.

Alexandre Fournier

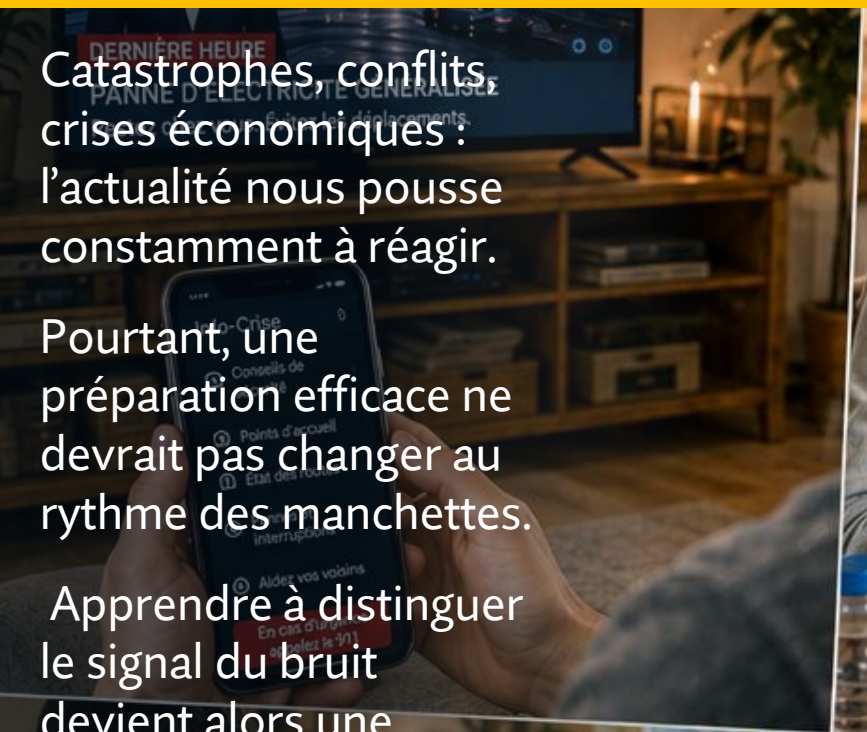
Karine Maréchal Richard

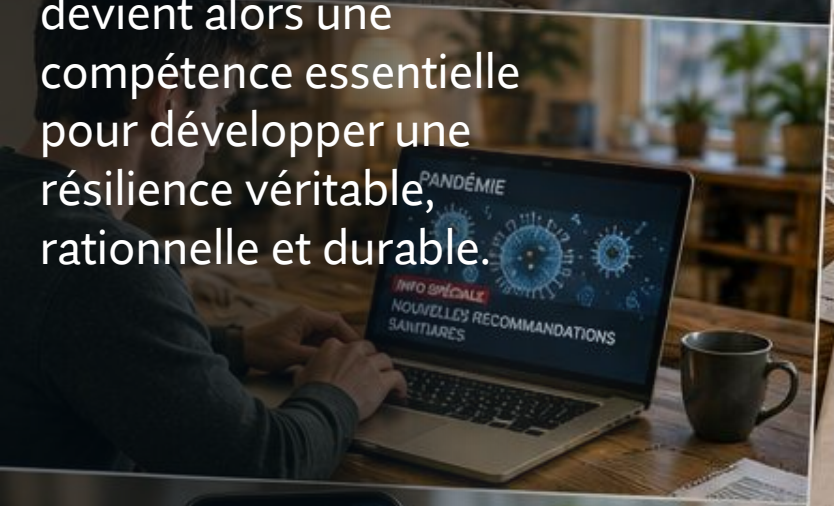
Se préparer sans céder au cycle anxiogène des nouvelles.

Catastrophes, conflits, crises économiques : l'actualité nous pousse constamment à réagir.

Pourtant, une préparation efficace ne devrait pas changer au rythme des manchettes.

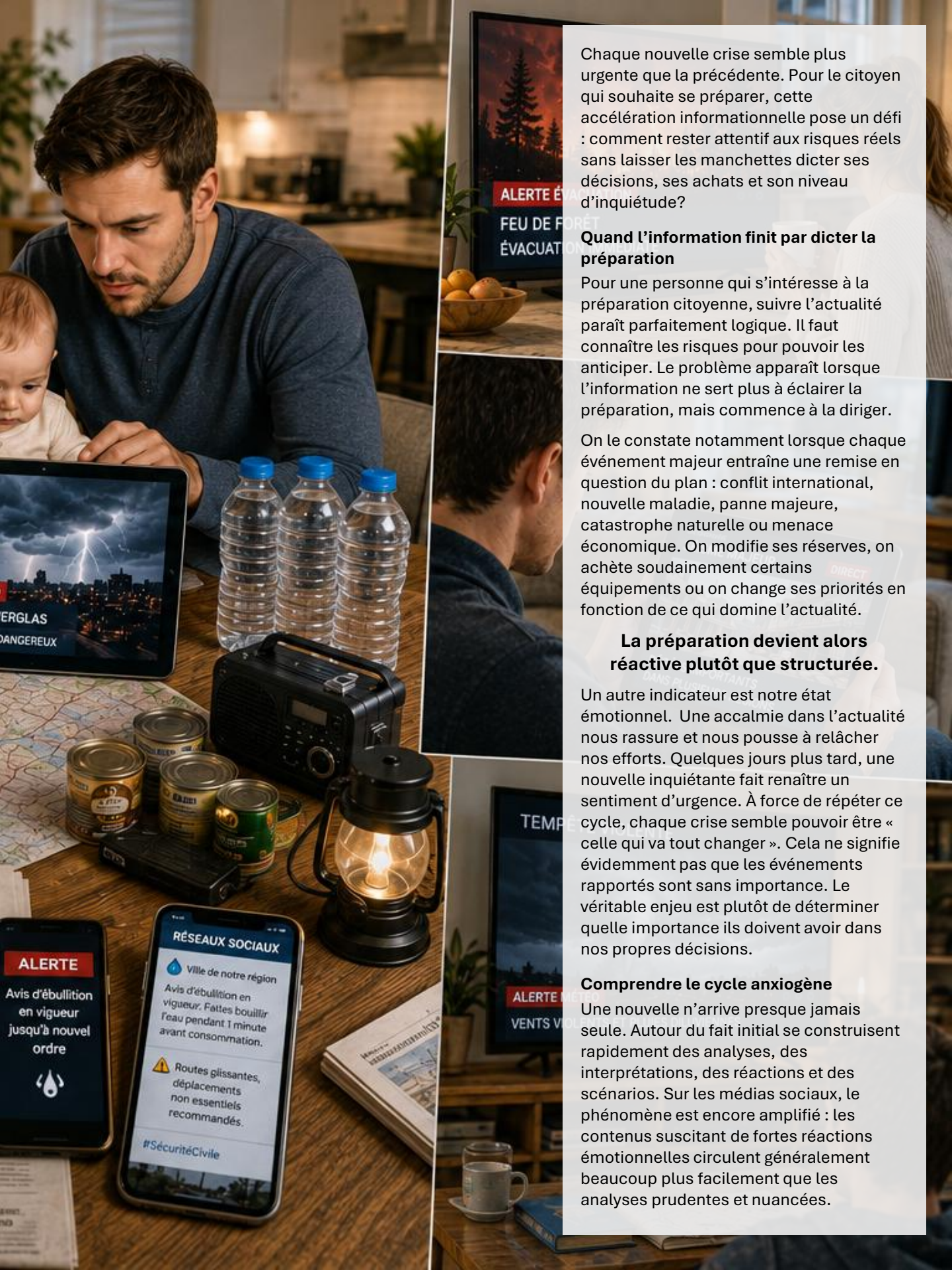
Apprendre à distinguer le signal du bruit devient alors une compétence essentielle pour développer une résilience véritable, rationnelle et durable.





Mathieu Montaroux

Expert-conseils en mesures d'urgence et résilience organisationnelle
Résilience organisationnelle, mesures d'urgence et préparation citoyenne



Chaque nouvelle crise semble plus urgente que la précédente. Pour le citoyen qui souhaite se préparer, cette accélération informationnelle pose un défi : comment rester attentif aux risques réels sans laisser les manchettes dicter ses décisions, ses achats et son niveau d'inquiétude?

Quand l'information finit par dicter la préparation

Pour une personne qui s'intéresse à la préparation citoyenne, suivre l'actualité paraît parfaitement logique. Il faut connaître les risques pour pouvoir les anticiper. Le problème apparaît lorsque l'information ne sert plus à éclairer la préparation, mais commence à la diriger.

On le constate notamment lorsque chaque événement majeur entraîne une remise en question du plan : conflit international, nouvelle maladie, panne majeure, catastrophe naturelle ou menace économique. On modifie ses réserves, on achète soudainement certains équipements ou on change ses priorités en fonction de ce qui domine l'actualité.

La préparation devient alors réactive plutôt que structurée.

Un autre indicateur est notre état émotionnel. Une accalmie dans l'actualité nous rassure et nous pousse à relâcher nos efforts. Quelques jours plus tard, une nouvelle inquiétante fait renaître un sentiment d'urgence. À force de répéter ce cycle, chaque crise semble pouvoir être « celle qui va tout changer ». Cela ne signifie évidemment pas que les événements rapportés sont sans importance. Le véritable enjeu est plutôt de déterminer quelle importance ils doivent avoir dans nos propres décisions.

Comprendre le cycle anxiogène

Une nouvelle n'arrive presque jamais seule. Autour du fait initial se construisent rapidement des analyses, des interprétations, des réactions et des scénarios. Sur les médias sociaux, le phénomène est encore amplifié : les contenus suscitant de fortes réactions émotionnelles circulent généralement beaucoup plus facilement que les analyses prudentes et nuancées.

Une situation complexe peut ainsi rapidement devenir une succession de messages simplifiés : il faut avoir peur, être rassuré, s'indigner ou choisir un camp.

S'ajoute à cela la vitesse du cycle informationnel. Une information présentée comme déterminante le matin peut être nuancée quelques heures plus tard, puis contredite le lendemain. Pour celui qui tente d'adapter continuellement sa préparation à ce flux, il devient extrêmement difficile de conserver des priorités stables.

Le problème n'est donc pas de s'informer.

Il est de confondre l'importance médiatique d'un événement avec son importance réelle pour notre propre niveau de risque.

Une crise internationale peut être extrêmement importante sans nécessiter que votre famille change quoi que ce soit aujourd'hui. À l'inverse, une alerte météorologique locale relativement peu spectaculaire peut justifier des actions immédiates. Cette distinction est fondamentale.

Du risque médiatisé au risque réel

La préparation citoyenne devrait d'abord répondre à une réalité beaucoup plus proche :

- Notre territoire;
- Notre habitation;
- Notre famille;
- Nos vulnérabilités;
- Et les risques auxquels nous sommes réellement exposés.

Une panne de courant prolongée, une tempête hivernale, une interruption d'approvisionnement en eau, un incendie résidentiel ou une évacuation peuvent avoir beaucoup plus d'incidence sur un ménage québécois qu'un événement international pourtant omniprésent dans les médias.

Pourtant, le risque le plus médiatisé tend naturellement à occuper davantage notre esprit.

C’est ainsi que certaines personnes accumulent soudainement un type de matériel en réaction à une crise, avant de passer à une autre préoccupation quelques semaines plus tard.

Le résultat peut être une accumulation d’équipements sans véritable cohérence, alors que des besoins fondamentaux demeurent parfois négligés.

Une préparation structurée fonctionne exactement à l’inverse.

Elle commence par :

- Identifier les risques pertinents;
- Développer progressivement des capacités permettant de répondre à plusieurs situations :
    - Disposer d’eau et de nourriture,
    - Pouvoir traverser une panne de courant,
    - Communiquer avec ses proches,
    - Évacuer rapidement,
    - Posséder une certaine autonomie financière
    - Et connaître les ressources disponibles dans sa communauté.

Ces capacités restent utiles indépendamment des manchettes du jour.

Retrouver une préparation calme et progressive

L’objectif n’est donc certainement pas de se couper de l’information. Il s’agit plutôt de retrouver une distance suffisante pour que l’information demeure un outil d’aide à la décision.

Lorsqu’un événement survient, la première question ne devrait pas être :

« Est-ce grave? », mais plutôt :
« Est-ce que cela modifie concrètement mon niveau de risque? »

Cette différence change complètement la manière de se préparer.

Elle permet également de revenir à une réalité souvent beaucoup moins spectaculaire, mais beaucoup plus importante :

- Connaît-on le plan familial en cas d'urgence?
- Les réserves essentielles sont-elles suffisantes?
- Les détecteurs de fumée fonctionnent-ils?
- Avons-nous une solution lors d'une panne prolongée?
- Savons-nous où aller si nous devons évacuer?

Un ménage qui maîtrise ces éléments possède déjà une résilience considérable, même s'il ne suit pas les nouvelles, heure par heure.

La préparation citoyenne est fondamentalement une démarche de long terme.

Elle se construit progressivement, lorsque tout va bien, plutôt que dans l'urgence provoquée par la crise du moment. S'informer demeure nécessaire. Mais savoir

filtrer, hiérarchiser et remettre l'information dans son contexte

fait désormais partie des compétences essentielles de la résilience.

Car au bout du compte, l'objectif de la préparation n'est pas d'avoir peur avant les autres.

C'est d'avoir suffisamment anticipé pour pouvoir rester calme lorsque les autres commencent à avoir peur.

Se préparer ne signifie pas anticiper chaque crise ni réagir à chaque nouvelle inquiétante. Il s'agit plutôt de développer progressivement les capacités qui permettent de faire face à l'imprévu. L'information demeure essentielle, mais elle doit éclairer nos décisions plutôt que les dicter. Une préparation fondée sur les risques réels, les besoins de son foyer et des actions concrètes procure quelque chose que le cycle des nouvelles ne pourra jamais offrir : de l'autonomie, de la confiance et la capacité de traverser une situation difficile avec davantage de calme.

Mathieu Montaroux

Expert en résilience et mesures d'urgence, Mathieu Montaroux œuvre depuis plus de 20 ans dans les domaines de l'urgence, de la sécurité et de la préparation. Il est également fondateur de Québec Preppers, plateforme québécoise consacrée à la préparation citoyenne.
Site Web : www.quebecpreppers.com

5 réflexes pour ne plus préparer selon les manchettes

1. Appliquez le filtre des 72 heures

Lorsqu'une nouvelle vous inquiète, demandez-vous : Est-ce que cet événement peut réellement affecter ma famille ou ma région dans les 72 prochaines heures? Si la réponse est non, évitez de modifier immédiatement votre préparation.

2. Cherchez l'information à la source

Avant d'agir, consultez les sources directement responsables du risque concerné : autorités municipales, sécurité civile, Environnement et Changement climatique Canada, services d'urgence ou organismes spécialisés. Une donnée vérifiable devrait toujours avoir plus de poids qu'un commentaire ou une publication virale.

3. Identifiez ce qui change réellement

Demandez-vous ensuite : Cette information révèle-t-elle une vulnérabilité que je n'avais pas prévue? Si votre plan couvre déjà la situation, poursuivez simplement votre préparation. Une nouvelle inquiétante ne nécessite pas automatiquement une nouvelle action.

4. Revenez aux besoins fondamentaux

Avant d'acheter un nouvel équipement, vérifiez vos capacités essentielles : eau, nourriture, médicaments, éclairage, communications, chauffage, finances, évacuation et plan familial. Corriger une faiblesse réelle est généralement plus utile que préparer le scénario médiatisé du moment.

5. Transformez l'inquiétude en une action proportionnée

Si un risque mérite réellement votre attention, choisissez une action concrète : compléter une réserve, vérifier un équipement, discuter du plan familial ou consulter une alerte officielle. Puis revenez à votre plan.

La bonne question n'est donc pas : « De quoi devrais-je avoir peur aujourd'hui? », ... mais plutôt :

« Qu'est-ce que je peux raisonnablement améliorer aujourd'hui pour être plus résilient demain? »

Quand le numérique lâche, la résilience hospitalière se mesure.

À l'hôpital, tout le monde parle de résilience.

Jusqu'au jour où les écrans s'éteignent, où les résultats n'arrivent plus et où le mode dégradé sort des procédures pour entrer dans la vraie vie.

