Le substrat numérique des cascades de défaillance

Propagation inter-sectorielle dans les infrastructures critiques européennes

Nicolas Roux, août 2026
DOI: https://doi.org/10.5281/zenodo.21285147

Synthèse liminaire

La numérisation des fonctions critiques a transformé un ensemble de systèmes coexistants en un graphe de dépendances unique, dont le numérique constitue le substrat commun et dans lequel l'énergie et les télécommunications occupent une position amont dont dépend la quasi-totalité des autres secteurs. L'analyse de pannes majeures (péninsule ibérique 2025, Texas 2021, Italie et Amérique du Nord 2003) et l'exploitation systématique des interdépendances contre l'Ukraine montrent que les défaillances se propagent entre secteurs selon des motifs récurrents : divergence d'une défaillance depuis un nœud dont dépendent plusieurs secteurs, convergence de plusieurs défaillances amont vers les mêmes services aval, boucles de rétroaction empêchant la restauration, héritage transitif des dépendances. Ces propagations surviennent quelle que soit la nature du déclencheur, accidentelle ou adversariale.

Six mécanismes capables d'interrompre ces propagations sont identifiés à partir des études de cas : séparation, architecture en mode dégradé, redondance locale, réplication, substitution et compétence organisationnelle. L'analyse établit que ces mécanismes constituent eux-mêmes des surfaces de vulnérabilité : ils peuvent être ciblés, sous-dimensionnés, dépendants d'un tiers dont la coopération est révocable, ou inopérants faute de compétence pour les activer. L'existence d'un mécanisme de contention ne renseigne pas sur son efficacité dans les conditions réelles d'un incident.

La projection des cas documentés sur les cadres existants (CER, NIS2, DORA) montre que chacun couvre son périmètre avec cohérence et que le mécanisme de propagation inter-sectorielle tombe dans l'interstice entre ces périmètres, leur partition sectorielle reproduisant une topologie antérieure à l'unification numérique. Les exercices publics documentés simulent des environnements inter-sectoriels sans faire de la propagation un objet d'évaluation doté de critères propres. Les initiatives politiques européennes récentes, du rapport Niinistö à la stratégie d'Union de la préparation, reconnaissent l'enjeu sans encore en fournir l'outillage.

La note propose en conséquence des critères d'évaluation dérivés des cas d'étude, applicables aux scénarios d'exercice comme aux mécanismes de contention, et utilisables par tout lecteur disposant d'un accès aux dispositifs existants, publics ou non. La note ne propose aucune modification des instruments qu'elle examine et n'avance aucun constat sur les exercices dont la documentation n'est pas publique.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147

Table des matières

Synthèse liminaire..... 1
Introduction..... 3
1 - Le graphe de dépendances..... 4
2 - Cas d'étude des propagations en cascade..... 6
2.1 - Cas d'étude civils..... 6
2.1.1 - Panne électrique ibérique, 28 avril 2025..... 6
2.1.2 - Tempête hivernale texane, février 2021..... 7
2.1.3 - Panne électrique italienne, 28 septembre 2003..... 8
2.1.4 - Panne électrique nord-américaine, 14 août 2003..... 8
2.2 - Exploitation adversariale des interdépendances..... 9
2.2.1 - Exploitation des interdépendances contre l'Ukraine..... 9
2.2.2 - Cascade inter-sectorielle adversariale hors conflit : Change Healthcare..... 11
3 - Ce qui contient les propagations..... 11
3.1 - Mécanismes de contention des cascades..... 11
3.1.1 - Mécanismes de contention intégrés à la conception..... 12
3.1.2 - Capacités pré-positionnées..... 13
3.1.3 - Bascule vers une infrastructure tierce..... 14
3.1.4 - La compétence conditionne l'utilité des mécanismes de contention..... 14
3.2 - Les mécanismes de contention sont eux-mêmes vulnérables..... 14
3.2.1 - Les mécanismes peuvent être ciblés et dégradés..... 14
3.2.2 - Le dimensionnement temporel des mécanismes de contention..... 15
3.2.3 - La maîtrise des mécanismes de contention..... 15
3.2.4 - Coût observé de la réponse non planifiée..... 17
3.2.5 - Résumé des enseignements empiriques sur les mécanismes de contention..... 17
4 - Conclusions analytiques et cadre évaluatif..... 18
4.1 - Ce que les données empiriques révèlent..... 18
4.2 - Projection sur les cadres régulatoires existants..... 19
4.3 - Critères d'évaluation dérivés des cas documentés..... 22
4.4 - Questions ouvertes..... 24
Conclusion..... 26
Remerciements..... 27

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

Introduction

Les infrastructures modernes présentent des modes de défaillance en cascade, comme le montrent des cas documentés en Espagne, en Italie et aux États-Unis, tandis que le conflit en Ukraine a mis en lumière l'exploitation adversariale délibérée de ces mêmes mécanismes. Ces cas d'étude et modes de défaillance en cascade présentent des caractéristiques communes qui émergent de la connectivité forte et encore croissante entre différents secteurs d'activité, notamment par le biais du numérique.

La migration généralisée du contrôle-commande vers le protocole IP[1], la numérisation de la santé[2] et du secteur bancaire[3], l'interconnexion croissante du maillage électrique européen[4] ou encore plus récemment l'adoption massive de l'IA[5] ont transformé un ensemble de systèmes co-existants en un unique graphe de dépendances liant tous les secteurs d'activité. Cette couche numérique commune est désignée dans la suite de cette note comme le substrat du graphe : c'est par elle que des secteurs sans lien physique partagent désormais des chemins de propagation, et c'est son extension continue qui fait du graphe un objet mouvant plutôt qu'un état stabilisé. La section 1 formule une description de ce graphe de dépendances.

