Le substrat numérique des cascades de défaillance

Propagation inter-sectorielle dans les infrastructures critiques européennes

Résumé opérationnel

Nicolas Roux - Analyste indépendant, résilience stratégique et dépendances numériques, août 2026.

Note d'analyse, DOI : https://doi.org/10.5281/zenodo.21285147, Licence CC BY 4.0

Note intégrale : nicolasroux.eu/publications, Contact : nr@nicolasroux.eu

Objet

Cette note analyse les défaillances en cascade entre secteurs d'infrastructures critiques à partir de six cas documentés : les pannes électriques ibérique (2025), texane (2021), italienne et nord-américaine (2003), l'exploitation systématique des interdépendances contre l'Ukraine (2017-2024) et l'attaque contre Change Healthcare (2024). Elle établit que ces cascades partagent un même substrat : la couche numérique par laquelle les défaillances traversent les frontières sectorielles. Elle en dérive une grille de critères permettant d'évaluer si un dispositif existant, cadre réglementaire ou exercice, prend la propagation inter-sectorielle pour objet. L'analyse repose exclusivement sur la documentation publique. Les critères qu'elle dérive sont prescriptifs au niveau de la conception des exercices et des plans, et elle ne propose aucune modification des instruments qu'elle examine.

Constats

1. La numérisation a unifié les infrastructures critiques en un graphe de dépendances unique, aux motifs de propagation récurrents. L'énergie et les télécommunications y occupent une position amont dont dépend la quasi-totalité des autres secteurs, de plus en plus par le biais du numérique. Quatre motifs reviennent dans les cas étudiés : la divergence (un nœud défaillant dégrade simultanément plusieurs secteurs qui en dépendent), la convergence (plusieurs défaillances amont atteignent le même service aval, comme la perte simultanée de l'électricité et des télécommunications pour les services d'urgence ibériques), la boucle de rétroaction (deux secteurs s'empêchent mutuellement de se rétablir, comme l'électricité et le gaz au Texas) et l'héritage transitif (un secteur hérite des dépendances des services dont il dépend). Ces propagations surviennent quelle que soit la nature du déclencheur :météorologique, accidentelle, criminelle ou étatique. Les cascades par dépendance numérique partagée (M.E.Doc 2017, Change Healthcare 2024) empruntent des liens qui n'existaient pas avant la numérisation des fonctions concernées.

2. Les mécanismes capables de contenir ces propagations existent, mais leur existence ne renseigne pas sur leur efficacité. Six mécanismes de contention sont identifiés à partir des données empiriques : séparation, architecture en mode dégradé, redondance locale, réplication, substitution, et la compétence organisationnelle qui conditionne l'activation des cinq autres. Les cas documentés

montrent que ces mécanismes constituent eux-mêmes des surfaces de vulnérabilité, selon quatre modes : ils peuvent être ciblés délibérément ou défaillir silencieusement (destruction des sauvegardes de Kyivstar, panne muette du système d'alarme lors du blackout nord-américain de 2003) ; leur dimensionnement temporel peut être inférieur à la durée de la perturbation (générateurs hospitaliers ibériques) ; leur disponibilité peut dépendre d'un tiers dont la coopération est révocable (limitations rapportées du service Starlink en Ukraine) ; et la compétence nécessaire à leur activation peut faire défaut, par non-acquisition ou par érosion. Un inventaire des mécanismes déployés, aussi complet soit-il, ne mesure aucun de ces quatre modes d'échec des mécanismes de contention.

3. La propagation inter-sectorielle échappe aux cadres existants, dont la partition sectorielle précède l'unification numérique. La projection des cas documentés sur les cadres CER, NIS2, DORA et, en France, la DGI 320 montre que chaque instrument couvre son périmètre avec cohérence, et que le mécanisme de propagation entre secteurs échappe à chacun d'eux. La classification demeure sectorielle, l'évaluation s'effectue au niveau de l'entité, et la coordination entre résilience physique et cybersécurité relève de dispositions de principe dont la mise en œuvre reste à la main des États membres.

Les dispositions relatives à la chaîne d'approvisionnement courent le long de chaque lien bilatéral entre une entité et ses fournisseurs, et laissent inobservée la concentration d'un grand nombre d'entités sur un même intermédiaire partagé. DORA est le seul instrument qui supervise directement un tel intermédiaire, mais il le fait pour le seul secteur financier.

La DGI 320 illustre la même configuration au niveau national : la transversalité figure dans sa matrice d'analyse et disparaît de sa partie prescriptive, qui reste sectorielle. Les exercices publics documentés, y compris les plus avancés comme Locked Shields, simulent des environnements inter-sectoriels sans faire de la propagation un objet d'évaluation doté de critères propres. Les initiatives politiques récentes, du rapport Niinistö à la stratégie d'Union de la préparation, reconnaissent explicitement les crises en cascade. Le traitement proposé porte cependant sur la coordination de la réponse, et aucune méthodologie publique ne définit à ce jour les critères permettant de tester la propagation *ex ante*.

Livrable : une grille d'évaluation dérivée de l'empirie

La note propose dix critères, applicables par tout lecteur disposant d'un accès aux dispositifs existants, publics ou non. Cinq portent sur le scénario : teste-t-il la propagation causale entre au moins deux secteurs interdépendants ; couvre-t-il la convergence de plusieurs défaillances amont vers les mêmes services aval ; intègre-t-il la dimension temporelle de la cascade (vitesse, fenêtre d'intervention, seuil d'irréversibilité) ; inclut-il une condition initiale dégradée ; teste-t-il la propagation au-delà du périmètre national ou juridictionnel de l'entité évaluée. Cinq portent sur les mécanismes de contention : sont-ils eux-mêmes soumis au stress du scénario ; le scénario prévoit-il leur neutralisation (destruction des sauvegardes, défaillance silencieuse de la détection, boucle de rétroaction bloquant la restauration) ; l'évaluation identifie-t-elle les dépendances à des acteurs dont la coopération est révocable, et la juridiction dont relèvent ces acteurs ; l'organisation a-t-elle démontré, dans les conditions du scénario, la capacité à les activer ; et leur activation dépend-elle d'une couche de détection ou d'orchestration incluse dans le périmètre du scénario.

La confrontation de ces critères aux exercices, plans et architectures en place relève des acteurs qui en ont la charge et l'accès. Des travaux non publics peuvent couvrir tout ou partie des lacunes identifiées et seul le lecteur qui y a accès est en position d'en juger.

Périmètre et limites

La note se concentre sur l’illustration des modes de propagation et des mécanismes de contention, à travers les nœuds les mieux documentés dans les cas d’étude (énergie, télécommunications). Les structures internes de dépendance de ces nœuds amont ou des secteurs aval sont tout aussi pertinentes pour un acteur privé ou public intervenant dans un de ces nœuds ou secteurs, mais leur analyse dépasse le périmètre de cette note, qui n’a pour objectif que de rendre manifeste l’existence du graphe de dépendances et des mécanismes associés. Trois questions ouvertes sont identifiées pour des travaux ultérieurs : la conception des systèmes critiques pour le mode dégradé, l'absence de cadre bilatéral européen de continuité numérique, et enfin l'allocation de l'effort de résilience à travers le graphe, entre durcissement des nœuds où se concentrent les exigences de résilience héritées et élévation du niveau de base qu'appelle la propagation par le maillon le plus faible.

Citation suggérée : Roux, N., « Le substrat numérique des cascades de défaillance : propagation inter-sectorielle dans les infrastructures critiques européennes », août 2026, DOI 10.5281/zenodo.21285147, CC BY 4.0.