La question n'est plus de savoir si cela arrivera, mais comment l'établissement tiendra quand le numérique recule…
ou quand un "kill switch", autrement dit un mécanisme d'arrêt d'urgence, lointain, coupe l'IA dont il dépend.

Pascal Nahon

Directeur Cyber / Agence Paris IDF / Atos Group
Gouvernance, Risques, Conformité et notamment organisation de gestion de crise

La cyberattaque hospitalière n'est plus un cas d'école, c'est un stress test grandeur nature pour l'organisation, les équipes et la gouvernance.

Avec l'essor des IA embarquées dans les systèmes de santé, une autre réalité s'impose : nos hôpitaux peuvent devenir dépendants de décisions technologiques ou géopolitiques prises à des milliers de kilomètres.

La résilience ne se décrète pas,
elle se construit… et
elle s'ancre aussi dans la souveraineté.

Quand le numérique s'arrête, l'hôpital se révèle

Un hôpital moderne fonctionne comme un organisme finement interconnecté. Dossier patient informatisé, prescription connectée, imagerie, biologie, pharmacie, bloc opératoire, dispositifs médicaux : tout est lié, tout circule, tout s'accélère.

En routine, c'est un formidable accélérateur de qualité et de sécurité des soins. En crise, c'est aussi un amplificateur de dépendances.

Une cyberattaque, une panne majeure, une coupure réseau ne provoquent pas seulement une interruption de service : ils mettent à nu la manière dont l'hôpital s'organise, décide et communique lorsque le confort numérique disparaît.

Le numérique a renforcé l'hôpital, mais il l'a aussi rendu plus vulnérable à certains chocs.

La vraie question n'est pas de savoir si les équipes informatiques sont compétentes – elles le sont souvent, et très engagées – mais : combien de temps l'hôpital peut-il continuer à soigner correctement lorsque les outils numériques se taisent ?

Un *"kill switch"* qui n'est pas dans le sous-sol de l'hôpital

Avec l'arrivée de modèles d'IA avancés comme Mythos 5 et Fable 5 d'Anthropic, capables d'analyser des flux, d'optimiser des décisions et, potentiellement, d'être intégrés dans des dispositifs médicaux ou des plateformes de décision clinique, une nouvelle dépendance apparaît :

la dépendance à un modèle d'IA
opéré par un acteur non européen,
soumis au droit d'un État tiers.

L'épisode de la coupure brutale de Mythos 5 et Fable 5 pour l'ensemble des utilisateurs non américains a montré que cette dépendance n'est pas théorique.

En une lettre de l'administration américaine, deux modèles utilisés dans le monde entier ont été désactivés, rappelant très concrètement que :

- Le "bouton OFF" peut être situé hors d'Europe ;
- L'accès à un modèle d'IA peut être interrompu pour des raisons de sécurité nationale, de régulation ou de politique industrielle ;
- Les utilisateurs finaux héritent de la conséquence, sans avoir voix au chapitre.

Vu depuis un hôpital français, cela signifie qu'un dispositif biomédical ou un logiciel clinique reposant massivement sur une IA externe peut se retrouver instantanément amputé d'une partie de ses capacités, non pas à cause d'un ransomware, mais à la suite d'une décision réglementaire étrangère. C'est une forme de *"kill switch"* souverain : l'interrupteur n'est plus dans la salle technique, il est au cœur d'une capitale alliée, mais pas neutre.

Dispositifs médicaux, IA embarquée et dépendances cachées

L'intégration d'IA avancées dans le biomédical et le médical est déjà en cours : aides à la décision, interprétation d'images, optimisation de flux, maintenance prédictive, pilotage de certains dispositifs. Même lorsque l'IA n'est pas directement dans l'appareil, elle peut être dans la plateforme cloud qui le pilote, le met à jour ou le surveille.

Cette intégration crée de nouveaux points de fragilité :

- Un dispositif médical (DM) qui reste physiquement fonctionnel mais perd ses algorithmes d'aide à la décision ;
- Un système d'imagerie qui devient "aveugle" à ses propres outils d'analyse ;
- Un orchestrateur de bloc opératoire ou de lits dont les moteurs d'IA sont soudain indisponibles.

Le risque n'est pas seulement technique : il devient stratégique dès lors que ces briques reposent sur des IA opérées depuis l'étranger, sans plan B. L'hôpital dépend alors de la continuité d'accès à ces services, donc de décisions prises par un autre État.

Pourquoi cela renforce la nécessité du mode dégradé

On pourrait être tenté de répondre : « dans ce cas, il n'y a qu'à espérer que le service ne soit jamais coupé ». Mais l'épisode Fable 5 et Mythos 5 a montré l'inverse : une coupure peut intervenir soudainement, de manière unilatérale, pour des raisons qui échappent totalement aux utilisateurs finaux.

Pour les hôpitaux, cela renforce trois exigences :

- Disposer de procédures dégradées éprouvées, pas seulement en cas de panne interne ou de cyberattaque, mais aussi en cas de retrait soudain d'un service d'IA critique ;
- S'assurer que les dispositifs médicaux restent utilisables en sécurité sans la surcouche d'IA (au besoin avec un niveau de performance moindre, mais acceptable) ;
- Intégrer ce risque de "kill switch externe" dans la réflexion sur la souveraineté en santé : que se passe-t-il si, demain, un modèle d'IA central dans un parcours de soins est suspendu pour l'Europe ?

Plans, procédures… et réalité du terrain

Dans la plupart des établissements, les plans de gestion de crise et de continuité d'activité existent. Ils ont été rédigés avec sérieux, validés en instances, parfois enrichis au fil des retours d'expérience. Le sujet n'est donc pas l'absence de plan, mais l'écart classique entre le document et la pratique.

Entre un plan bien construit et une crise bien gérée, il reste quelques zones de turbulence :

- Des responsabilités définies sur le papier, mais parfois floues en situation réelle ;
- Des procédures de "mode dégradé" connues des encadrants, mais moins des équipes de nuit ou des remplaçants ;
- Des parcours de soins pensés pour le numérique et, de plus en plus, pour des services d'IA externes, qui n'ont pas été révisés en version "papier + téléphone + expertise clinique humaine".

Et il faut le dire : les soignants, eux, vivent déjà des micro-crises numériques toute l'année. Un serveur d'imagerie en panne, un accès labo indisponible, une application de prescription qui ralentit… Pour eux, la résilience n'est pas un concept nouveau. C'est parfois leur quotidien, géré avec des "trucs et astuces", de l'ingéniosité et beaucoup de bonne volonté.

L'enjeu pour les directions, les DSI, les services biomédicaux et les RSSI n'est donc pas de "créer" la résilience, mais de canaliser, organiser et sécuriser cette capacité d'adaptation existante, afin qu'elle reste compatible avec la sécurité des soins… et avec le droit.

Quand l'IA aide à se mettre à la place de l'attaquant… et du régulateur étranger

L'arrivée d'outils d'IA générative change aussi la donne. Des modèles comme Mythos 5 ou Fable 5, et d'autres solutions du même esprit, permettent aujourd'hui de générer des scénarios de crise très réalistes, adaptés à un établissement, à un territoire, à un plateau technique précis.

On peut, en quelques minutes, imaginer :

- Une attaque chiffrante qui touche d'abord la biologie ;
- Un blocage partiel des accès aux données de radiologie ;
- Un logiciel biomédical critique qui devient subitement indisponible ;
- Un scénario où une décision réglementaire coupe l'accès à un modèle d'IA embarqué dans plusieurs briques du système d'information.

Utilisée ainsi, l'IA n'est pas qu'un gadget : c'est un moyen d'explorer les zones grises, de tester les effets domino auxquels on ne pense pas toujours, y compris ceux qui viennent de décisions extérieures à l'hôpital… et même extérieures à l'Europe.

Le message n’est pas de dire que “l’IA américaine est dangereuse par nature”. Le message est que toute dépendance univoque à un acteur unique, situé hors de notre cadre juridique, crée un risque systémique. L’enjeu, pour les directions et les RSSI, est de s’approprier ces outils pour imaginer, à froid, les conséquences de ce type de coupure et prévoir des marges de manœuvre.

Un sujet de gouvernance… et de souveraineté en santé

La cyber résilience à l’hôpital n’est plus un sujet réservé à la DSI ou au RSSI. Elle touche la continuité des soins, la gestion des risques, les dispositifs médicaux, la conformité réglementaire, la communication de crise et, de plus en plus, la souveraineté opérationnelle des établissements.

Lorsque la direction générale, les instances médicales, la DSI, le biomédical et les équipes de soins se mettent autour de la table, la question change : il ne s’agit plus seulement de savoir si le pare-feu est à jour, mais de prioriser les activités vitales, d’identifier les points de dépendance critiques à des services d’IA non européens, de prévoir des alternatives locales et d’assumer les arbitrages en cas de coupure.

Les directeurs d’hôpitaux, les médecins, les équipes biomédicales et les RSSI sont souvent les premiers à porter ce discours, parfois avec des moyens contraints et des équipes sous tension. Leur rôle n’est pas de promettre l’invulnérabilité – elle n’existe pas – mais de rendre l’établissement capable de continuer à soigner, même quand une partie du numérique, ou de l’IA qui le fait fonctionner, se retrouve soudain inaccessible.

Dans ce cadre, l’exercice de crise n’est plus un passage obligé pour “cocher une case”, mais un outil de pilotage stratégique : il révèle où l’hôpital est solide, où il est fragile, où il dépend d’un fournisseur unique, et où il doit investir pour regagner des marges de manœuvre, y compris en soutenant des solutions plus souveraines.

La cybercrise à l'hôpital n'est plus un scénario théorique ; elle fait désormais partie du paysage des risques. L'épisode Mythos 5 et Fable 5 a ajouté une couche supplémentaire : la prise de conscience qu'un *"kill switch"* géopolitique peut couper, du jour au lendemain, l'accès à une IA largement intégrée dans les pratiques.

Face à cette réalité, la résilience hospitalière se mesure moins au nombre de pages des plans qu'à la capacité des équipes à se réorganiser lorsque le numérique lâche, qu'une IA embarquée devient muette ou qu'un fournisseur étranger se retire. Pour les directions, les DSI, le biomédical et les RSSI, l'enjeu est double : faire vivre les procédures dégradées, et inscrire l'hôpital dans une trajectoire de souveraineté opérationnelle en santé.

Atos in Pascal Nahon

Avec une carrière impressionnante dans la tech et la cybersécurité, Pascal est une figure incontournable du secteur. Depuis plus de 30 ans, il explore les arcanes du numérique, de l'exploitation des systèmes à la gouvernance SSI, en passant par les tests d'intrusion, la gestion de crise et l'IA.

Aujourd'hui Directeur Cybersécurité de l'agence Atos Paris / Ile de France, il conjugue expertise technique, vision stratégique et capacité à embarquer les organisations dans une véritable culture cyber. Passé par la banque, le retail, la santé ou encore la supply chain — sans oublier une aventure entrepreneuriale à l'international de plus d'une décennie — Pascal a vu le numérique évoluer… et les cybermenaces avec.

Son regard éclairé sur les enjeux actuels de la cybersécurité et de l'IA en fait un interlocuteur qui compte, capable de vulgariser sans simplifier, et de faire réfléchir sans moraliser.

Sans prétention, mais avec conviction, il continue de sensibiliser, d'accompagner et de faire progresser les structures.

Toujours avec un pas de côté et un brin d'humour, Pascal partage son expérience sans dogmatisme. Il sait que la cybersécurité n'est jamais acquise, que les certitudes sont souvent les premières failles, et que le bon sens fait parfois plus que les grandes théories. Il sait que dans ce métier, on n'a jamais vraiment « tout vu ». Et tant mieux : c'est ce qui le pousse à rester alerte, à apprendre encore, et à transmettre sans jamais se prendre trop au sérieux. Il préfère les échanges concrets aux discours figés, et les discussions humaines aux grandes incantations techniques. Bref, un passionné qui garde les pieds sur terre — et les systèmes sous contrôle, autant que possible.

5 leviers concrets pour faire vivre la résilience

Clarifier les activités vitales, sans ambiguïté : Identifier et prioriser les activités qui doivent absolument continuer : urgences, réanimation, bloc, maternité, biologie et imagerie critiques, pharmacie clinique, plateau technique biomédical indispensable. Cette hiérarchisation doit être discutée et validée au niveau de la gouvernance, puis traduite en décisions concrètes en cas de crise : qui protège-t-on, qui bascule-t-on en mode dégradé, avec ou sans IA.

Cartographier les vraies dépendances… y compris aux IA externes : Pour chaque activité vitale, recenser les applications, réseaux, dispositifs biomédicaux, prestataires et services d'IA tiers. Identifier les points uniques de panne : modèles d'IA, clouds ou API indispensables à un processus critique. L'objectif n'est pas une carte parfaite, mais une vision claire pour savoir quoi protéger, quoi rétablir en premier… et où un "kill switch" extérieur pourrait frapper.

Construire des scénarios qui interrogent, pas qui accusent : S'appuyer sur l'IA générative (Mythos 5, Fable 5 ou équivalents) pour imaginer des scénarios réalistes et adaptés à l'établissement. Travailler sur quelques scénarios ciblés, qui font ressortir les vraies questions : qui décide, quoi arrêter, quoi maintenir, avec quels moyens, et que fait-on si un fournisseur d'IA coupe l'accès à son modèle ?

Multiplier les exercices courts et réalistes : Organiser des exercices réguliers, de petite ampleur, intégrés dans le fonctionnement normal : une matinée sans DPI dans un service, une simulation de blocage d'imagerie, une chaîne labo–urgences ralentie, une perte simulée d'un service d'IA utilisé pour la planification ou l'aide à la décision. Ce format limite l'impact sur l'activité et permet d'ancrer les réflexes nécessaires en cas de coupure réelle, technique ou géopolitique.

Faire de la direction un joueur sur le terrain… et un acteur de souveraineté : Associer la direction, le comité de direction, la Commission Médicale d'Établissement (CME), la Commission des Soins Infirmiers, de Rééducation et Médico-Techniques (CSIRMT), la DSI, le biomédical et la gestion des risques aux exercices. Les décisions prises en simulation doivent ressembler à celles qu'il faudra assumer en réel : hiérarchiser, trancher, expliquer, éventuellement renoncer temporairement à certains usages avancés de l'IA pour protéger le cœur des soins. Plus la gouvernance est présente dans ces exercices, plus l'hôpital sera à l'aise pour défendre, dans la durée, une stratégie de résilience et de souveraineté en santé.

CRISE & RÉSILIENCE

ANTICIPER | RÉAGIR | REBONDIR

De la planification à l'action.

FORMATION

CONSTRUISEZ VOTRE PROPRE EXERCICE DE GESTION DE CRISE

DES ÉQUIPES MIEUX PRÉPARÉES POUR UN AVENIR PLUS RÉSILIENT.

Pas un modèle générique.
Pas un exercice fictif.

Le vôtre.

VOTRE SCÉNARIO

Un scénario réaliste et adapté à votre réalité

VOS RÔLES ET RESPONSABILITÉS

Des rôles clairs et opérationnels

VOTRE CHRONOGRAMME

Une séquence réaliste et structurée

UNE MÉTHODE RÉUTILISABLE

Des outils concrets pour vos prochains exercices

INCLUS

- Rencontre préparatoire individuelle
- 1 heure de coaching après la formation
- Accès au Club Crise & Résilience

FORMAT

- 4 demi-journées : 17, 19, 24 et 26 novembre 2026
- 8 h à 12 h (Québec) 14 h à 18 h (France)
- 100 % à distance
- Places limitées pour favoriser l'accompagnement individuel

Des compétences aujourd'hui pour une organisation plus résiliente demain.

1 397 $ CA + taxes

RÉSERVEZ VOTRE PLACE DÈS MAINTENANT

INFOS : info@crise-resilience.com

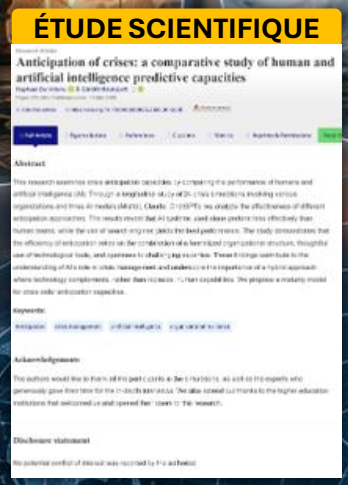
CRISE-RESILIENCE.COM

Anticiper les crises : Humains, IA… et Google

Face aux crises, l'IA seule ne suffit, et l'expertise humaine non plus.