Plusieurs cadres internationaux et exercices inter-sectoriels de grande ampleur visent à tester la résilience des infrastructures critiques. On retrouve parmi les principaux cadres le Handbook for Cyber Stress Tests de l'Agence de l'Union européenne pour la cybersécurité (ENISA)[6], le cadre d'action de Sendai[7], le Digital Operational Resilience Act européen[8], la directive CER (UE 2022/2557) sur la résilience des entités critiques[9] ou encore les NATO Baseline Requirements for National Resilience[10]. Côté exercices on retrouve les Locked Shields et Crisis Management Exercise de l'OTAN, le Cyber Storm des USA ou encore le Cyber Europe 2026 de l'UE. Cette préoccupation a par ailleurs atteint le niveau politique le plus élevé de l'Union : le rapport remis par Sauli Niinistö à la présidente de la Commission européenne en octobre 2024[11] recommande une approche de préparation globale couvrant l'ensemble des risques, et la stratégie d'Union de la préparation publiée en mars 2025[12] en décline les orientations en trente actions, dont la conduite régulière d'exercices de préparation à l'échelle de l'Union.

Toutefois, l'examen des rapports publics disponibles révèle un décalage entre la sophistication croissante des environnements simulés et le traitement de la propagation inter-sectorielle comme objet d'évaluation. Les exercices techniques les plus avancés simulent désormais des systèmes inter-sectoriels au sein d'un même environnement : Locked Shields intègre des systèmes de contrôle industriel simulés couvrant le réseau électrique, le traitement de l'eau, les télécommunications et le secteur bancaire, y compris certaines dépendances entre systèmes telles que l'alimentation en carburant d'une base aérienne pilotée par automates.[13] [14] [15] Les rapports publics et analyses académiques disponibles documentent l'évaluation des tactiques de défense, de la préparation des équipes nationales et de la coordination multi-acteurs lorsque plusieurs systèmes sont attaqués.[16] En revanche, aucun de ces documents ne fait de la propagation causale d'une défaillance entre secteurs interdépendants un objet d'évaluation en soi, doté de critères de réussite propres : ni boucle de rétroaction entre secteurs simulés, ni condition initiale dégradée, ni neutralisation des mécanismes

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

de contention, ni dimension temporelle de la cascade. Le déclencheur y demeure par ailleurs principalement cyber (à l'exception du CMX de l'OTAN), quand les données empiriques relatées dans cette note montrent des couplages opérant dans les deux sens entre défaillances physiques et numériques. Le manuel ENISA illustre le même décalage sur le plan réglementaire : il identifie les effets en cascade et les interdépendances parmi les objectifs des stress tests, tout en définissant l'exercice comme une évaluation individuelle d'entités, avec un unique exemple développé mono-sectoriel.

Par ailleurs, le cadre européen lui-même sépare structurellement la résilience physique de la cybersécurité.[17] La directive CER exclut explicitement de son périmètre les matières couvertes par la directive NIS2 (article 1(2)), et prescrit leur coordination par un article de principe dont la mise en œuvre est laissée à chaque État membre. Les cas documentés dans cette note, en particulier les attaques cyber-cinétiques contre le réseau électrique ukrainien, illustrent pourquoi le couplage entre ces deux domaines est précisément ce que cette séparation peine à capturer.

La présente analyse repose exclusivement sur la documentation publique accessible. Des exercices classifiés ou des volets non publiés peuvent couvrir tout ou partie des mécanismes de propagation documentés ici. Le lecteur disposant d'un accès à ces travaux est en position d'évaluer dans quelle mesure les lacunes identifiées dans cette note sont effectivement comblées. Il reste que ce sont les publications accessibles qui guident la très grande majorité des organisations, y compris publiques, soumises à ces cadres.

1 - Le graphe de dépendances

Les termes caractérisant ce graphe sont entendus ici au sens établi dès 2001 par Rinaldi, Peerenboom et Kelly[18] : une dépendance est une relation orientée par laquelle l'état d'un secteur conditionne celui d'un autre, et une interdépendance est la relation bidirectionnelle que forment deux dépendances de sens opposés.

La structure de ce graphe produit des motifs de propagation récurrents. Le premier est la divergence : un nœud dont dépendent plusieurs secteurs en parallèle les dégrade tous simultanément lorsqu'il défaille. Ce motif recouvre deux phénomènes que la littérature distingue : la défaillance de cause commune décrite par Rinaldi et al., où le nœud commun est le déclencheur lui-même, comme la tempête texane de 2021 frappant à la fois les infrastructures gazières et les moyens de production électrique, et la défaillance par dépendance partagée, où le nœud commun est un service dont dépendent des secteurs par ailleurs indépendants, comme le logiciel comptable ukrainien M.E.Doc en 2017.

Le deuxième est la convergence : plusieurs défaillances amont, quelle que soit leur origine, atteignent le même service aval et y produisent un effet multiplicateur. Lors de la panne électrique ibérique de 2025, la défaillance du réseau électrique et celle, induite, des télécommunications ont convergé vers les services d'urgence, privés à la fois de leurs outils et de leur capacité de coordination.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

Le troisième est la boucle de rétroaction, c’est à dire l’activation d'une interdépendance dans laquelle deux nœuds s'empêchent mutuellement de se rétablir : lors de la panne électrique italienne de 2003, les routeurs internet sont tombés avec le courant, rendant impossible la communication nécessaire à la reconnexion électrique. Cette boucle peut être directe comme dans l’exemple cité ou indirecte, transitant par un ou plusieurs nœuds tiers.

Le quatrième est l'héritage transitif : un secteur hérite des dépendances des services dont il dépend. Lors de la panne électrique ibérique, ce n'est pas la santé qui a été frappée mais le réseau électrique, cependant la chaîne de dépendances a transmis la défaillance jusqu'au soin des patients via les dossiers numériques et les serveurs qui les hébergent.

À ces motifs structurels s'ajoute une condition d'état : Rinaldi et al. nomment défaillance aggravante (*escalating failure*) la situation où une perturbation survient alors qu'une autre, indépendante, dégrade déjà la capacité de réponse. Les opérations documentées en section 2.2, où les cyberattaques accompagnent les campagnes de frappes physiques, en constituent l'illustration la plus nette. Cette condition est reprise comme critère d'évaluation en section 4.3.