Nos recherches sur 24 simulations montrent qu'une autre combinaison fait réellement la différence.

Découvrez pourquoi certaines cellules de crise voient plus loin que les autres, et comment vous pouvez renforcer dès maintenant votre capacité d'anticipation.



Raphaël de Vittoris

professeur de stratégie et de gestion de crise à Clermont School Of Business / fondateur de Antifragile.fr

Carole Bousquet

Professeure Associée / Management, RH & Conduite du Changement

Les organisations parlent beaucoup d'anticipation, mais la plupart découvrent encore les crises trop tard. En comparant cellules humaines, IA génératives et outils numériques classiques, nous avons identifié ce qui distingue les équipes qui anticipent vraiment des autres. Un enseignement clé :

la technologie n'est efficace que dans une structure pensée pour l'anticipation.

Anticiper une crise, ce n'est pas prédire l'avenir

Anticiper une crise ne consiste pas à deviner exactement ce qui va se passer, mais à repérer tôt les signaux révélateurs, imaginer plusieurs futurs plausibles et préparer des réponses crédibles. C'est une compétence organisationnelle autant que technique : elle dépend de vos routines, de vos rôles, de vos modes de décision, pas seulement de vos outils.

Dans nos travaux, nous avons étudié un scénario de crise psychosociale sensible : le suicide d'un collaborateur sur son lieu de travail. Ce type d'événement peut toucher n'importe quel secteur et déclenche une forte charge émotionnelle. Cette configuration permet de tester la capacité réelle d'une équipe à garder lucidité, à anticiper les effets en chaîne et à décider sous pression.

Sur la base des évènements de France Télécom notamment entre les années 2008 et 2009.

Quatre stratégies d'anticipation : où se situe votre organisation ?

La littérature et nos observations font ressortir quatre grandes stratégies d'anticipation, que l'on retrouve aussi dans les cellules de crise :

- *Stratégie réactive* : on ne consacre quasiment aucun temps à l'anticipation. On « improvise » le jour où la crise survient, en bricolant avec les ressources disponibles.
- *Stratégie désordonnée* : quelques signaux sont analysés « à la volée », sans cadre, sans plan formel, au gré des sensibilités des acteurs présents.
- *Stratégie régulière* : l'équipe s'appuie sur une expertise structurée, des scénarios connus, des plans de contingence élaborés collectivement.
- *Stratégie continue* : la cellule de crise surveille systématiquement les risques, met à jour ses scénarios, tient un registre formel des menaces et ruptures possibles.

Nos résultats sont clairs : plus la stratégie d'anticipation est formalisée (régulière ou continue), plus la qualité des décisions collectives dans la simulation est élevée. À l'inverse, les approches réactives et désordonnées amplifient l'incertitude, réduisent le nombre d'options pertinentes, et exposent l'organisation à des erreurs coûteuses.

Pour un manager, la question n'est donc pas « Avons-nous un plan de crise ? » mais « Notre cellule de crise dispose-t-elle d'un véritable processus d'anticipation, vivant, mis à jour, partagé ? ».

Le changement est radical, l'anticipation (qui n'est que trop rarement une activité à temps plein dans la cellule de crise) s'illustre comme LE facteur clef de succès du processus de décision de la cellule.

IA générative : un allié… mais pas le stratège

Nous avons testé trois grands modèles de langage en tant que « cellules de crise virtuelles ». Concrètement, l'IA recevait le même prompt que les équipes humaines, décrivant la situation de crise et les choix à faire. Son rôle : proposer des anticipations et décisions pour les minutes et heures à venir.

Résultat : les IA utilisées seules ont obtenu les plus faibles scores de pertinence des décisions, en dessous des équipes humaines, qu'elles soient novices ou expérimentées. Elles repèrent des tendances, proposent des actions génériques, mais peinent à saisir les enjeux politiques, culturels, émotionnels d'une crise réelle. Elles n'ont ni responsabilité, ni jugement moral, ni compréhension fine des dynamiques sociales internes. Autrement dit,

l'IA peut aider à traiter l'information, mais elle ne remplace pas une cellule de crise humaine, surtout dans les situations où la confiance, l'éthique et la crédibilité publique sont centrales.

Quand Google surperforme l'IA…

Un résultat inattendu est apparu dans nos simulations : les meilleures performances ne viennent ni des équipes « sans outils », ni des équipes appuyées sur l'IA générative, mais des cellules qui utilisent de façon structurée… un simple moteur de recherche.

Les équipes qui ont pris le temps de chercher des retours d'expérience, des cas similaires, des bonnes pratiques, ont produit plus de scénarios de rupture, anticipé davantage de conséquences et pris des décisions plus pertinentes. Ce sont souvent les membres les moins expérimentés qui ont spontanément utilisé le moteur de recherche pour enrichir la réflexion collective.

À l'inverse, les membres les plus expérimentés avaient tendance à s'appuyer principalement sur leur vécu, parfois au détriment de l'ouverture à des situations qu'ils n'avaient jamais rencontrées. Ce biais d'expertise joue aussi quand ils interrogent l'IA : leurs convictions orientent les questions… et donc les réponses.

La leçon à retenir pour les managers : un outil numérique performant n'a d'impact que s'il est intégré dans un dispositif d'anticipation collectif, ouvert, qui accepte de remettre en cause les certitudes, y compris celles des experts maison.

Vers une cellule de crise « mature »

À partir des 24 simulations, nous avons proposé un modèle de maturité des cellules de crise en matière d'anticipation. Les cellules les plus efficaces partagent trois caractéristiques :

Une structure formalisée : rôles clairs, processus d'anticipation documentés, rituels de mise à jour des scénarios.

Un usage réfléchi des outils : moteur de recherche pour élargir la vision, IA pour explorer des options, mais jamais en pilotage automatique.

Une culture de remise en question : les experts acceptent d'être challengés, les novices sont encouragés à contribuer, les signaux faibles sont pris au sérieux.

Pour un dirigeant, renforcer la capacité d'anticipation ne consiste donc pas à « acheter de l'IA », mais à construire une cellule qui sait combiner intelligemment compétences humaines, information disponible et outils numériques.

Inspiré de l'article scientifique : De Vittoris, R. & Bousquet C. (2026). Anticipation of crises: a comparative study of human and artificial intelligence predictive capacities, International Studies of Management & Organization, DOI: 10.1080/00208825.2026.2642235

CLERMONT SCHOOL OF BUSINESS

Raphaël de Vittoris

Raphaël De Vittoris est Docteur en sciences de gestion, il est aussi professeur associé et fondateur d'Antifragile.fr.

Auteur de plusieurs ouvrages, il explore la résilience et l'antifragilité des organisations. Il accompagne les entreprises dans la consolidation de leur pérennité. Son parcours mêle recherche, enseignement et action, au croisement du management, de la stratégie et de la gestion de crise.

https://antifragile.fr/

IDRAC BUSINESS SCHOOL DEVENEZ REMARQUABLE

Carole Bousquet

Associate Professor of Management & Human Resources at IDRAC Business School
Associate researcher, Magellan, Jean Moulin Lyon 3 University
Division Chair of Management Consulting Division – Academy of Management

4 clés pour doper l'anticipation de votre cellule de crise

Clarifiez la mission d'anticipation : Désignez explicitement un binôme ou un petit groupe chargé de surveiller les signaux faibles, d'actualiser les scénarios de rupture et de préparer des options avant que la crise n'éclate. Intégrez cette mission dans les fiches de rôle de la cellule de crise. Ce rôle doit devenir central et être porté par des profil à la fois créatifs et connaissant l'organisation et son environnement en profondeur.

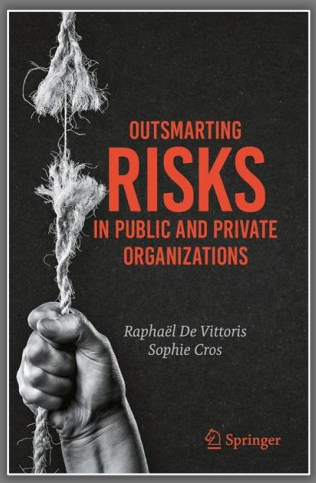
Formalisez vos scénarios de crise : Partir d'un scénario psychosocial (suicide, harcèlement, accident grave) et d'un scénario technologique (cyberattaque, panne majeure) suffit pour structurer vos premiers exercices. Documentez les décisions clés, les zones d'incertitude et les effets domino (incluant les moins plausibles), puis mettez à jour ces scénarios au moins une fois par an.

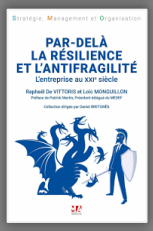
Organisez des simulations courtes mais régulières : Préférez des formats de trois heures, centrés sur quelques décisions critiques, plutôt que de grands exercices ponctuels. Après chaque simulation, faites un débrief axé sur les anticipations manquées, les biais d'expertise et l'usage des outils (moteurs de recherche, IA).

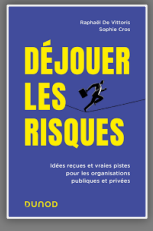
Institutionnalisez l'usage des outils numériques : Décidez quand et comment la cellule utilise moteurs de recherche et IA : recherche de cas similaires, veille réglementaire, brainstorming d'actions. Apprenez à écrire des prompts pertinents.

À LIRE

RAPHAËL DE VITTORIS…





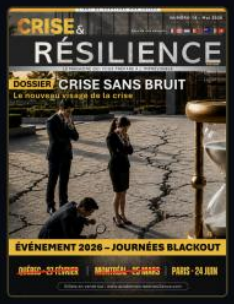


MAGAZINE CRISE ET RÉSILIENCE

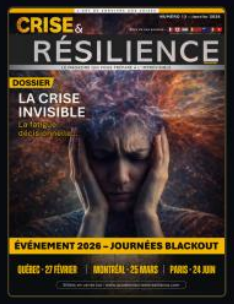
L'art de survivre aux crises

Quatorze numéros.
Un seul sujet : tenir le choc.

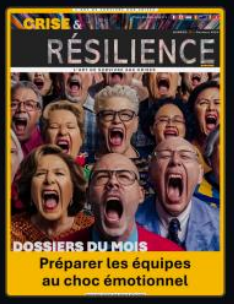
De janvier 2023 à mai 2026, **quatorze dossiers** sur la gestion de crise, la continuité d'activité, le cyber et le leadership. Pour les équipes qui préfèrent se préparer plutôt que subir.



N° 14 · Mai 2026
Crise sans bruit, le nouveau visage de la crise



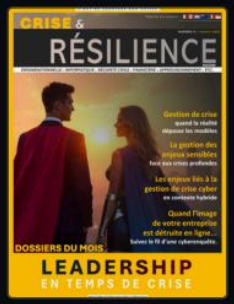
N° 13 · Janvier 2026
La fatigue décisionnelle, la crise invisible



N° 12 · Octobre 2025
Préparer les équipes au choc émotionnel

N° 11 · Juillet 2025
Cadre de gestion de crise, lutte contre le terrorisme

N° 10 · Avril 2025
I.A. et gestion de crise



N° 9 · Janvier 2025
Leadership en temps de crise

N° 8 · Octobre 2024
Black-out, une menace invisible mais bien réelle

N° 7 · Juillet 2024
Comment réaliser un exercice de crise

N° 6 · Avril 2024
Risques climatiques, une approche globale devenue vitale

N° 5 · Janvier 2024
Comment mettre en place un plan de gestion de crise

N° 4 · Octobre 2023
Comment mettre en place un plan de continuité d'activité

N° 3 · Juillet 2023
Gestion de la continuité des services dans les villes

N° 2 · Avril 2023
Fragilité des chaines d'approvisionnement

N° 1 · Janvier 2023
Blackout informatique

Tous les numéros, en ligne

Feuilletez les quatorze couvertures et lisez chaque dossier.

Recevez le prochain par l'infolettre.

magazine.crise-resilience.com

Magazine, radio, académie : un même regard sur la résilience

par Crise et Résilience
info@crise-resilience.com

Vous n’êtes pas la cible mais vous pouvez quand même être la victime.

Cocktail Molotov contre la maison du patron d’OpenAI, tirs contre un élu favorable aux data centers, pylônes sabotés en France, fibre incendiée : une frange de la contestation technologique est passée des discours aux actes.

Pour les entreprises, le risque est moins lointain qu’il n’y paraît : il n’est pas nécessaire d’être visé pour subir l’attaque.

Thomas Scorticati

Gestion de crise & PCA pour ETI | Exercices immersifs + plans opérationnels | ISO 22301 Lead Implementer, MBCI

Le 10 avril 2026, un homme de vingt ans lance un cocktail Molotov contre le domicile de Sam Altman, patron d'OpenAI.

Selon les autorités américaines, il avait traversé les États-Unis avec l'intention de s'en prendre au dirigeant et transportait des écrits présentant l'intelligence artificielle comme une menace pour l'humanité.

Quelques jours plus tôt, treize coups de feu avaient été tirés contre le domicile d'un élu d'Indianapolis ayant soutenu l'installation d'un data center.

L'histoire ne s'arrête pas aux États-Unis.

En juin, en Isère, deux pylônes électriques alimentant notamment STMicroelectronics et Soitec sont sabotés.

Quelques jours plus tard, une armoire de fibre optique située dans un bâtiment accueillant notamment Dassault Systèmes à Meylan, dans la région Auvergne-Rhône-Alpes, est incendiée. Les actions sont revendiquées dans des publications issues de la mouvance libertaire.

En août, la police écossaise demande même un renforcement des mesures de sécurité autour d'un futur data center dédié à l'IA, confronté à une forte opposition locale.

Cette contestation reste très majoritairement pacifique. Mais le symbole a changé :

le data center n'est plus seulement un bâtiment technique. Il devient la représentation physique de l'intelligence artificielle.

Quand l'IA devient une cible physique

C'est tout le paradoxe. L'intelligence artificielle semble immatérielle : quelques secondes sur un téléphone suffisent pour interroger un modèle situé on ne sait où.

Pourtant, derrière cette apparente abstraction se trouvent des serveurs, des fibres, des transformateurs, des systèmes de refroidissement et d'immenses bâtiments.

Le numérique a toujours un corps.
Et ce corps peut devenir une cible.

Mauro Lubrano, chercheur spécialiste de la violence politique, distingue deux tendances :

- Viser les personnalités qui incarnent la technologie, comme Sam Altman;
- Attaquer directement les infrastructures qui permettent à cette technologie de fonctionner.

Le phénomène reste fragmenté, sans mouvement organisé unique, mais les cibles commencent à se ressembler.

Les motivations varient :

- Crainte de l'automatisation du travail;
- Impact environnemental des data centers;
- Rejet du pouvoir des géants technologiques;
- Peur d'une IA devenue incontrôlable.

Pour une minorité, cette opposition quitte désormais le débat politique pour devenir violente.

Vous n'avez pas besoin d'être la cible

Pour une entreprise ordinaire, le sujet pourrait sembler assez exotique. Après tout, personne ne prévoit probablement d'incendier votre serveur comptable au nom de la lutte contre l'intelligence artificielle.

Le problème est ailleurs : nous partageons les mêmes infrastructures.

Un data center héberge des dizaines d'organisations. Une fibre dessert plusieurs bâtiments. Une alimentation électrique peut servir simultanément une PME, un laboratoire et un industriel stratégique. Votre fournisseur informatique dépend lui-même d'autres fournisseurs que vous ne connaissez parfois même pas.

Vous pouvez donc subir une attaque qui ne vous concernait absolument pas. C'est le risque par voisinage.

Votre entreprise n'est pas visée, mais elle partage une infrastructure avec quelqu'un qui l'est. Le risque de votre voisin devient alors le vôtre.

Et c'est là que le PCA devient utile

La continuité d'activité n'a pas besoin d'un nouveau scénario intitulé « extrémisme anti-tech ». Elle pose une question beaucoup plus simple : si une ressource indispensable disparaît, pouvons-nous continuer à fonctionner ?

Ces attaques invitent surtout à regarder derrière certaines phrases rassurantes : « nos données sont dans le cloud », « nous avons deux fournisseurs », « notre prestataire dispose d'un site de secours ».

Où se trouvent réellement ces infrastructures ? Partagent-elles le même bâtiment, la même alimentation ou le même réseau ? Et surtout, avec qui les partageons-nous ?

Deux solutions indépendantes sur un contrat peuvent finalement dépendre du même morceau de fibre dans le monde réel.

La prochaine crise pourrait ne rien avoir à voir avec vous

Il serait excessif d'annoncer une vague de terrorisme anti-IA. Les actions violentes restent rares et ne doivent évidemment pas être confondues avec l'opposition légitime aux technologies ou aux data centers.

Mais quelque chose a changé. Ces infrastructures concentrent désormais les débats sur l'emploi, l'environnement, l'énergie et le pouvoir des géants technologiques. Elles deviennent visibles, politiques et, pour certaines, des cibles.

Pour les entreprises, la bonne question n'est donc peut-être plus seulement, « Qui pourrait vouloir nous attaquer ? »

Mais aussi :

« Avec qui partageons-nous ce qui nous permet de fonctionner ? »

Thomas Scorticati

SCORT CONSEIL Site Web : https://www.scortconseil.com/

Thomas Scorticati est consultant indépendant avec dix ans d'expérience en continuité d'activité et gestion de crise. Certifié MBCI et ISO 22301 Lead implementer, il accompagne les organisations de tous secteurs, finance, industrie, santé ou encore administration publique. Il a également créé Y Crisis, une plateforme de simulation de crise immersive.

BESOIN DE FORMATION...

L'académie Crise et Résilience vous offre

Ces formations sont garanties « satisfait ou remboursé ». Oui... vous avez bien lu!

Visitez-nous...

www.academiecriseetresilience.com

LA RADIO CRISE ET RÉSILIENCE

En continu, tous les jours

EN DIRECT

22 émissions à l'antenne.
La crise, on en parle avant.

La radio de la gestion de crise, de la continuité des opérations et de la reprise informatique.
Plus de 15 heures d'émissions, une grille recomposée chaque jour.

La reprise informatique dans le cloud AWS
89 min

Moderniser la gestion des risques
81 min

Le cloud et la continuité d'activité
59 min

L'effet domino iranien : vos plans tiennent-ils ?
55 min

Survivre à un blackout informatique
51 min

Cyberrésilience contre cybersécurité
51 min

Blackout total : et si c'était demain ?
50 min

Le lancement de l'Académie
49 min

Crue centennale à Paris : le scénario du siècle
47 min

Négocier une rançon avec des pirates
46 min

L'antifragilité : faire de la menace une force
44 min

Le métier de responsable de continuité
42 min

Communiquer quand la crise est là
41 min

Le survivalisme appliqué à l'entreprise
34 min

Récupérer ses données après l'attaque
30 min

Piéger un service RH par la psychologie
28 min

Tester son plan avant que ça arrive
27 min

Anticiper les crises
26 min

Le plan de pandémie en entreprise
20 min

Les biais cognitifs en pleine crise
19 min

Dans les coulisses d'un exercice cyber
17 min

Pourquoi la reprise passe par le cloud
17 min

Écoutez en direct

Tout le monde entend la même chose, au même moment.

Aussi en balado

YouTube · Spotify
Deezer · Apple

Et 27 capsules

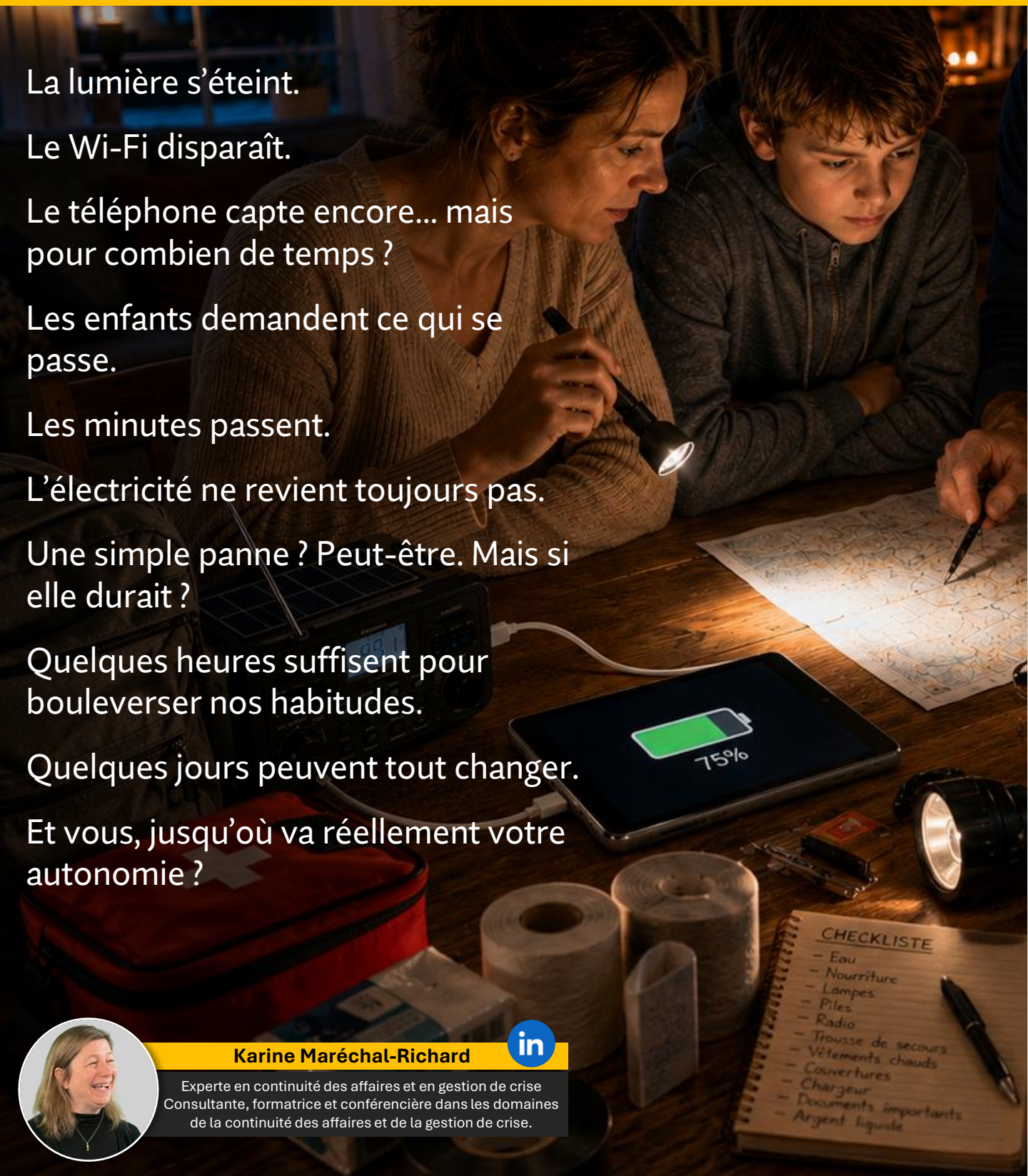
De courtes pastilles entre deux émissions.

radio.crise-resilience.com

On écoute, on lit, puis on s'entraîne : radio, magazine, académie

par Crise et Résilience
info@crise-resilience.com

Blackout familial : comment protéger sa famille lorsque tout s'arrête ?



La lumière s'éteint.

Le Wi-Fi disparaît.

Le téléphone capte encore… mais pour combien de temps ?

Les enfants demandent ce qui se passe.

Les minutes passent.

L'électricité ne revient toujours pas.

Une simple panne ? Peut-être. Mais si elle durait ?

Quelques heures suffisent pour bouleverser nos habitudes.

Quelques jours peuvent tout changer.

Et vous, jusqu'où va réellement votre autonomie ?

Karine Maréchal-Richard

Experte en continuité des affaires et en gestion de crise
Consultante, formatrice et conférencière dans les domaines de la continuité des affaires et de la gestion de crise.

Un blackout n'est pas une simple panne de courant. Contrairement à une panne classique, qui se règle généralement en quelques minutes ou quelques heures,

un blackout touche un vaste territoire, perturbe plusieurs services essentiels à la fois, et ses conséquences peuvent s'étendre progressivement sur plusieurs jours.

Les communications deviennent incertaines, les paiements électroniques cessent de fonctionner, l'accès à certains services se complique et les habitudes du quotidien sont bouleversées. En quelques heures, une famille peut devoir prendre des décisions auxquelles elle n'avait jamais pensé.

Les événements des dernières années nous rappellent qu'aucune société n'est à l'abri d'une interruption majeure de l'alimentation électrique. Plus nos modes de vie dépendent de l'électricité, plus ses conséquences deviennent importantes lorsqu'elle disparaît.

C'est pourquoi plusieurs pays, dont le Canada, la France et les pays de l'Union européenne,

recommandent aujourd'hui aux citoyens de pouvoir être autonomes pendant 72 heures en cas de crise majeure.

Ce dossier a été conçu pour vous accompagner durant ces premières heures, et les jours qui peuvent suivre. Tout au long de ce parcours, vous suivrez David, Éva et leurs enfants Lucas et Emma, une famille comme tant d'autres, confrontée à un blackout qui s'installe plus longtemps que prévu.

À travers leur histoire, vous découvrirez comment s'organiser en famille comme une véritable cellule de crise, préserver les ressources essentielles au fil des jours et protéger les personnes les plus vulnérables du foyer, même celles dont les besoins restent parfois invisibles au quotidien.

Ce dossier n'a pas pour objectif de faire de vous un spécialiste de la survie. Il vise à vous aider à prendre des décisions simples, concrètes et adaptées à la réalité d'une famille. Car, face à un blackout, la meilleure préparation ne repose pas uniquement sur le matériel que l'on possède. Elle repose avant tout sur la capacité à s'organiser, à rester calme et à agir ensemble.

QUAND TOUT S'ÉTEINT

Le choc des premières minutes

La lumière s'éteint d'un coup. Le bruit du réfrigérateur disparaît. Le téléviseur devient noir. Le Wi-Fi cesse de fonctionner.

Pendant quelques secondes, personne ne bouge!

Puis Emma demande depuis le salon : « Que se passe-t-il ? » Lucas lève les yeux de son téléphone : l'écran est toujours allumé, mais son fil d'actualité reste bloqué, incapable de le rafraîchir.

« Est-ce que c'est seulement chez nous ? » « Est-ce que ça va revenir ? »

Dehors, tout le quartier est lui aussi plongé dans l'obscurité. Dans la rue, quelques fenêtres s'illuminent à la lueur des téléphones.

David vérifie son téléphone. Le réseau fonctionne encore, mais les messages mettent du temps à partir. À la radio, un animateur évoque une panne importante, sans pouvoir en préciser l'origine, l'étendue ni la durée.

Sur le trottoir, les voisins commencent déjà à échanger leurs hypothèses. Une simple panne ? Peut-être. Mais les minutes passent et l'électricité ne revient pas. À cet instant, personne ne sait encore ce qui est réellement en train de se passer.

Le cerveau sous pression : chacun réagit à sa manière

Face à l'inconnu, nous cherchons naturellement à comprendre ce qui se passe et à retrouver des repères. Or, lors d'un blackout, les questions arrivent souvent plus vite que les réponses.

Combien de temps la panne va-t-elle durer ? Jusqu'où s'étend-elle ? Le téléphone va-t-il continuer à fonctionner ? Nos proches sont-ils en sécurité ? Pourrons-nous encore nous déplacer ou obtenir de l'information ?

Lorsque les réponses manquent, notre esprit cherche à combler les vides, parfois en imaginant des scénarios plus inquiétants que la réalité.

L'incertitude augmente alors le stress et peut influencer notre manière de réfléchir, de décider et d'agir.

Certains passent immédiatement à l'action, parfois en voulant tout faire en même temps. D'autres hésitent, attendent ou restent momentanément figés.

Sous pression, il peut également devenir plus difficile de prendre du recul, de hiérarchiser les priorités et de distinguer ce qui est urgent de ce qui peut attendre.

L’objectif n’est donc pas de tout comprendre ni de tout résoudre immédiatement, mais de retrouver suffisamment de calme et de repères pour savoir quoi faire en premier.

C’est là que la préparation prend tout son sens ***: elle ne supprime pas l’incertitude, mais elle évite d’avoir à tout improviser lorsque la pression monte.***

Les premiers réflexes

Dans les premières minutes, inutile de chercher à tout résoudre. La priorité est de sécuriser, vérifier et commencer à s’organiser. Quelques gestes simples permettent déjà de reprendre la main :

> **Rester calme :** prenez quelques instants pour observer la situation avant d’agir. Votre attitude influence celle de toute la famille, particulièrement celle des enfants.
>
> **Vérifier avant d’imaginer le pire :** contrôlez le disjoncteur, regardez si le voisinage est également touché et recherchez une information officielle si elle est disponible.
>
> **Préserver les ressources :** évitez d’ouvrir inutilement le réfrigérateur ou le congélateur, de multiplier les appels ou d’utiliser toutes vos sources d’éclairage dès les premières minutes.
>
> **Rassembler la famille :** assurez-vous que chacun est en sécurité et que tout le monde sait ce qui se passe. L’organisation viendra ensuite

💡 **L'œil de l'expert**

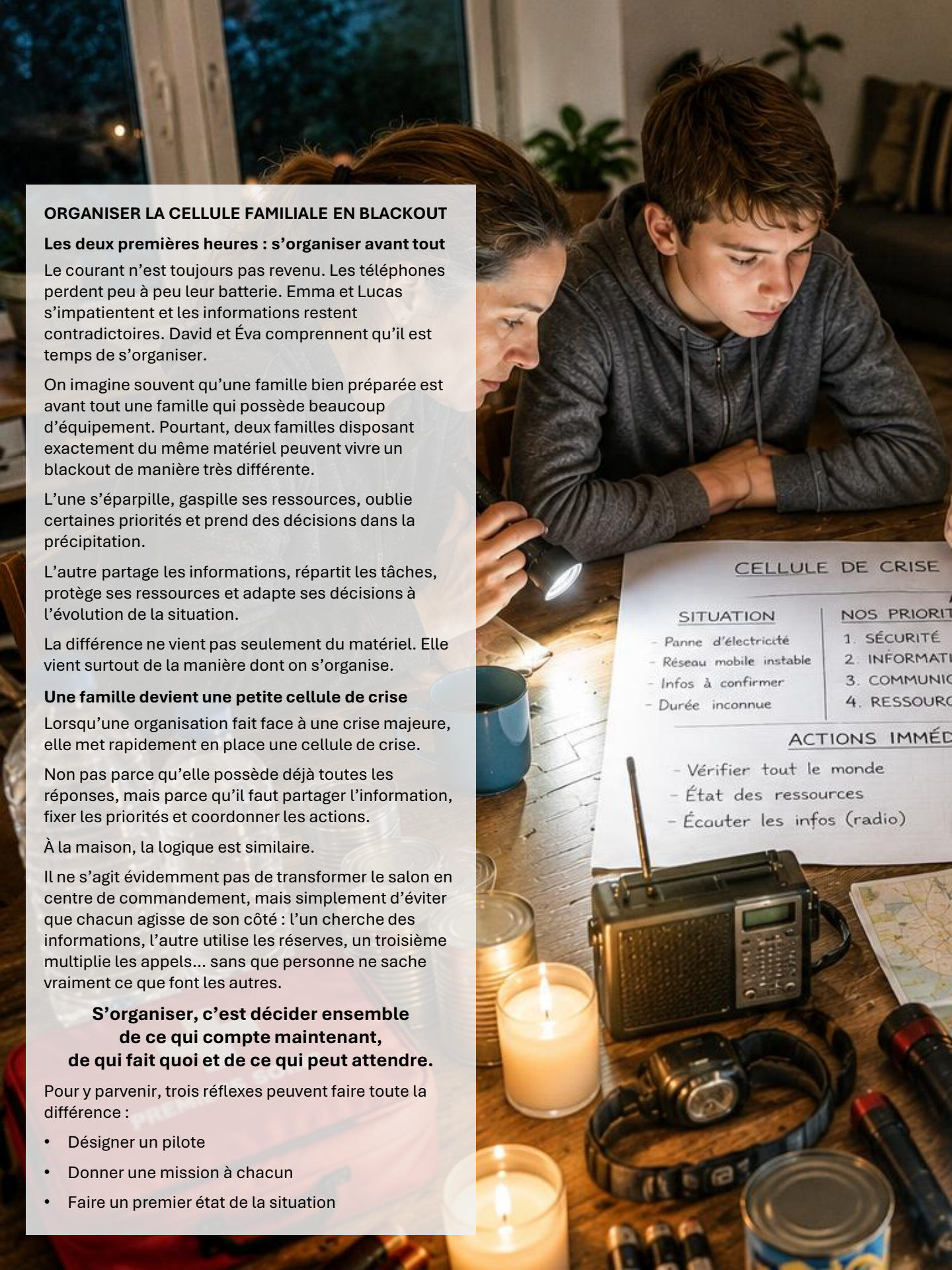
Dans les organisations confrontées à des crises majeures, nous observons toujours le même phénomène : les équipes qui traversent le mieux les premières heures ne sont pas celles qui disposent immédiatement de toutes les réponses.