Ces caractéristiques conduisent à rendre certains nœuds du graphe particulièrement critiques. Le fait que les quatre cas d’étude civils documentés dans cette note impliquent le réseau électrique comme vecteur central de propagation n’est pas un artefact de sélection : il reflète la position de l’électricité comme nœud amont dont dépend le fonctionnement de la quasi-totalité des autres secteurs, notamment à travers le numérique. Le numérique occupe dans ce graphe une position double. Il en constitue l'un des nœuds amont, au même titre que l'énergie : la défaillance des télécommunications ou des services numériques dégrade l'ensemble des secteurs qui en dépendent. Il en constitue surtout le substrat : la couche commune par laquelle les secteurs se lient entre eux, y compris lorsqu'ils n'entretiennent aucun couplage matériel. Les cas M.E.Doc et Change Healthcare documentés en section 2.2 relèvent de ce second rôle : des secteurs physiquement indépendants y partagent des modes de défaillance parce que leurs fonctions transitent par les mêmes intermédiaires numériques. La distinction importe pour l'analyse, car chaque numérisation d'une fonction ajoute au graphe une arête qui n'est déclarée nulle part et qui ne devient visible, le plus souvent, qu'à son activation.

La présente note se concentre sur les nœuds amont du graphe de dépendances (énergie, télécommunications) et sur les interfaces numériques par lesquelles les défaillances se propagent entre secteurs. Les secteurs aval (dont l’eau, l’alimentation, le transport, la santé) apparaissent dans les cas d'étude en tant que récepteurs des cascades documentées. L'analyse de leurs structures internes de dépendance et de leurs mécanismes de contention spécifiques dépasse le périmètre de cette note.

Le niveau de granularité du graphe est à adapter aux besoins de l’analyse et aux données disponibles. La présente note retient volontairement le niveau descriptif du graphe, la modélisation quantitative constituant un champ établi[19] hors de son périmètre.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

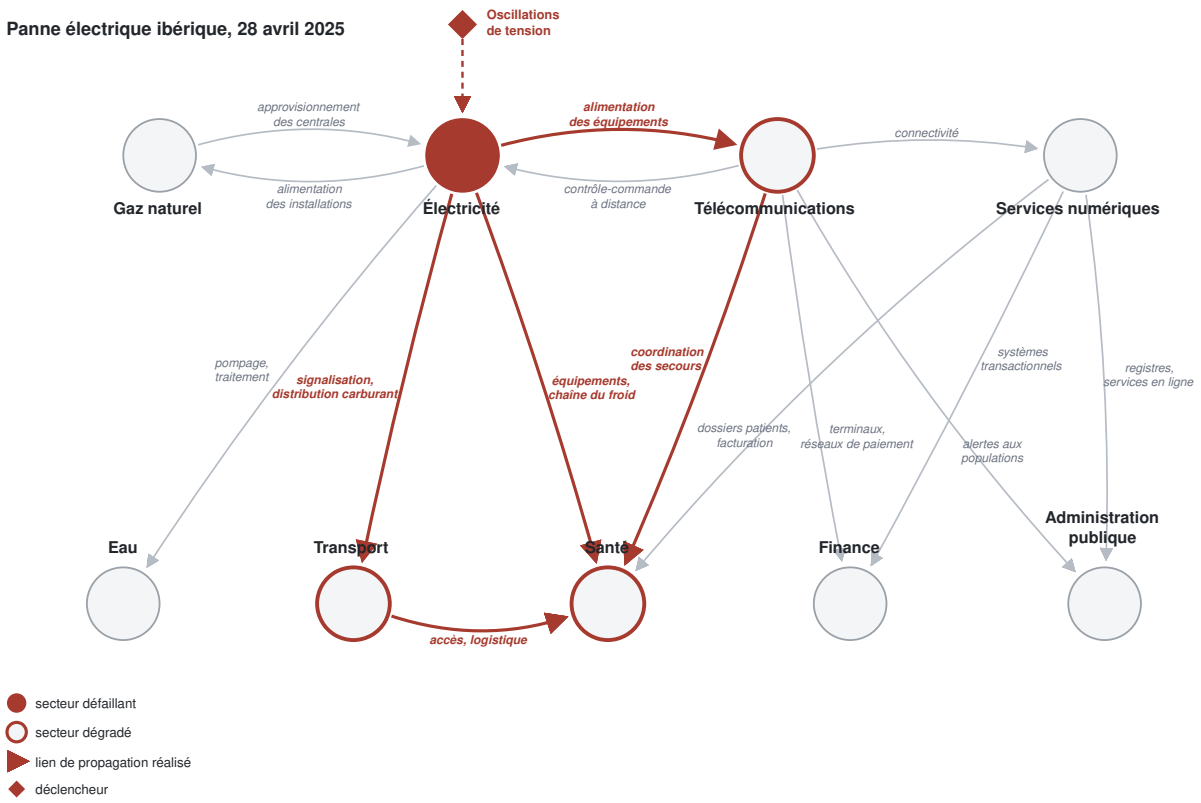

Figure 1: Représentation simplifiée à visée illustrative de la panne ibérique (en rouge) projetée sur le graphe de dépendances

2 - Cas d’étude des propagations en cascade

Cette section vise à identifier comment les interdépendances entre différents secteurs impactent les infrastructures en cas d’évènements non intentionnels (évènements météorologiques, défaillances internes à un ou plusieurs systèmes) ou intentionnels (attaques par une entité tierce).

2.1 - Cas d’étude civils

Les évènements d’origine accidentelle ou exogène listés ici sont abordés sous l’angle des modes de défaillance cités en section 1. Les cascades, boucles de rétroaction et chaînes de dépendances présentées ici ont été révélées par leur activation suite à un évènement imprévu, par opposition à une exploitation intentionnelle.

2.1.1 - Panne électrique ibérique, 28 avril 2025

Ce cas est le plus récent cas civil d’échec en cascade d’infrastructures, et il a bénéficié d’une analyse extensive[20] menée par un panel international d’experts. La panne a touché plus de 50 millions de personnes et a duré plus de 10 heures[21]. La défaillance initiale observée a été une série d’oscillations de tension dans le réseau électrique, conduisant à des déconnexions des stations

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

productrices d’énergie renouvelable. La perte de génération électrique a induit un effondrement du trafic réseau à 10 % de la normale[22].