Ce sont celles qui acceptent de décider avec les informations disponibles, d'ajuster leurs choix au fur et à mesure et de conserver une organisation claire.

Une famille fonctionne exactement de la même manière.

Face à un blackout, attendre de tout savoir avant d’agir n’est pas réaliste. Il faut accepter une part d’incertitude, commencer par l’essentiel et s’adapter ensuite.

La résilience ne consiste pas à tout prévoir ni à tout contrôler. Elle consiste à être suffisamment préparé pour savoir par où commencer.



ORGANISER LA CELLULE FAMILIALE EN BLACKOUT

Les deux premières heures : s'organiser avant tout

Le courant n'est toujours pas revenu. Les téléphones perdent peu à peu leur batterie. Emma et Lucas s'impatientent et les informations restent contradictoires. David et Éva comprennent qu'il est temps de s'organiser.

On imagine souvent qu'une famille bien préparée est avant tout une famille qui possède beaucoup d'équipement. Pourtant, deux familles disposant exactement du même matériel peuvent vivre un blackout de manière très différente.

L'une s'éparpille, gaspille ses ressources, oublie certaines priorités et prend des décisions dans la précipitation.

L'autre partage les informations, répartit les tâches, protège ses ressources et adapte ses décisions à l'évolution de la situation.

La différence ne vient pas seulement du matériel. Elle vient surtout de la manière dont on s'organise.

Une famille devient une petite cellule de crise

Lorsqu'une organisation fait face à une crise majeure, elle met rapidement en place une cellule de crise.

Non pas parce qu'elle possède déjà toutes les réponses, mais parce qu'il faut partager l'information, fixer les priorités et coordonner les actions.

À la maison, la logique est similaire.

Il ne s'agit évidemment pas de transformer le salon en centre de commandement, mais simplement d'éviter que chacun agisse de son côté : l'un cherche des informations, l'autre utilise les réserves, un troisième multiplie les appels… sans que personne ne sache vraiment ce que font les autres.

S'organiser, c'est décider ensemble de ce qui compte maintenant, de qui fait quoi et de ce qui peut attendre.

Pour y parvenir, trois réflexes peuvent faire toute la différence :

- Désigner un pilote
- Donner une mission à chacun
- Faire un premier état de la situation

1- Désigner un pilote : Dans une crise, quelqu'un doit garder une vision d'ensemble. Nous l'appellerons le pilote. Il n'est pas là pour tout décider ni pour commander les autres.

Son rôle est de maintenir le cap : ***écouter, aider à fixer les priorités, coordonner les actions et s'assurer que chacun sait ce qu'il doit faire.*** Le pilote peut changer au cours du blackout selon la situation, la fatigue ou les compétences de chacun. L'essentiel n'est pas de savoir qui commande, mais de savoir qui coordonne.

2- Donner une mission à chacun : David comprend rapidement qu'il ne peut pas tout faire seul. Pendant qu'il écoute les informations à la radio, Éva vérifie les réserves d'eau. Lucas prépare les lampes de poche et Emma rassemble les jeux de société. En quelques minutes, chacun connaît son rôle.

Ce simple partage des tâches change l'ambiance dans la maison. Les enfants cessent de poser les mêmes questions. Les adultes retrouvent progressivement un sentiment de contrôle.

En gestion de crise, on ne se contente pas de répartir les tâches : on désigne aussi un responsable pour chacune d'elles. Cela évite le classique :

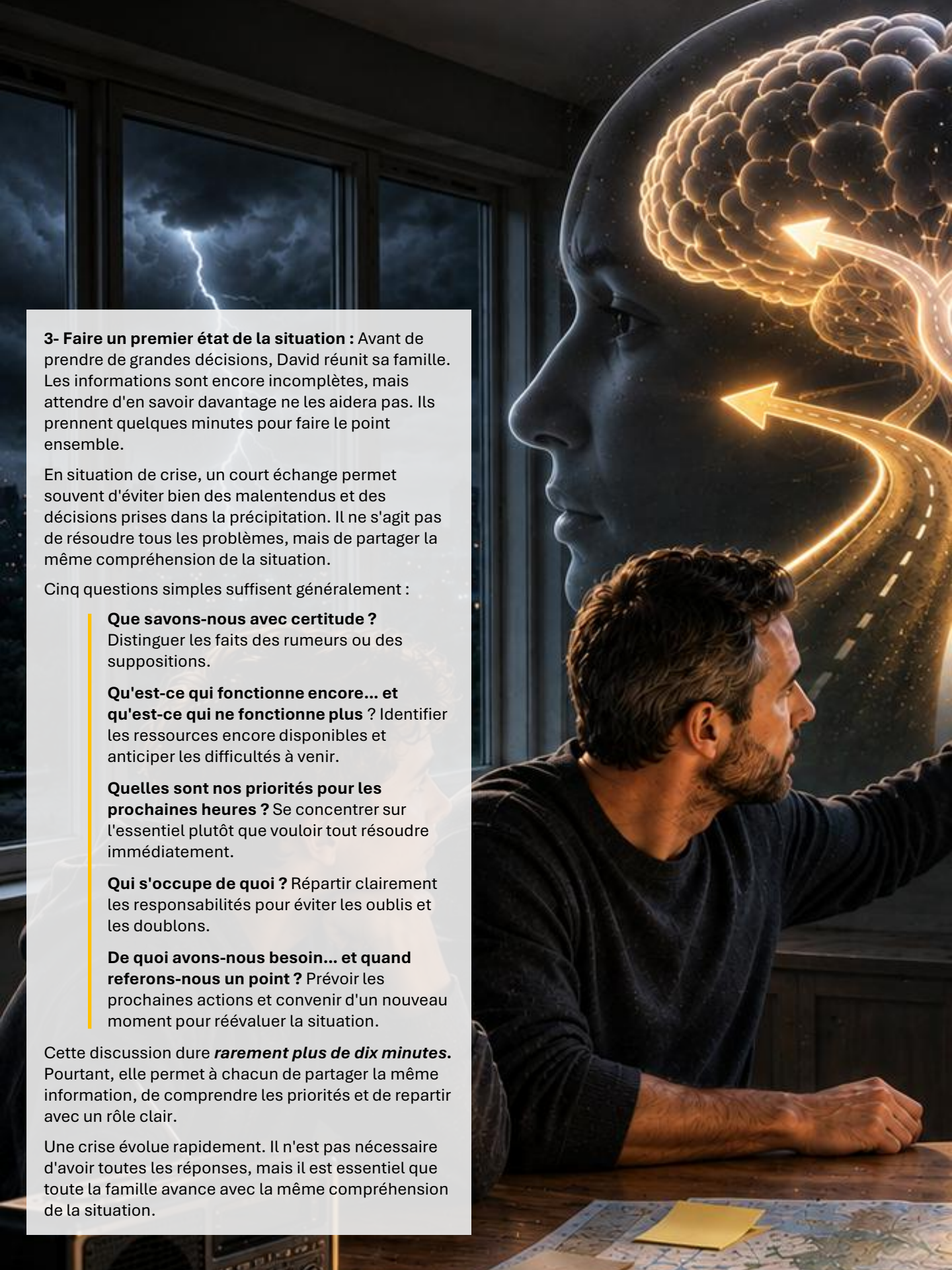
« Je pensais que quelqu'un d'autre s'en occupait. »

Six grands rôles peuvent structurer l'organisation familiale. Qui s'occupe de :

> **L'information et les communications :** Écouter les informations officielles, envoyer les messages importants, noter les nouvelles.
>
> **L'eau et l'alimentation :** Vérifier les réserves d'eau, planifier les repas, gérer les aliments et limiter le gaspillage.
>
> **L'énergie et l'éclairage :** Surveiller les batteries, préparer les lampes, gérer les recharges et économiser l'énergie.
>
> **La sécurité de la maison :** Vérifier les portes et les fenêtres, surveiller les sources de chaleur, prévenir les risques d'accident.
>
> **Les enfants et les personnes vulnérables :** Maintenir une routine, rassurer, proposer des activités et veiller aux besoins particuliers.
>
> **Les animaux (si nécessaire) :** Vérifier leur eau, leur nourriture et leur sécurité.

Ces rôles n'ont pas besoin d'être figés.

Ils peuvent évoluer au fil de la crise selon les compétences de chacun, l'âge des enfants ou les besoins du moment.



3- Faire un premier état de la situation : Avant de prendre de grandes décisions, David réunit sa famille. Les informations sont encore incomplètes, mais attendre d'en savoir davantage ne les aidera pas. Ils prennent quelques minutes pour faire le point ensemble.

En situation de crise, un court échange permet souvent d'éviter bien des malentendus et des décisions prises dans la précipitation. Il ne s'agit pas de résoudre tous les problèmes, mais de partager la même compréhension de la situation.

Cinq questions simples suffisent généralement :

> **Que savons-nous avec certitude ?** Distinguer les faits des rumeurs ou des suppositions.
>
> **Qu'est-ce qui fonctionne encore… et qu'est-ce qui ne fonctionne plus** ? Identifier les ressources encore disponibles et anticiper les difficultés à venir.
>
> **Quelles sont nos priorités pour les prochaines heures ?** Se concentrer sur l'essentiel plutôt que vouloir tout résoudre immédiatement.
>
> **Qui s'occupe de quoi ?** Répartir clairement les responsabilités pour éviter les oublis et les doublons.
>
> **De quoi avons-nous besoin… et quand referons-nous un point ?** Prévoir les prochaines actions et convenir d'un nouveau moment pour réévaluer la situation.

Cette discussion dure ***rarement plus de dix minutes.*** Pourtant, elle permet à chacun de partager la même information, de comprendre les priorités et de repartir avec un rôle clair.

Une crise évolue rapidement. Il n'est pas nécessaire d'avoir toutes les réponses, mais il est essentiel que toute la famille avance avec la même compréhension de la situation.

Décider malgré l’incertitude

David regarde une nouvelle fois son téléphone. Toujours aucune information précise. Le courant reviendra-t-il dans une heure ? Demain ? Dans trois jours ? Impossible de le savoir.

Pourtant, certaines décisions ne peuvent pas attendre: faut-il économiser davantage les batteries ? Préparer un repas maintenant ? Remplir des contenants d’eau ? Contacter certains proches ?

En situation de crise, une décision est rarement parfaite. Elle est prise avec les informations disponibles à un moment donné, puis ajustée lorsque la situation évolue.

L’important est donc moins de chercher la décision parfaite que de prendre une décision adaptée au moment présent et réversible lorsque c’est possible.

Penser par étapes

Une erreur fréquente consiste à vouloir résoudre toute la crise immédiatement. Les questions s’accumulent, les scénarios se multiplient et, avec eux, la charge mentale augmente.

Pour éviter de s’éparpiller, mieux vaut se concentrer sur un horizon plus court : Que devons-nous réussir pendant les deux prochaines heures ? Puis, une fois cette étape franchie : Que devons-nous faire ensuite ?

Cette approche permet de réduire la charge mentale, de rester concentré sur les priorités immédiates et de s’adapter progressivement à l’évolution de la situation.

Il ne s’agit pas d’ignorer ce qui pourrait arriver demain, mais de ne pas chercher à tout résoudre aujourd’hui.

En situation de crise, penser par étapes permet de garder son énergie et son attention pour ce qui compte maintenant.

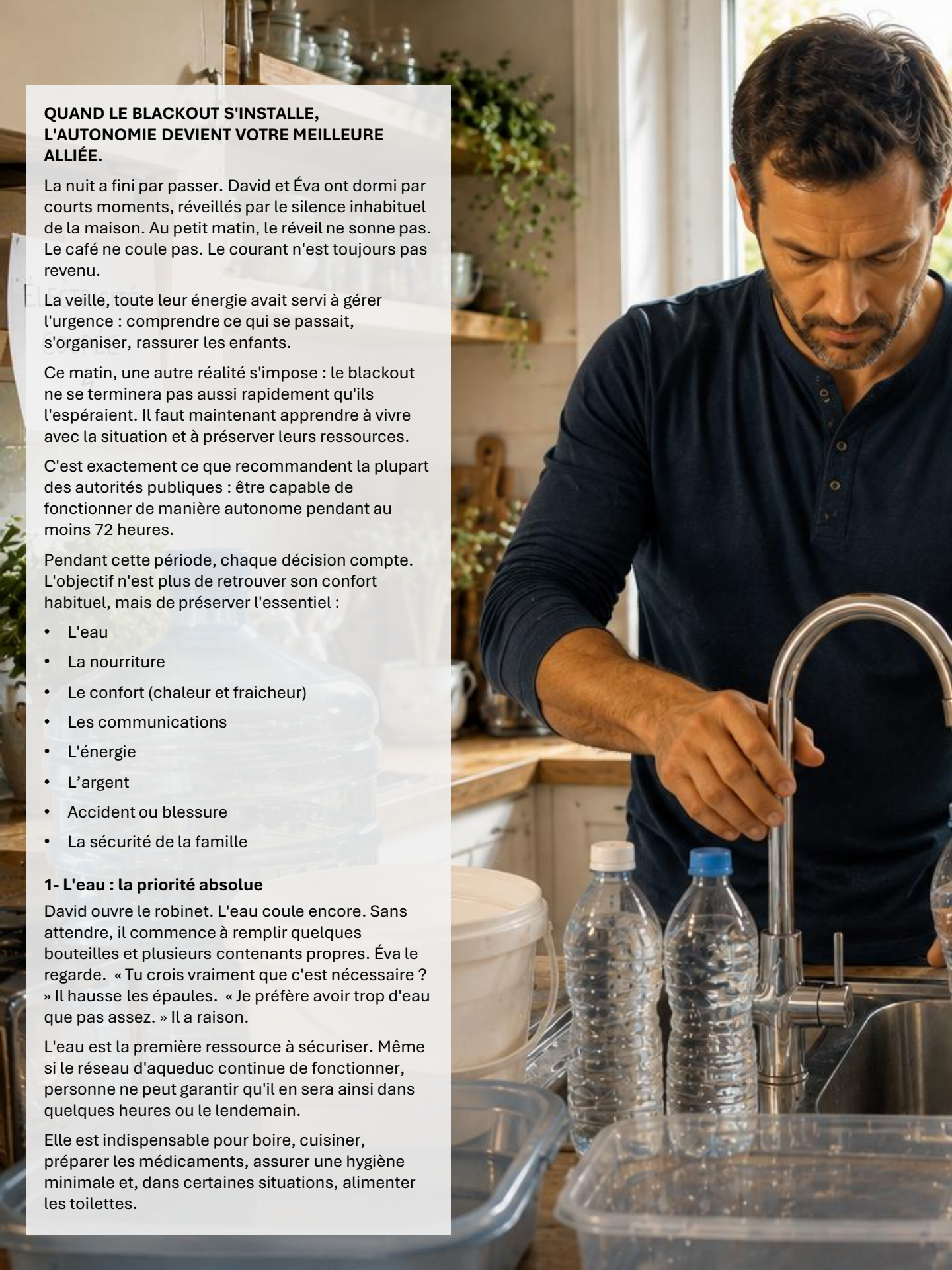
💡 L'œil de l'expert

Dans les exercices de gestion de crise, nous rappelons souvent qu'une décision imparfaite prise au bon moment vaut généralement mieux qu'une décision parfaite prise trop tard.

Une famille ne dispose jamais de toutes les informations lorsqu'un blackout débute.

En revanche, elle peut décider de protéger ses ressources, de s'organiser et de réévaluer régulièrement la situation.

La résilience ne consiste pas à tout prévoir. Elle consiste à savoir s'adapter.



QUAND LE BLACKOUT S'INSTALLE, L'AUTONOMIE DEVIENT VOTRE MEILLEURE ALLIÉE.

La nuit a fini par passer. David et Éva ont dormi par courts moments, réveillés par le silence inhabituel de la maison. Au petit matin, le réveil ne sonne pas. Le café ne coule pas. Le courant n'est toujours pas revenu.

La veille, toute leur énergie avait servi à gérer l'urgence : comprendre ce qui se passait, s'organiser, rassurer les enfants.

Ce matin, une autre réalité s'impose : le blackout ne se terminera pas aussi rapidement qu'ils l'espéraient. Il faut maintenant apprendre à vivre avec la situation et à préserver leurs ressources.

C'est exactement ce que recommandent la plupart des autorités publiques : être capable de fonctionner de manière autonome pendant au moins 72 heures.

Pendant cette période, chaque décision compte. L'objectif n'est plus de retrouver son confort habituel, mais de préserver l'essentiel :

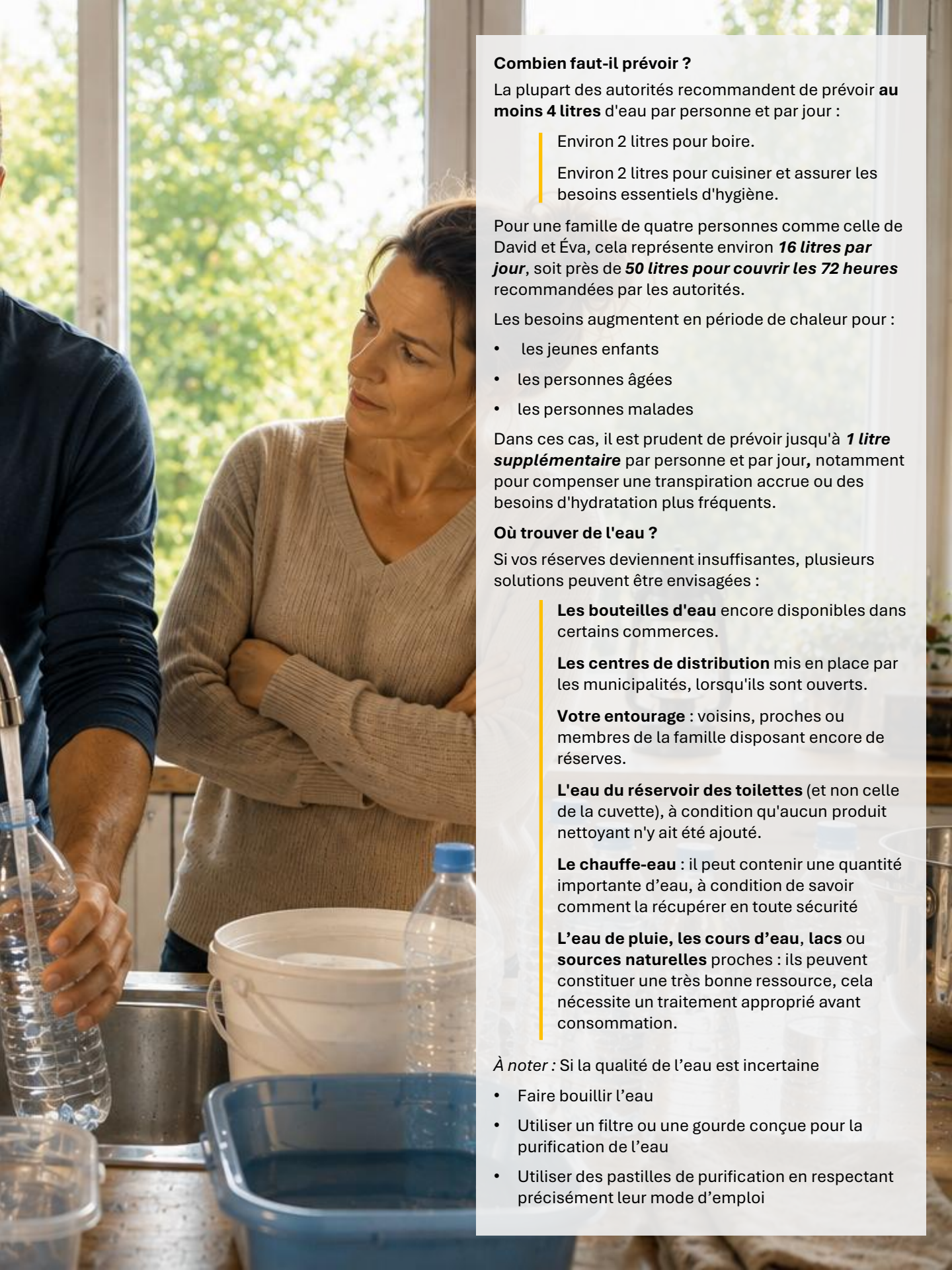
- L'eau
- La nourriture
- Le confort (chaleur et fraicheur)
- Les communications
- L'énergie
- L’argent
- Accident ou blessure
- La sécurité de la famille

1- L'eau : la priorité absolue

David ouvre le robinet. L'eau coule encore. Sans attendre, il commence à remplir quelques bouteilles et plusieurs contenants propres. Éva le regarde. « Tu crois vraiment que c'est nécessaire ? » Il hausse les épaules. « Je préfère avoir trop d'eau que pas assez. » Il a raison.

L'eau est la première ressource à sécuriser. Même si le réseau d'aqueduc continue de fonctionner, personne ne peut garantir qu'il en sera ainsi dans quelques heures ou le lendemain.

Elle est indispensable pour boire, cuisiner, préparer les médicaments, assurer une hygiène minimale et, dans certaines situations, alimenter les toilettes.



Combien faut-il prévoir ?

La plupart des autorités recommandent de prévoir **au moins 4 litres** d'eau par personne et par jour :

> Environ 2 litres pour boire.
>
> Environ 2 litres pour cuisiner et assurer les besoins essentiels d'hygiène.

Pour une famille de quatre personnes comme celle de David et Éva, cela représente environ ***16 litres par jour***, soit près de ***50 litres pour couvrir les 72 heures*** recommandées par les autorités.

Les besoins augmentent en période de chaleur pour :

- les jeunes enfants
- les personnes âgées
- les personnes malades

Dans ces cas, il est prudent de prévoir jusqu'à ***1 litre supplémentaire*** par personne et par jour**,** notamment pour compenser une transpiration accrue ou des besoins d'hydratation plus fréquents.

Où trouver de l'eau ?

Si vos réserves deviennent insuffisantes, plusieurs solutions peuvent être envisagées :

> **Les bouteilles d'eau** encore disponibles dans certains commerces.
>
> **Les centres de distribution** mis en place par les municipalités, lorsqu'ils sont ouverts.
>
> **Votre entourage** : voisins, proches ou membres de la famille disposant encore de réserves.
>
> **L'eau du réservoir des toilettes** (et non celle de la cuvette), à condition qu'aucun produit nettoyant n'y ait été ajouté.
>
> **Le chauffe-eau** : il peut contenir une quantité importante d'eau, à condition de savoir comment la récupérer en toute sécurité
>
> **L'eau de pluie, les cours d'eau**, **lacs** ou **sources naturelles** proches : ils peuvent constituer une très bonne ressource, cela nécessite un traitement approprié avant consommation.

À noter : Si la qualité de l'eau est incertaine

- Faire bouillir l'eau
- Utiliser un filtre ou une gourde conçue pour la purification de l'eau
- Utiliser des pastilles de purification en respectant précisément leur mode d'emploi

2- Nourrir la famille sans gaspiller

Vers midi, Emma demande ce qu'il y aura pour manger. David ouvre le réfrigérateur quelques secondes, puis le referme aussitôt. Chaque ouverture laisse s'échapper le froid et réduit le temps de conservation des aliments.

Pendant un blackout, l'objectif n'est plus de cuisiner comme d'habitude. Il est d'abord de préserver les aliments et d'utiliser intelligemment les réserves disponibles. Commencez par consommer les produits les plus périssables, puis privilégiez progressivement les aliments qui peuvent être conservés à température ambiante.

En situation de crise, les habitudes alimentaires évoluent rapidement. Sans réfrigération ni moyen de cuisson habituel, certains aliments deviennent impropres à la consommation en quelques heures. Le stress peut également modifier l'appétit : certaines personnes mangent moins, tandis que d'autres ressentent un besoin accru d'énergie.

L'objectif n'est pas de préparer des repas élaborés, mais de fournir à chacun l'énergie nécessaire tout en limitant le gaspillage.

À privilégier

> Des aliments non périssables, comme le riz, les pâtes, les lentilles, les haricots secs, les flocons d'avoine, les céréales, les craquelins ou les biscuits secs.
>
> Des conserves, telles que des légumes, fruits, compotes, des légumineuses, du thon, du saumon, du poulet, des soupes ou des plats préparés (n'oubliez pas un ouvre-boîte manuel).
>
> Des repas prêts à manger, qui ne nécessitent ni réfrigération ni cuisson.
>
> Des collations énergétiques, comme les noix, les amandes, les arachides, les fruits séchés, les barres tendres ou les barres protéinées.
>
> Du lait UHT ou du lait en poudre, ainsi que des boissons de longue conservation.
>
> Des aliments adaptés aux besoins particuliers, notamment pour les bébés, les personnes ayant des allergies ou suivant un régime médical spécifique.
>
> Un moyen de cuisson d'appoint, comme un réchaud de camping utilisé à l'extérieur ou dans un endroit bien ventilé, pour préparer des aliments simples, comme des pâtes, du riz ou des soupes.

3- Le confort : garder la chaleur… ou la fraîcheur

Au Québec, la température peut rapidement devenir un enjeu de sécurité lors d'un blackout.

En hiver, l'absence de chauffage entraîne une baisse progressive de la température intérieure.

En été, une canicule combinée à une panne d'électricité peut transformer une habitation en véritable fournaise.

Dans les deux cas, l'objectif n'est pas de maintenir toute la maison à une température confortable. L'objectif est avant tout de protéger les occupants les plus vulnérables.

En hiver : conserver la chaleur

Une maison met plusieurs heures avant de se refroidir complètement, mais plus la panne se prolonge, plus les risques augmentent.

Les enfants, les personnes âgées et les personnes malades perdent leur chaleur corporelle plus rapidement.

Les bons réflexes

> Regrouper la famille dans une même pièce.
>
> Fermer les pièces inutilisées.
>
> Limiter les ouvertures vers l'extérieur.
>
> Porter plusieurs couches de vêtements plutôt qu'un seul vêtement épais.
>
> Utiliser des couvertures supplémentaires, des couvertures de survie ou des sacs de couchage si nécessaire.
>
> Surveiller les signes d'hypothermie chez les personnes les plus vulnérables.

En été : limiter les effets de la chaleur

En plein été, et particulièrement lors d’une canicule, la température à l’intérieur d’un logement peut rapidement devenir difficile à supporter, surtout lorsqu’il est fortement exposé au soleil.

Lorsque la chaleur persiste plusieurs jours, le logement accumule la chaleur et les nuits ne suffisent parfois plus à le rafraîchir.

Sans climatisation ni ventilation électrique, l’inconfort peut alors s’accentuer, tout comme les risques de déshydratation et de coup de chaleur. Pendant un blackout, l’enjeu est donc double : empêcher autant que possible la chaleur d’entrer le jour et profiter des périodes plus fraîches pour rafraîchir le logement.

Les bons réflexes

> Fermer les rideaux et les stores pendant les heures les plus chaudes.
>
> Ouvrir les fenêtres uniquement lorsque l'air extérieur devient plus frais (le soir ou la nuit).
>
> Limiter les efforts physiques.
>
> Boire régulièrement, même sans sensation de soif.
>
> Porter des vêtements légers et de couleur claire.
>
> Rafraîchir régulièrement le corps avec un linge humide.
>
> Surveiller attentivement les jeunes enfants, les personnes âgées et les personnes souffrant de problèmes de santé.

Les erreurs fréquentes pour préserver son confort

> Utiliser un barbecue, un réchaud au propane ou un appareil de combustion à l'intérieur pour cuisiner ou se réchauffer.
>
> Faire fonctionner une génératrice dans la maison, le garage ou trop près des ouvertures, avec un risque d'intoxication au monoxyde de carbone.
>
> Chercher à chauffer ou à refroidir toutes les pièces de la maison.
>
> Sous-estimer les effets du froid ou de la chaleur sur les personnes vulnérables.
>
> Attendre l'apparition des premiers malaises avant de réagir.

4- Communication : l'information devient une ressource

Lors d'un blackout majeur, les réseaux deviennent rapidement saturés. Les téléphones cellulaires continuent parfois de fonctionner quelques heures, mais :

- Les batteries diminuent rapidement
- Les antennes peuvent être touchées
- Et les réseaux deviennent instables

Dans plusieurs crises, l'information contradictoire devient alors une source importante de stress. Le risque, passé des heures à chercher des nouvelles fiables.

Les bons réflexes

> Disposer d'une radio à piles ou à manivelle pour recevoir les informations officielles.
>
> Vérifier les informations à intervalles réguliers plutôt qu'en continu afin d'économiser les batteries.
>
> Privilégier les messages texte (SMS), qui nécessitent généralement moins de ressources réseau que les appels téléphoniques.
>
> Limiter les appels aux communications réellement importantes afin d'éviter la saturation des réseaux.
>
> Si vous en disposez, utiliser des talkies-walkies pour communiquer entre membres de la famille ou avec les voisins à proximité.
>
> Déterminer à l'avance un point de rassemblement et une personne-ressource à contacter si les membres de la famille sont séparés.
>
> Se fier aux informations diffusées par les autorités.

5- L'énergie : gérer chaque source disponible

Lors d'un blackout, l'électricité devient rapidement une ressource précieuse. Les appareils que nous utilisons quotidiennement : téléphone, radio, lampe de poche, ou ordinateur, dépendent tous d'une réserve d'énergie limitée.

Plus le blackout se prolonge, plus chaque watt compte. Heureusement, plusieurs familles disposent aujourd'hui de solutions leur permettant de prolonger leur autonomie.

Selon votre niveau de préparation, vous pourriez avoir accès à différentes sources d'énergie :

- Les batteries externes (power banks) pour recharger les téléphones, tablettes ou petits appareils électroniques.
- Les panneaux solaires portatifs, qui permettent de recharger progressivement certains appareils lorsque les conditions d'ensoleillement le permettent.
- Les génératrices, qui offrent une autonomie importante, mais nécessitent du carburant et doivent être utilisées de façon sécuritaire.

- Les systèmes solaires résidentiels avec batteries, lorsqu'ils sont conçus pour fonctionner en mode autonome.
- Les petites éoliennes domestiques, plus rares, mais qui peuvent compléter l'alimentation électrique dans certaines propriétés.

Chaque solution présente des avantages, mais aussi des limites.

Aucune ne fournit une énergie illimitée. Plus que la quantité d'énergie disponible, c'est souvent la manière dont elle est utilisée qui fait la différence.