Ces effets combinés (génération électrique et télécommunications) ont entre autres atteint les services hospitaliers, dont les mécanismes d’adaptation (utilisation de générateurs de secours, triage des équipements, dossiers papier) ont rapidement atteint leurs limites (capacité des générateurs de secours, utilisation restreinte d’équipements, chaîne du froid médicaments menacée). L’impact sur la santé s’est étendu au-delà des seuls services hospitaliers : le volume d’appels d’urgence s’est effondré, les feux de signalisation et les stations-service ont cessé de fonctionner[23], créant un effet accidentogène conjoint et réduisant la réactivité des secours pour répondre à cette incidence accrue d’accidents. Huit décès directement liés à la panne ont été rapportés, avec une surmortalité probablement supérieure à ce bilan direct[24], pour une panne qui a duré 10 heures et dans un contexte d’état initial non dégradé.

Aucune région concernée n'avait de plan de continuité spécifique pour une panne électrique prolongée affectant les services médicaux d'urgence. Cette fragilité n’est pas un cas isolé : les causes sont similaires à un incident ayant eu lieu dans le sud-est de l’Europe en 2024[25].

Les impacts sur le secteur de la santé illustrent le fait qu’un secteur hérite des dépendances des secteurs dont lui-même dépend : les services de secours dépendent d’un accès aux points de vente de carburant et à un système de signalisation fonctionnel, qui eux-mêmes dépendent du bon fonctionnement du réseau électrique, et donc les services de secours dépendent indirectement du réseau électrique. Cette analyse peut sembler évidente dans ce cas précis mais certains services ont des chaînes de dépendances à la fois plus complexes et tout aussi critiques pour leur bon fonctionnement, rendant nécessaires la cartographie et la prise en compte du graphe de dépendances complet d’un acteur lorsque des cadres ou exercices visent à mesurer sa résilience.

2.1.2 - Tempête hivernale texane, février 2021

Une tempête hivernale a frappé le réseau électrique texan pendant l’hiver 2021, privant d’électricité environ 4,5 millions de foyers au pic de la panne, certains pendant plusieurs jours[26]. Ce cas d’étude est illustratif des boucles de rétroaction inter-sectorielles mentionnées en section 1.

La séquence d’évènements a débuté par un évènement météorologique (épisode de froid extrême) ayant conduit au gel de têtes de puits gaziers et de certaines infrastructures de traitement du gaz naturel. La production de gaz a en conséquence chuté, et les centrales à gaz (qui représentaient la principale source de production électrique texane) ont vu leur approvisionnement chuter à leur tour, ce qui a forcé les opérateurs du réseau électrique à procéder à des délestages massifs.

Ces délestages ont privé les installations gazières d’électricité dont elles dépendent pour fonctionner, ce qui a aggravé la perte de production de gaz, et donc de nouveau aggravé les

DOI: https://doi.org/10.5281/zenodo.21285147

délestages. Le rapport conjoint de la Federal Energy Regulatory Commission (FERC) et de la North American Electric Reliability Corporation (NERC) mentionne explicitement ce verrouillage mutuel[27] et le communiqué de presse associé indique que 43,3% des baisses de production de gaz étaient dues au gel et aux conditions météo, et 21,5% aux pertes d'alimentation électrique des installations de production, de collecte ou de traitement[28]. La forte interdépendance entre ces deux secteurs a conduit à une boucle de rétroaction aggravant le problème[29] et les empêchant mutuellement de se rétablir.

La panne aura causé 246 décès dont une majorité par hypothermie[30], illustrant par comparaison à la panne ibérique le fait que la durée de la panne et son contexte ont une forte incidence sur les effets finaux.

Le rapport FERC/NERC montre que les infrastructures gazières n'avaient pas été identifiées par l'opérateur électrique Electric Reliability Council of Texas (ERCOT) comme « charges critiques » à garder en priorité actives lors des plans de délestage. Quand les délestages ont été ordonnés, l'opérateur a coupé l'alimentation des installations mêmes qui devaient fournir le gaz aux centrales de production d'électricité.

Cette boucle de rétroaction semble donc évitable ou au moins mitigeable, mais cela implique d'avoir au préalable identifié les dépendances des systèmes critiques et responsabilisé leurs fournisseurs, et peut aussi dépendre de facteurs externes comme le montre la section 3 de la présente note.

2.1.3 - Panne électrique italienne, 28 septembre 2003

Cette panne a impacté environ 45 à 57 millions de personnes selon les estimations en Italie et s'est propagée dans les zones frontalières suisses, pour une durée de restauration allant jusqu'à 19 heures selon les régions, et a provoqué des coupures au-delà des frontières italiennes, en Suisse (canton de Genève, environ 3 heures).[31]

Sa particularité est d'avoir exposé elle aussi une boucle de rétroaction, cette fois entre le secteur de l'énergie et celui des télécommunications. Le contrôle-commande permettant de piloter le réseau électrique transite par internet, mais l'accès à internet nécessite que les dispositifs physiques (routeurs) soient alimentés en électricité. Une fois ces routeurs désalimentés, le rétablissement du réseau électrique est compromis. Ce cas est le fondement empirique de la formalisation par Buldyrev et al.[32] de la fragilité non-linéaire des réseaux couplés : la défaillance d'un nœud dans le réseau A provoque des défaillances dans le réseau B qui aggravent à leur tour la défaillance de A.

2.1.4 - Panne électrique nord-américaine, 14 août 2003

Quelques semaines avant la panne italienne, une panne d'ampleur comparable a frappé le nord-est des États-Unis et l'Ontario (Canada), privant d'électricité environ 50 millions de personnes. L'enquête conjointe États-Unis/Canada a identifié parmi les causes principales une perte de conscience situationnelle des opérateurs du réseau : le système d'alarme logiciel du centre de

DOI: https://doi.org/10.5281/zenodo.21285147

contrôle de FirstEnergy, l'opérateur à l'origine de la cascade, est tombé en panne silencieusement en raison d'un défaut logiciel, privant les opérateurs de toute alerte visuelle et sonore sur l'état du réseau pendant plus d'une heure sans qu'ils en soient informés[33]. Les opérateurs ont continué à travailler en croyant observer un réseau électrique stable alors que des lignes de transmission surchargées tombaient successivement, propageant la défaillance jusqu'à l'effondrement en cascade du réseau régional. Ce cas est mobilisé dans la section 3 de la présente note pour illustrer la vulnérabilité des mécanismes de détection eux-mêmes.

2.2 - Exploitation adversariale des interdépendances

Les cas civils de la section 2.1 documentent l'existence manifeste des modes de défaillance en cascade et en boucle des infrastructures modernes. Ces modes de défaillance, dans le cas de conflits ouverts ou non, constituent un moyen d'action exploitable par un adversaire. Les données empiriques montrent que pour maximiser les effets d'une attaque, un adversaire peut simultanément cibler des systèmes interdépendants et les moyens (voir section 3) permettant d'interrompre la propagation des modes de défaillance (générateurs de secours, stocks de matériels de rechange, moyens logistiques, solutions alternatives etc), le tout dans un contexte externe initial difficile pour le défenseur.

2.2.1 - Exploitation des interdépendances contre l'Ukraine

Avant même l'offensive russe en Ukraine, en juin 2017, le mécanisme de mise à jour d'un logiciel comptable largement utilisé en Ukraine (M.E.Doc) a été compromis par le renseignement militaire russe et utilisé pour distribuer un logiciel destructeur à l'ensemble de ses utilisateurs[34][35]. L'attaque s'est propagée via les réseaux d'entreprise des organisations infectées jusqu'à leurs partenaires commerciaux dans au moins 65 pays.[36] Les secteurs touchés n'avaient aucune dépendance physique entre eux mais ont pourtant été simultanément affectés : opérations portuaires du premier transporteur maritime mondial paralysées pendant plus d'une semaine, chaînes de production pharmaceutique interrompues, dossiers patients et systèmes de radiologie inaccessibles dans des établissements hospitaliers américains, système de surveillance des radiations de Tchernobyl hors service[37]. Ce qui relie ces secteurs est le substrat numérique lui-même : leur dépendance commune à des services partagés. La numérisation de la comptabilité, de la logistique portuaire, de la production industrielle et de la gestion hospitalière a créé le chemin de propagation commun par lequel une attaque ciblant un seul pays a dégradé des fonctions critiques dans des secteurs physiquement indépendants à l'échelle mondiale.

Le 24 février 2022, l'Ukraine a subi une cyberattaque d'ampleur ciblant les modems et routeurs (moyens d'accès à internet) de l'opérateur d'accès par satellite Viasat. L'opérateur de cybersécurité SentinelOne évoque comme raison plausible de l'attaque une tentative de priver les forces armées ukrainiennes d'une partie de leurs moyens de contrôle-commande à distance. L'attaque a eu pour effet collatéral de priver 5800 éoliennes d'accès à internet en Allemagne, interrompant leurs moyens de contrôle et de supervision et les rendant ainsi temporairement inopérantes.[38] Des accès à internet résidentiels ont aussi subi des défaillances en France, Hongrie, Grèce, Italie et Pologne.

DOI: https://doi.org/10.5281/zenodo.21285147

En avril 2022, une cyberattaque a visé le réseau électrique ukrainien. Le logiciel malveillant utilisé ciblait les équipements de contrôle-commande des sous-stations haute tension, avec pour objectif la déconnexion physique de sous-stations électriques alimentant plus de 2 millions de personnes[39]. L'attaque a été déjouée par les défenseurs ukrainiens assistés du service d'intervention numérique d'urgence ukrainien (CERT-UA) et de l'entreprise de cybersécurité ESET. Elle s'inscrit dans une série commencée en 2015[40] et 2016[41], où des cyberattaques du même acteur affilié au GRU russe avaient effectivement provoqué des coupures de courant en Ukraine, établissant la capacité de franchir la frontière entre le domaine du cyber et les flux physiques via le contrôle-commande industriel.

Cette synergie cyber-cinétique a depuis été exploitée de façon continue par l'attaquant. Le CERT-UA indique, au sujet des cyberattaques russes, que « ces attaques sont souvent observées avant les frappes de missiles, ce qui suggère une stratégie de guerre hybride coordonnée ».[42] Des chercheurs en cybersécurité américains établissent explicitement en 2024 que les cyberattaques et les attaques physiques sont dorénavant utilisées conjointement de façon à maximiser leur efficacité respective.[43]

En décembre 2023 l'opérateur de télécommunications ukrainien Kyivstar a été à son tour la cible d'une attaque d'ampleur, visant son infrastructure numérique. L'attaque, orchestrée par une sous-entité du renseignement russe[44], a affecté (selon le groupe revendiquant l'attaque) des milliers de postes de travail et serveurs, les systèmes de stockage cloud ainsi que les sauvegardes prévues pour restaurer les systèmes en cas de panne. L'attaque a perturbé le système d'alertes aériennes dans plus de 80 localités du seul oblast de Kyiv ainsi que dans de larges portions des oblasts de Tcherkassy, Dnipropetrovsk, Kharkiv et Soumy, dont les dispositifs d'alerte dépendaient de l'infrastructure Kyivstar,[45] favorisant la campagne de frappes physiques contre l'Ukraine alors en cours. L'accès mobile et internet de 25 millions de personnes ainsi que de certains terminaux bancaires ont été coupés. Le chef du département cybersécurité du SBU note que les attaquants étaient présents dans le système depuis au moins mai 2023, avec un accès probablement total depuis novembre, ce qui leur a permis de cartographier l'infrastructure et de cibler les systèmes de sauvegarde en même temps que les systèmes principaux.[46]