Les bons réflexes :

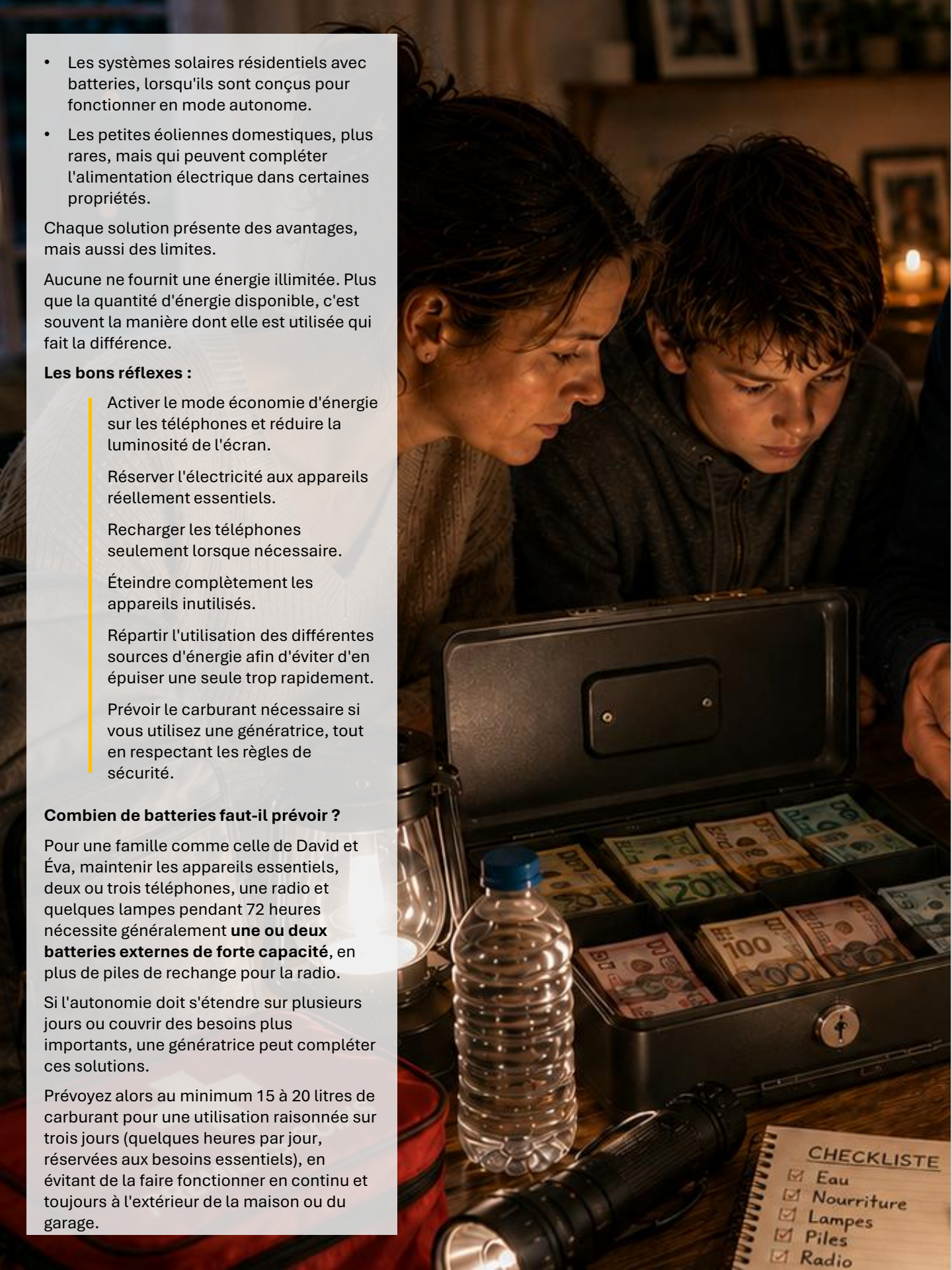
> Activer le mode économie d'énergie sur les téléphones et réduire la luminosité de l'écran.
>
> Réserver l'électricité aux appareils réellement essentiels.
>
> Recharger les téléphones seulement lorsque nécessaire.
>
> Éteindre complètement les appareils inutilisés.
>
> Répartir l'utilisation des différentes sources d'énergie afin d'éviter d'en épuiser une seule trop rapidement.
>
> Prévoir le carburant nécessaire si vous utilisez une génératrice, tout en respectant les règles de sécurité.

Combien de batteries faut-il prévoir ?

Pour une famille comme celle de David et Éva, maintenir les appareils essentiels, deux ou trois téléphones, une radio et quelques lampes pendant 72 heures nécessite généralement **une ou deux batteries externes de forte capacité**, en plus de piles de rechange pour la radio.

Si l'autonomie doit s'étendre sur plusieurs jours ou couvrir des besoins plus importants, une génératrice peut compléter ces solutions.

Prévoyez alors au minimum 15 à 20 litres de carburant pour une utilisation raisonnée sur trois jours (quelques heures par jour, réservées aux besoins essentiels), en évitant de la faire fonctionner en continu et toujours à l'extérieur de la maison ou du garage.



6- L'argent liquide : une ressource qu'on oublie trop souvent

David se souvient soudain d'un détail : les terminaux de paiement ne fonctionnent plus depuis la panne. Au dépanneur du coin, un client tente en vain de payer par carte. Sans électricité ni réseau, la plupart des commerces ne peuvent plus traiter les paiements électroniques, même lorsqu'ils restent ouverts.

Lors d'un blackout prolongé, l'argent liquide devient rapidement indispensable.

Les guichets automatiques cessent souvent de fonctionner, les commerces privilégient les transactions en espèces lorsqu'ils le peuvent, et certains services d'urgence ou de dépannage n'acceptent que ce mode de paiement.

Les bons réflexes

> Conserver une réserve d'argent liquide accessible en petites coupures, plus faciles à utiliser lorsque la monnaie devient rare.
>
> Prévoir un montant suffisant pour quelques jours de dépenses essentielles (eau, essence, nourriture).
>
> Garder cette réserve dans un endroit sûr, mais facilement accessible en cas de départ précipité.

Combien prévoir ?

Il n’existe pas de montant universel, mais pour une famille de quatre personnes, une réserve d’environ 200 à 400 $ CA (125 à 250 € environ) constitue une base raisonnable pour faire face aux dépenses essentielles pendant 72 heures :

- Quelques achats alimentaires de dépannage
- Du carburant
- Certaines dépenses imprévues

Privilégiez les petites coupures (5, 10 et 20 $ ou €).

Le bon réflexe : prévoir cette réserve à l’avance et la conserver dans un endroit sûr et facilement accessible.

7- Les accidents ou les blessures

En voulant ouvrir une boîte de conserve à la lueur de son téléphone, Lucas se coupe légèrement au doigt. Rien de grave, mais assez pour que David réalise qu'il n'a pas vérifié depuis longtemps le contenu de la trousse de premiers soins familiale.

« On a encore des pansements ? » demande-t-il à Éva, un peu inquiet.

Ce petit incident illustre une réalité fréquente lors des blackouts : plusieurs blessures surviennent non pas à cause de la panne elle-même… mais à cause des comportements improvisés.

Le stress pousse souvent les individus à agir rapidement sans toujours mesurer les risques. En situation de crise, ralentir reste parfois le meilleur réflexe.

Les situations les plus fréquentes ne sont généralement pas spectaculaires :

- Utilisation dangereuse de génératrices ou intoxication au monoxyde de carbone.
- Bougies laissées sans surveillance, brûlures causées par des bougies, réchauds ou appareils de cuisson.
- Chutes ou déplacements inutiles dans l'obscurité.
- Coupures lors de l'utilisation d'outils ou d'un ouvre-boîte.
- Entorses, petits traumatismes ou malaises liés à la chaleur, au froid ou à la déshydratation.

Un blackout n'augmente pas seulement le risque d'accident. Il peut aussi allonger le délai avant l'arrivée des secours. Les routes peuvent être encombrées, les communications perturbées et les services d'urgence fortement sollicités.

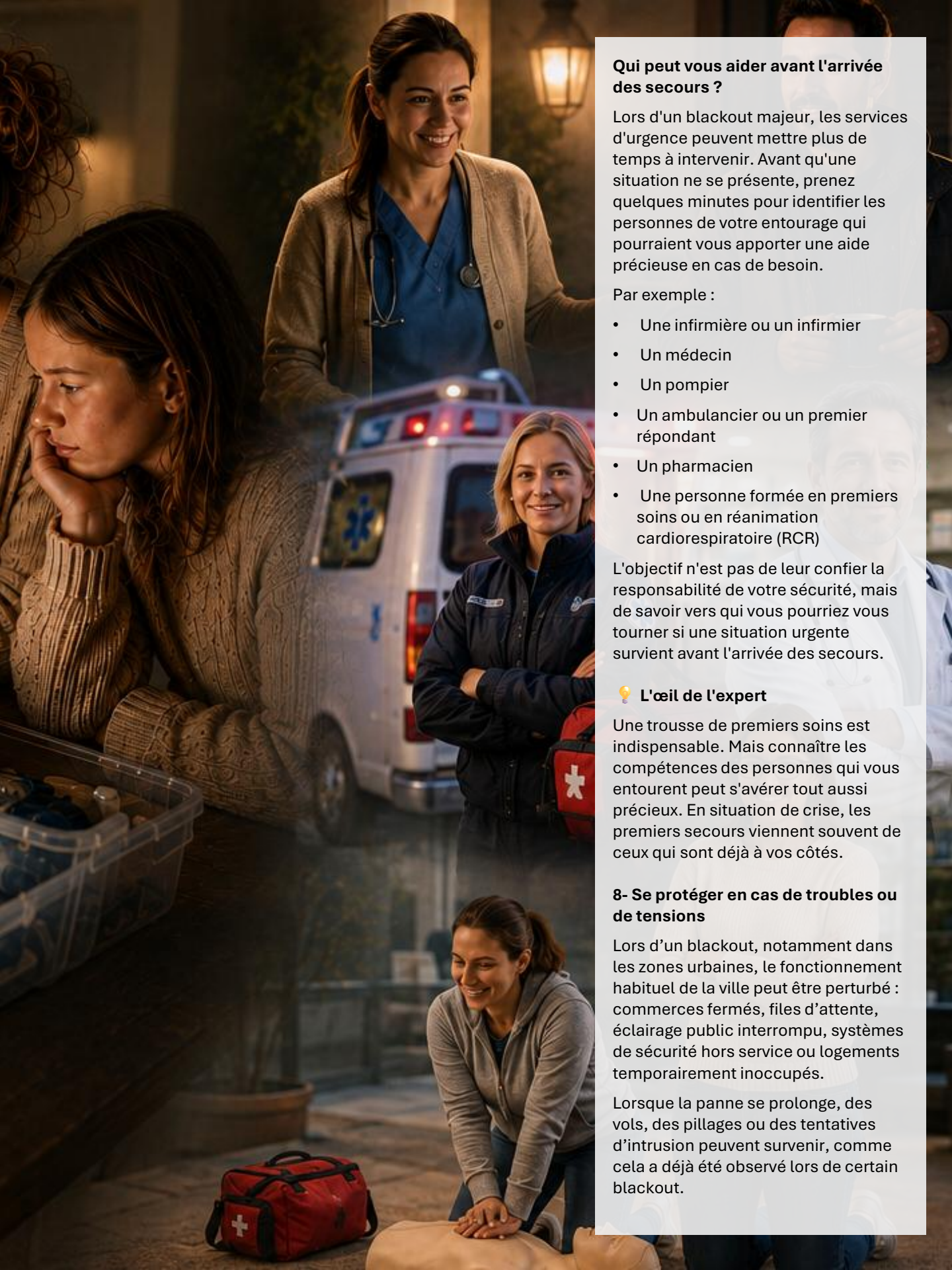
Dans ce contexte, la famille devient souvent le premier maillon de la chaîne de secours.

Être prêt avant que l'accident survienne

Une trousse de premiers soins devrait être facilement accessible et contenir notamment :

- Des pansements de différentes tailles.
- Des compresses stériles.
- Des bandages.
- Un antiseptique.
- Des gants jetables.
- Une couverture isothermique.
- Des ciseaux et une pince à épiler.
- Les médicaments personnels des membres de la famille.

Au-delà du matériel, une formation en premiers secours et en réanimation cardiorespiratoire (RCR) constitue un véritable atout. En cas d'arrêt cardiaque ou d'urgence médicale, les premiers gestes posés avant l'arrivée des secours peuvent faire toute la différence.



Qui peut vous aider avant l'arrivée des secours ?

Lors d'un blackout majeur, les services d'urgence peuvent mettre plus de temps à intervenir. Avant qu'une situation ne se présente, prenez quelques minutes pour identifier les personnes de votre entourage qui pourraient vous apporter une aide précieuse en cas de besoin.

Par exemple :

- Une infirmière ou un infirmier
- Un médecin
- Un pompier
- Un ambulancier ou un premier répondant
- Un pharmacien
- Une personne formée en premiers soins ou en réanimation cardiorespiratoire (RCR)

L'objectif n'est pas de leur confier la responsabilité de votre sécurité, mais de savoir vers qui vous pourriez vous tourner si une situation urgente survient avant l'arrivée des secours.

💡 **L'œil de l'expert**

Une trousse de premiers soins est indispensable. Mais connaître les compétences des personnes qui vous entourent peut s'avérer tout aussi précieux. En situation de crise, les premiers secours viennent souvent de ceux qui sont déjà à vos côtés.

8- Se protéger en cas de troubles ou de tensions

Lors d'un blackout, notamment dans les zones urbaines, le fonctionnement habituel de la ville peut être perturbé : commerces fermés, files d'attente, éclairage public interrompu, systèmes de sécurité hors service ou logements temporairement inoccupés.

Lorsque la panne se prolonge, des vols, des pillages ou des tentatives d'intrusion peuvent survenir, comme cela a déjà été observé lors de certain blackout.

Sans dramatiser ni céder à la peur, quelques précautions simples permettent de mieux protéger son logement et sa famille :

> Rester discret sur les ressources dont vous disposez : réserves de nourriture, carburant, argent liquide ou équipements de valeur.
>
> Fermer les rideaux ou les stores le soir pour limiter la visibilité de l'intérieur lorsque le quartier est plongé dans l'obscurité.
>
> Verrouiller systématiquement les portes et les fenêtres, même lorsque vous êtes à la maison.
>
> Limiter les déplacements non essentiels la nuit et privilégier, lorsque cela est possible, les sorties en journée.
>
> S'organiser avec des voisins de confiance pour rester en contact, partager les informations utiles et exercer une vigilance mutuelle.

LES PROFILS À RISQUE DANS LE FOYER

Chez David et Éva, une réalité s'impose depuis la première heure du blackout : Emma est diabétique, et son insuline dépend d'une conservation au froid. Une contrainte parmi tant d'autres pour cette famille… mais un rappel utile que chaque foyer porte ses propres vulnérabilités, parfois invisibles au quotidien.

La situation d'Emma rappelle une réalité essentielle : face à un blackout, nous ne sommes pas tous égaux.

Une même panne peut représenter un simple désagrément pour certains… et devenir rapidement un enjeu de santé ou de sécurité pour d'autres.

Chaque foyer possède ainsi ses propres vulnérabilités, parfois discrètes tant que tout fonctionne normalement, mais qui peuvent devenir prioritaires lorsque la panne se prolonge.

Des besoins médicaux qui ne peuvent pas attendre

Certains besoins deviennent rapidement prioritaires lorsque l'électricité disparaît : un médicament qui doit être conservé dans des conditions particulières, un appareil médical dépendant de l'électricité, une batterie à recharger ou un traitement qui ne peut pas être interrompu.

Dans le cas d'Emma, la question de l'insuline se pose immédiatement. Mais chaque situation est différente. L'essentiel est de connaître à l'avance les contraintes liées à son traitement et les solutions prévues en cas de panne prolongée.

Quelques questions permettent d'anticiper :

- Certains médicaments nécessitent-ils une conservation particulière ?
- Disposez-vous d'une réserve suffisante de médicaments essentiels ?
- Un équipement médical dépend-il de l'électricité ?
- Existe-t-il une batterie ou une solution de secours ?
- Savez-vous qui contacter si la panne se prolonge ?

Pour les médicaments et les équipements médicaux, ne laissez pas place à l'improvisation : conservez les consignes utiles accessibles et suivez les recommandations du pharmacien, du professionnel de santé ou du fabricant.

Des besoins différents selon les personnes

La vulnérabilité ne se limite pas aux besoins médicaux.

- **Les jeunes enfants** peuvent être davantage déstabilisés par l'obscurité et la rupture de leurs habitudes. Maintenir quelques repères, les rassurer et leur confier de petites responsabilités adaptées à leur âge peut les aider à mieux vivre la situation.
- **Les adolescents** peuvent ressentir particulièrement la perte des communications. Ne plus pouvoir joindre leurs amis, accéder aux réseaux ou obtenir de l'information peut devenir une source d'inquiétude. Avoir convenu à l'avance d'un point de rencontre et d'une façon de communiquer si les réseaux ne fonctionnent plus permet de réduire cette incertitude.
- **Les personnes âgées ou en perte d'autonomie** peuvent être plus sensibles au froid ou à la chaleur, rencontrer des difficultés pour se déplacer ou dépendre de certains services. Un ascenseur à l'arrêt, par exemple, peut rapidement devenir un obstacle important.
- Et n'oublions pas **les animaux domestiques** : eau, nourriture, médicaments éventuels et solution de transport doivent également faire partie de la préparation.