Le réseau électrique ukrainien constitue un point focal des attaques russes depuis le début de la guerre. La campagne de frappes systématiques sur l'infrastructure énergétique a débuté en octobre 2022, ciblant d'abord le réseau de transmission (sous-stations et lignes de distribution)[47]. Au printemps 2024, un changement tactique a visé directement les centrales de production[48], détruisant ou endommageant gravement environ 9 GW de capacité de génération, soit la moitié de la demande hivernale du pays. En juin 2024, 73 % des unités de production thermique étaient hors service[49]. Les délestages résultants ont dépassé douze heures quotidiennes dans certaines villes[50], propageant la défaillance à l'approvisionnement en eau, au chauffage, aux systèmes sanitaires, à la santé publique et à l'éducation[51]. Ce modèle d'attaque illustre dans un contexte adversarial le même mécanisme documenté dans les cas civils de la section 2.1 : la position de l'électricité comme nœud amont du graphe de dépendances transforme une frappe ciblant un seul secteur en dégradation inter-sectorielle.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

2.2.2 - Cascade inter-sectorielle adversariale hors conflit : Change Healthcare

En février 2024, un groupe criminel a ciblé Change Healthcare, un intermédiaire numérique par lequel transite une part importante des transactions entre les assureurs et les prestataires de santé aux États-Unis[52]. L'entreprise a été contrainte de mettre hors ligne l'ensemble de ses systèmes pendant plusieurs semaines[53].

Les effets se sont propagés au secteur de la santé malgré l'absence de toute atteinte aux infrastructures physiques de soins : les pharmacies ne pouvaient plus vérifier les couvertures d'assurance ni traiter les prescriptions, les hôpitaux ne pouvaient plus soumettre leurs demandes de remboursement. Les cabinets de petite taille ont été proportionnellement les plus affectés, 80 % des répondants à l'enquête de l'AMA déclarant des pertes de revenus plus d'un mois après l'attaque.[54]

Ce cas illustre le même mode de dégradation du secteur de santé que la panne ibérique : des infrastructures de soins physiquement fonctionnelles incapables de remplir leur mission parce qu'une dépendance numérique est rompue. Le nœud défaillant n'est ici ni l'électricité ni les télécommunications mais un intermédiaire transactionnel dont la numérisation a créé le lien de dépendance entre le secteur financier et la délivrance de soins. Ce lien n'existait pas avant la numérisation de la chaîne de facturation. Le fait que l'acteur soit criminel et non étatique confirme que l'exploitation des interdépendances ne requiert ni les ressources, ni l'intention stratégique d'un État : les vecteurs de propagation sont une propriété intrinsèque du substrat numérique, indépendante de la nature de l'attaquant.

3 - Ce qui contient les propagations

Les cas d’étude détaillés dans la section 2 montrent l’existence des boucles et cascades, ainsi que leur activation accidentelle ou intentionnelle par des conditions ou attaques adversariales. Concernant les attaques adversariales spécifiquement, il apparaît que les attaquants disposant de moyens adéquats cartographient les dépendances des systèmes qu’ils ciblent avant de frapper, comme l’illustrent les cas de Kyivstar ou du logiciel M.E.Doc. Les États-Unis ont documenté un cas de positionnement préalable maintenant un accès dormant à un système pendant au moins cinq ans.[55]

Cette connaissance en profondeur des dépendances d’un système potentiellement pris pour cible par l’adversaire soulève un problème conséquent : s’il connaît les dépendances et vulnérabilités, il connaît aussi les mécanismes de contention en place pour mitiger les dépendances et vulnérabilités, ou interrompre la propagation des défaillances à travers ces dépendances. Ces mécanismes eux-mêmes deviennent une cible que les attaquants visent pour maximiser l’effet de leurs actions[56]. Par corollaire, ils deviennent aussi un objet à protéger pour le défenseur.

3.1 - Mécanismes de contention des cascades

Les cas d'étude civils et issus des conflits armés présentés en section 2 permettent d'identifier six mécanismes, dont un transverse, ayant contenu ou interrompu les propagations. Les exemples illustrant ces mécanismes dans la section 3.1 sont concentrés sur l’Ukraine non par choix éditorial

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

mais par un biais de sélection découlant directement de la disponibilité des données, le service d'intervention d'urgence de cyberdéfense ukrainien (CERT-UA) publiant de façon prolifique les attaques subies par le pays. Ces mécanismes de contention se distinguent selon trois axes : leur régime d'utilisation (le mécanisme opère par construction, sans activation ; il repose sur une ressource pré-positionnée dont l'effet requiert une activation ; ou il mobilise *ex post* une capacité non pré-positionnée), leur localisation (la ressource mobilisée est interne au système protégé ou fournie par un tiers), et l'objet qu'ils préservent (la fonction rendue, les données, ou la capacité à activer les autres mécanismes). L'activation d'un mécanisme pré-positionné peut être pilotée par un opérateur ou automatique. La distinction porte sur le délai de réponse et sur l'objet à protéger : une activation automatique supprime la latence de détection et de décision humaines, et transfère la condition d'efficacité du mécanisme vers la couche qui l'exécute. La section 3.2 en traite les conséquences. Le tableau suivant positionne chaque mécanisme sur ces axes et les sous-sections qui suivent les regroupent par mode opératoire.

Mécanisme	Régime d'utilisation	Localisation	Objet préservé
Séparation	Par construction	Interne	La fonction, par absence de lien de propagation
Architecture en mode dégradé	Par construction	Interne	Une fonction partielle
Redondance locale	Pré-positionné, activation requise	Interne, sur site	La fonction, pour une durée bornée
Réplication	Pré-positionné, activation requise	Externe le plus souvent	Les données et l'état du système
Substitution	Mobilisation *ex post*	Externe	La fonction, via une infrastructure tierce
Compétence	Transverse	Organisationnelle	La capacité d'activation des cinq autres

3.1.1 - Mécanismes de contention intégrés à la conception

La séparation et l'architecture en mode dégradé opèrent par construction : elles ne requièrent aucune activation au moment de l'incident, et leur coût est entièrement supporté en amont.