Un blackout agit comme un révélateur. Il met en évidence tout ce qui dépend discrètement de l'électricité, des habitudes ou du confort quotidien. Avant même qu'une crise survienne, prenez le temps d'identifier les personnes qui pourraient avoir besoin d'une attention particulière.

💡 **L'œil de l'expert**

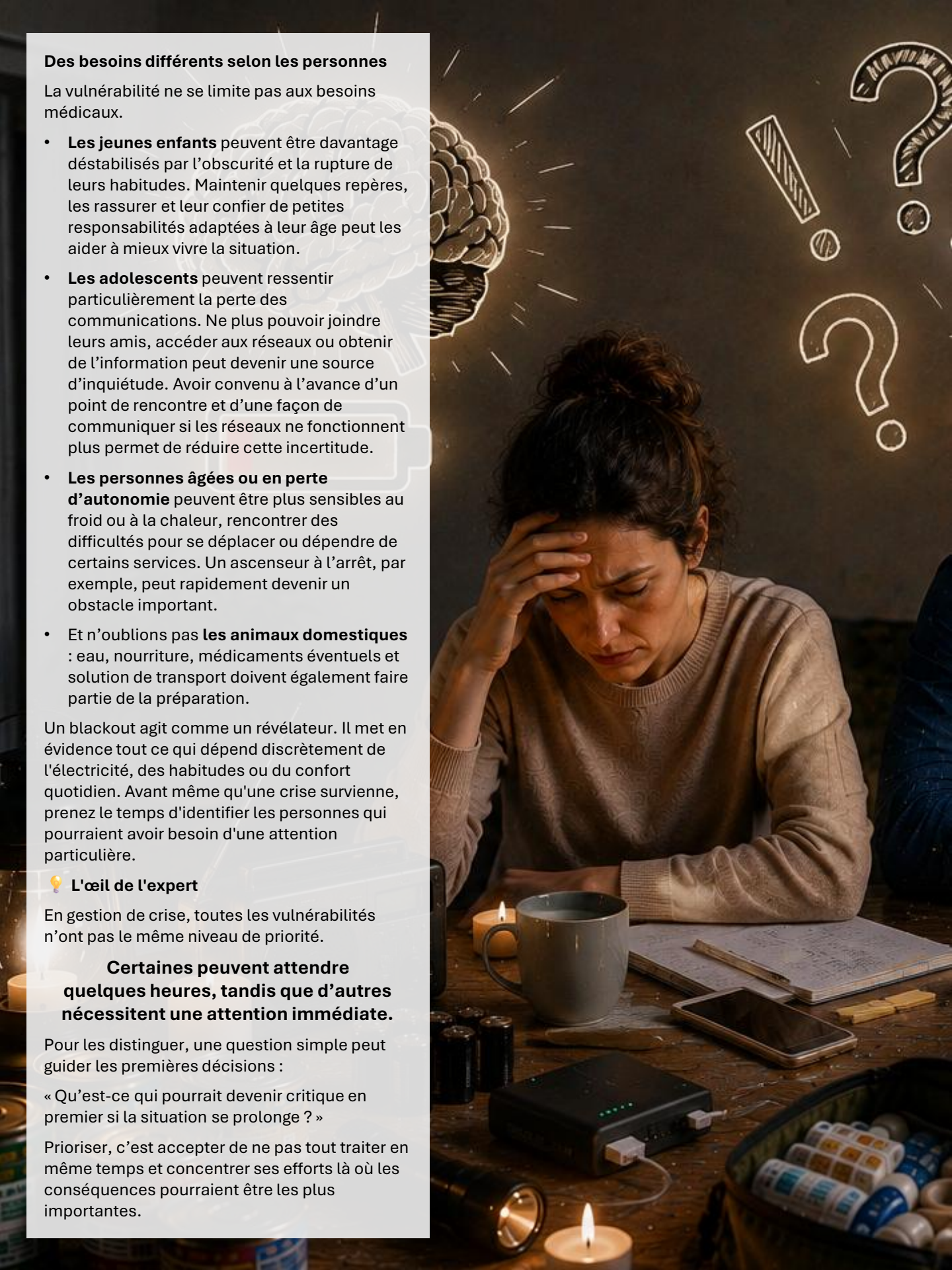
En gestion de crise, toutes les vulnérabilités n'ont pas le même niveau de priorité.

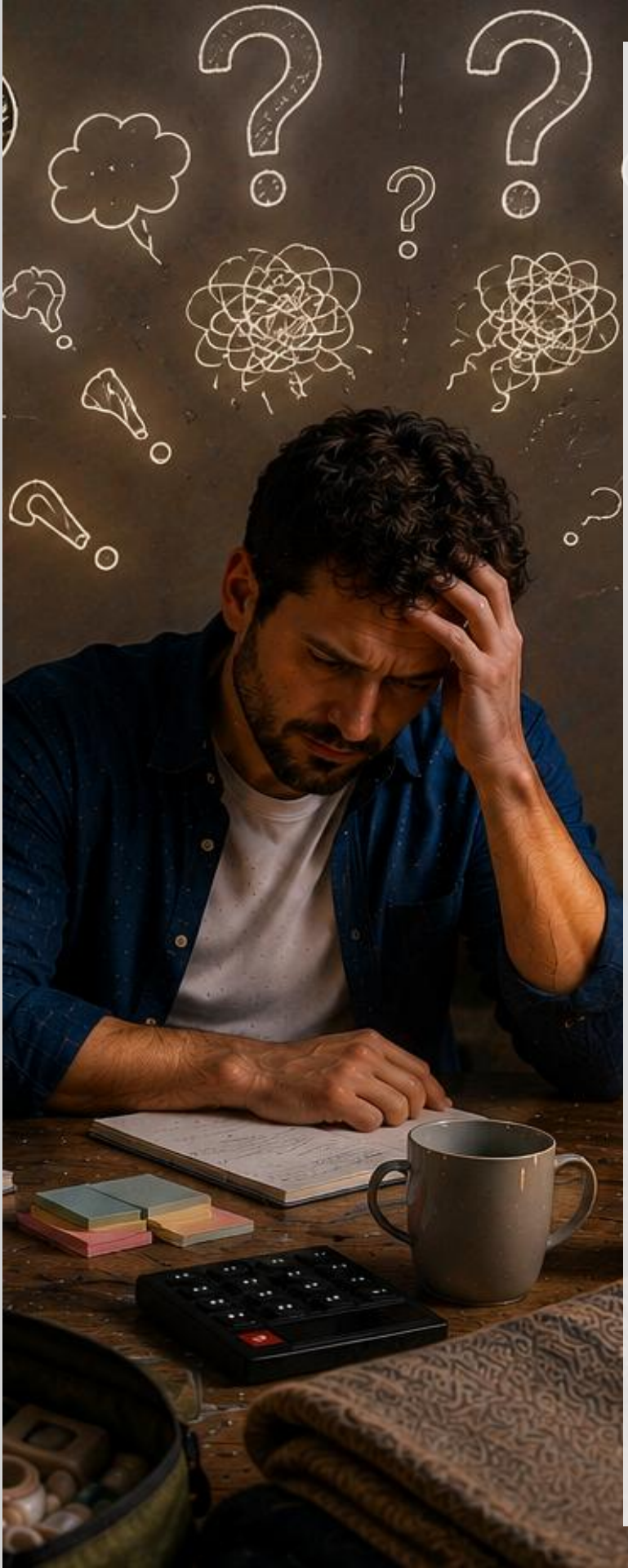
Certaines peuvent attendre quelques heures, tandis que d'autres nécessitent une attention immédiate.

Pour les distinguer, une question simple peut guider les premières décisions :

« Qu'est-ce qui pourrait devenir critique en premier si la situation se prolonge ? »

Prioriser, c'est accepter de ne pas tout traiter en même temps et concentrer ses efforts là où les conséquences pourraient être les plus importantes.





QUAND LA FATIGUE S'INSTALLE

Le deuxième jour touche à sa fin. Les gestes du début, remplir l'eau, répartir les rôles, rassurer les enfants sont devenus une routine. Mais cette routine a un coût. David et Éva dorment peu, mangent peu, et chaque discussion demande un effort qu'ils n'avaient pas anticipé. Ce soir-là, une simple question suffit à faire éclater la tension accumulée depuis 48 heures. David veut partir chez ses parents. Éva préfère rester pour surveiller la maison. Lucas prend parti. Emma pleure sans vraiment comprendre pourquoi.

Le blackout cesse progressivement d'être une crise logistique. Il devient une crise relationnelle.

Depuis plus de 48 heures, la famille prend des décisions en continu : quoi manger, qui appeler, comment économiser les batteries, quand dormir, faut-il partir, faut-il attendre. Chaque décision consomme de l'énergie mentale.

Les spécialistes parlent de fatigue décisionnelle : un phénomène où la qualité des décisions diminue à mesure que le cerveau s'épuise sous la pression, le stress et l'incertitude. Dans une famille, cette fatigue se manifeste rapidement :

- Irritabilité
- Impatience
- Conflits
- Difficulté à trancher
- Surcharge émotionnelle

Ces réactions sont normales. Elles traduisent la fatigue, le stress et l'incertitude.

Pour éviter que la situation ne se dégrade, il est utile de revenir à des objectifs simples : décider seulement des prochaines heures, communiquer calmement et accepter qu'aucune décision ne sera parfaite. La résilience familiale ne consiste pas à éviter tous les désaccords. Elle consiste à continuer d'avancer ensemble malgré eux.

Une astuce simple permet souvent de désamorcer ce type de désaccord : reformuler la question en

« qu'est-ce qu'on décide pour ce soir ? » plutôt que « qu'est-ce qu'on va faire ? ».

La première question a une réponse claire et atteignable.

La seconde, plus vaste, invite chacun à projeter ses craintes, ses hypothèses et ses désirs sur toute la durée de la crise, ce qui alimente inévitablement le désaccord.

En ramenant la discussion à un horizon très court, la famille cesse de négocier sur l'inconnu et recommence à négocier sur du concret.

Les bons réflexes

> Repérer les signes de fatigue décisionnelle chez soi ou chez un proche (impatience soudaine, ton qui monte, difficulté à se concentrer) avant qu'ils ne dégénèrent en conflit.
>
> Nommer ce que l'on ressent plutôt que de le laisser sortir sous forme de reproche : « je suis fatigué et à cran », plutôt que « tu ne comprends jamais rien ».
>
> Accorder une courte pause à la personne qui semble dépassée, plutôt que d'insister pour qu'elle décide immédiatement.
>
> Revenir sur une décision prise sous tension une fois le calme retrouvé, sans chercher à savoir qui avait raison.
>
> La résilience familiale ne consiste pas à éviter tous les désaccords. Elle consiste à continuer d'avancer ensemble malgré eux.

💡 L'œil de l'expert

En gestion de crise, nous observons souvent que les équipes les plus performantes ne sont pas celles qui prennent les meilleures décisions, mais celles qui continuent à communiquer malgré la fatigue.

Il en va de même pour une famille. Lorsque la tension monte, ralentir quelques minutes, partager les informations et fixer une priorité commune permet souvent d'éviter que la crise ne se transforme en conflit.

Conclusion

Un blackout nous rappelle une réalité que notre quotidien nous fait oublier : notre confort repose sur des systèmes dont nous dépendons sans même y penser. L'électricité, l'eau, les communications ou les paiements électroniques nous semblent acquis… jusqu'au moment où ils disparaissent.

Pourtant, la résilience d'une famille ne se mesure pas au nombre de lampes de poche ou de batteries qu'elle possède. Elle se construit bien avant la crise, dans les habitudes que l'on développe, les discussions que l'on prend le temps d'avoir et la capacité à rester calme lorsque tout devient incertain.

Personne ne peut empêcher une panne majeure ou une catastrophe. Mais chacun peut choisir de ne pas la subir. Quelques gestes simples, un minimum d'organisation et une compréhension des réactions humaines suffisent souvent à transformer une situation subie en une situation maîtrisée.

Alors, avant que la lumière ne s'éteigne pour de vrai, prenez le temps de vous préparer. Vérifiez votre matériel, parlez-en en famille, identifiez les fragilités et construisez un plan simple. Ces quelques heures de préparation peuvent changer complètement la manière dont vous vivrez les premières heures.

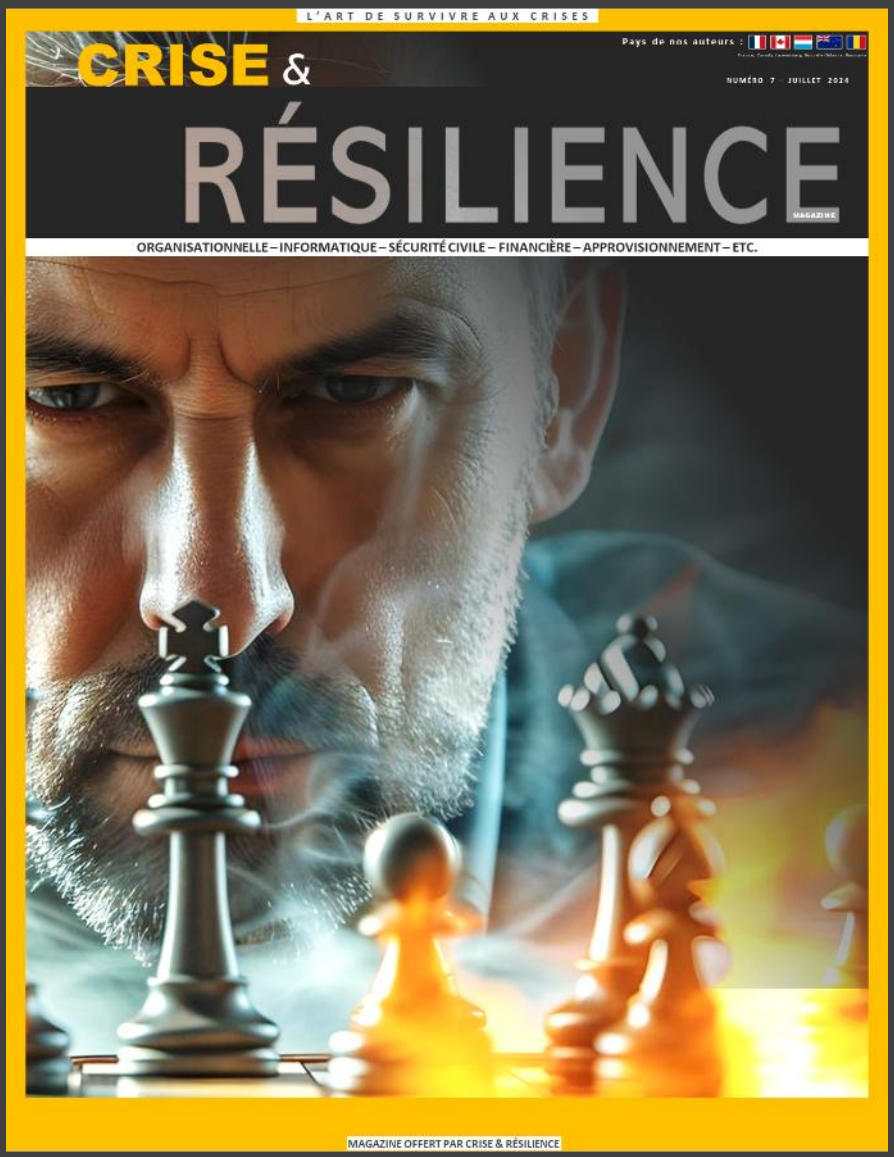
Car le jour où tout s'arrête, la question ne sera plus : "Que se passe-t-il ?" Mais : "Que fait-on maintenant ?" Et à ce moment-là, la ressource la plus précieuse ne sera pas l'électricité. Ce sera votre capacité à rester unie, organisée… et à garder votre sang-froid.

Chez David et Éva, le courant est finalement revenu au troisième jour, en pleine nuit. Personne ne s'en est rendu compte tout de suite, jusqu'à ce que le réfrigérateur se remette à ronronner. Emma, à moitié endormie, a simplement demandé : « C'est fini ? » Éva a souri : « Oui, ma chérie, c'est fini. »

Ce qu'ils retiendront de ces trois jours n'est pas la panne elle-même, mais la façon dont ils l'ont traversée ensemble. Et vous ?

Karine Maréchal Richard

RECEVEZ LE PROCHAIN MAGAZINE



Abonnez-vous

GRATUITEMENT

www.CriseEtResilience-Magazine.com