Deux systèmes séparés n'ont, par définition, aucun lien par lequel la défaillance de l'un pourrait se propager à l'autre. Le réseau de communications des forces armées ukrainiennes est resté fonctionnel pendant l'attaque contre Kyivstar de décembre 2023, parce qu'il repose sur des protocoles et une infrastructure distincts de l'opérateur civil attaqué.[57] De même, le rapport final du panel d'experts ENTSO-E sur la panne ibérique recommande que les communications vocales entre acteurs clés et les fonctions critiques de contrôle à distance restent opérationnelles lorsque les réseaux de télécommunications publics sont hors service[58], ce qui revient à prescrire une séparation architecturale entre les communications de pilotage du réseau électrique et le réseau public.

L'architecture en mode dégradé prévoit, dès la conception, un fonctionnement restreint mais opérationnel lorsque les dépendances du système (connectivité, électricité) sont interrompues. Le

DOI: https://doi.org/10.5281/zenodo.21285147

service ukrainien de gestion de documents d'identité Diia en offre un exemple partiel : le stockage local des documents permet un usage sans connectivité, bien que la vérification et les services transactionnels restent dépendants du réseau.[59] La distinction avec la séparation tient à l'objet : la séparation supprime le lien de dépendance tandis que l'architecture dégradée conserve le lien mais borne les conséquences de sa rupture.

3.1.2 - Capacités pré-positionnées

La redondance locale et la réplication reposent sur des ressources déployées avant l'incident mais dont l'effet ne se matérialise qu'à l'activation. Une variable critique commune aux mécanismes de contention mobilisant une ressource bornée est le dimensionnement : temporel pour la redondance, périmètre de couverture pour la réplication. Le dimensionnement temporel fait l'objet de la section 3.2.2.

La redondance locale est une capacité de secours physiquement disponible sur site, permettant de maintenir une fonction pendant une durée limitée sans dépendance au réseau. L'Ukraine y a alloué des moyens conséquents pour donner à son réseau de télécommunications une résilience aux coupures électriques, avec plus de 4 000 générateurs et 230 000 batteries déployés aux tours de télécommunication des opérateurs Lifecell-Datagroup-Volia[60] et Kyivstar[61]. Les générateurs de secours des hôpitaux ibériques relèvent du même mécanisme bien que leur dimensionnement se soit révélé insuffisant face à la durée de la panne.

La réplication consiste en la copie de données ou de systèmes vers un environnement alternatif, de sorte que la destruction de l'original ne détruit pas la fonction. La migration d'urgence des registres d'État ukrainiens vers le cloud en constitue l'exemple le plus documenté : 161 registres nationaux et environ 15 pétaoctets de données gouvernementales ont été répliqués hors du territoire à partir de février 2022.[62] PrivatBank, première banque du pays, a migré l'ensemble de ses opérations en moins de 45 jours.[63]

La réplication n'implique pas nécessairement une opération de bascule ultérieure. Les architectures distribuées maintiennent un service simultanément sur plusieurs sites, de sorte que la perte d'un nœud laisse la fonction disponible sans action d'un opérateur au moment de l'incident. Ce mode de fonctionnement est natif chez les grands fournisseurs de cloud, et il est également mis en œuvre en dehors d'eux, sur des logiciels ouverts déployés sur du matériel hétérogène et géographiquement dispersé.[64]

Lorsque la bascule est pilotée par un opérateur, le mécanisme dépend de la détection, de la décision et de l'exécution, dont la latence s'ajoute à la fenêtre de propagation. Lorsqu'elle est automatique, le mécanisme dépend de la couche qui détecte la défaillance et réachemine le trafic, laquelle devient à part entière un composant du mécanisme de contention. Dans les deux cas, la redondance n'est pas une propriété acquise sans conception : elle suppose un dimensionnement de la capacité survivante et une configuration dont la conformité au comportement attendu a été vérifiée et testée. Un déploiement présumé répliqué mais configuré au sein d'une seule zone de disponibilité, ou d'un seul site physique, offre l'apparence du mécanisme sans ses propriétés.[65]

DOI: https://doi.org/10.5281/zenodo.21285147

3.1.3 - Bascule vers une infrastructure tierce

La substitution consiste en la bascule d'un service vers une infrastructure alternative après la défaillance. Ce mécanisme activé *ex post* est le plus susceptible d'être externalisé vers une entité tierce, ce qui en fait le mécanisme le plus exposé aux risques de maîtrise traités en section 3.2.3.

Le déploiement de Starlink après la neutralisation de Viasat le 24 février 2022 en est l'illustration principale : bien que représentant une faible part du trafic internet ukrainien[66], le réseau a fourni une capacité de remplacement rapidement mobilisable en situation de crise. Le partage d'infrastructure entre opérateurs concurrents après l'attaque contre Kyivstar (Vodafone Ukraine, Lifecell) relève du même mécanisme, dans une configuration où le tiers est un pair national plutôt qu'un fournisseur étranger.

3.1.4 - La compétence conditionne l'utilité des mécanismes de contention

La compétence est de nature différente des cinq mécanismes précédents : elle n'interrompt pas une propagation par elle-même, mais détermine si les capacités pré-positionnées sont activées à temps, si la bascule vers un tiers est exécutée correctement, et si le dimensionnement de l'ensemble correspond aux besoins réels. Elle conditionne l'efficacité des mécanismes des sections 3.1.1 à 3.1.3 sans s'y substituer. L'expérience acquise par les services ukrainiens lors des attaques contre leur réseau électrique en 2015 et 2016 a permis la réponse qui a déjoué l'attaque d'avril 2022.[67] Ses modes de défaillance propres, non-acquisition et érosion, sont traités en section 3.2.3.

3.2 - Les mécanismes de contention sont eux-mêmes vulnérables

Comme évoqué dans l'introduction de la section 3, les mécanismes de contention des propagations des défaillances ne sont pas exempts d'être eux-mêmes défaillants, pour des raisons intentionnelles, accidentelles, ou de négligence. Ces mécanismes font partie intégrante du système concerné du point de vue de sa capacité à maintenir ou rétablir son fonctionnement, et ils doivent donc être soumis eux aussi à des critères de résilience.

3.2.1 - Les mécanismes peuvent être ciblés et dégradés

Lors de la campagne contre les opérateurs de télécommunications ukrainiens, le CERT-UA évoque un ciblage des sauvegardes de l'entreprise Kyivstar, dans le but explicite de rendre la récupération plus difficile. Le mécanisme de réplication a ici été ciblé en tant que tel.

Toujours dans le cas Kyivstar, la destruction du système d'enregistrement client a empêché la bascule des abonnés vers les opérateurs concurrents via l'itinérance nationale.[68] Le mécanisme de substitution n'a pas fonctionné parce que le système dont il dépendait a été détruit.

Lors de la panne nord-américaine de 2003, le système d'alarme logiciel (faisant partie du mécanisme de contention) du centre de contrôle de l'opérateur est tombé en panne silencieusement. Le mécanisme dont la fonction est précisément de détecter la dégradation du réseau et de signaler

DOI: https://doi.org/10.5281/zenodo.21285147

l'urgence a été le premier point de défaillance, et il a échoué sans se signaler. Les opérateurs ont continué à travailler en croyant observer un réseau stable alors que la cascade se propageait.

Lors de la panne italienne de 2003, le mécanisme de restauration du réseau électrique (communication via internet pour piloter la reconnexion) dépendait du réseau dont la restauration était l'objectif. La boucle de rétroaction couplant énergie et internet a empêché les deux réseaux de se rétablir mutuellement.

L'activation automatique déplace cette exposition sans la supprimer. La couche de détection et d'orchestration qui déclenche la bascule conditionne l'efficacité du mécanisme qu'elle opère : sa propre défaillance, silencieuse ou non, laisse des ressources redondantes disponibles et inutilisées. La défaillance silencieuse du système d'alarme de FirstEnergy en 2003 illustre ce mode sur un mécanisme dont la fonction était la détection. Lorsque cette couche est partagée par plusieurs services, sa défaillance les dégrade simultanément, ce qui est le motif de divergence décrit en section 1 appliqué au mécanisme de contention lui-même. Un mécanisme de contention est lui-même un nœud du graphe de dépendances, en ce sens qu'il porte ses propres dépendances et hérite des exigences de résilience de la fonction qu'il préserve.

3.2.2 - Le dimensionnement temporel des mécanismes de contention

Une vulnérabilité transverse à tous les mécanismes de contention mobilisant une ressource bornée est celle de leur portée temporelle. Les générateurs hospitaliers ibériques ont échoué parce qu'ils avaient une capacité de quelques heures et ont dû faire face à une panne de plus de 10 heures.[69] Un mécanisme de contention dont l'autonomie est inférieure à la durée de la perturbation ne fait que retarder la cascade, et la durée de perturbation étant *a priori* inconnue avant l'évènement déclencheur, le dimensionnement de chaque capacité d'autonomie mérite une attention particulière. La distinction conceptuelle entre interrompre une cascade et la retarder est évidente mais ses conséquences sont non-triviales : le dimensionnement de l'autonomie temporelle qu'un mécanisme de contention de cascade (générateur de secours, batterie, stock de nourriture, d'eau ou de médicaments, etc) permet doit être calculé en fonction des besoins des services dépendants, ce qui implique une cartographie précise de ces services et de leurs besoins.

Par exemple, l'autonomie d'un générateur dont dépendent un stock réfrigéré et des appareils vitaux se mesure contre le délai de réapprovisionnement en conditions dégradées.

3.2.3 - La maîtrise des mécanismes de contention

Les mécanismes de contention présentent des risques liés à leur maîtrise. En particulier, deux volets de cette maîtrise peuvent remettre en cause leur utilité opérationnelle : la souveraineté et la compétence.

Souveraineté. Un mécanisme de contention détenu et opéré par l'acteur qui en dépend présente des risques (pannes, sous-dimensionnement, erreur de conception), tous mitigeables par son détenteur. Lorsque le mécanisme appartient à un tiers, sa disponibilité, son périmètre d'emploi et ses

DOI: https://doi.org/10.5281/zenodo.21285147

conditions d'accès sont décidés par un acteur dont la coopération est révocable, comme l'a rapporté Reuters dans le cas du service Starlink fourni à l'Ukraine[70], tarifiable, conditionnée[71] ou instrumentalisée[72]. La position juridictionnelle de ce tiers module ce risque. En effet, un service fourni par un tiers relevant de la juridiction de l'acteur dépendant reste révocable en intention, mais demeure théoriquement contraignable par des dispositifs légaux tels que les obligations de service ou la réquisition[73], au prix d'un délai et d'une incertitude d'exécution qui relèvent des mêmes exigences de dimensionnement temporel que les autres mécanismes (section 3.2.2). Un fournisseur de service tiers situé hors de cette juridiction n'est accessible que par des leviers contractuels ou diplomatiques.[74] Le partage d'infrastructure entre opérateurs ukrainiens après l'attaque contre Kyivstar et la substitution par Starlink après la neutralisation de Viasat illustrent ces deux positions (section 3.1.3). Cette distinction ne remet pas en cause l'utilité d'un mécanisme tiers, mais elle en caractérise la disponibilité (contraignable dans un cas, négociable dans l'autre, et sans garantie dans les deux cas).

Le degré d’autonomie permis par une capacité donnée est intrinsèquement lié au degré de souveraineté de cette capacité. Cette souveraineté est un spectre continu et mouvant, nécessitant une analyse proportionnée à la criticité de la capacité ou du mécanisme de contention.[75]

Compétence. La capacité organisationnelle à activer les mécanismes de contention dans les conditions réelles d'un incident conditionne leur efficacité au même titre que leur existence. Un mécanisme présent mais activé trop tard, mal dimensionné ou jamais éprouvé produit un résultat proche de celui d'un mécanisme absent.

Cette capacité échoue par deux voies. La non-acquisition, d'abord, lorsque l'organisation n'a jamais confronté le scénario : aucune région concernée par la panne ibérique ne disposait d'un plan de continuité pour une panne électrique prolongée affectant les services médicaux d'urgence. Bien que les générateurs existaient, leur articulation avec les besoins des services dépendants n'avait jamais été éprouvée.

L'érosion, ensuite, lorsque la compétence organisationnelle se dégrade faute de pratique. La compétence est un actif périssable. La littérature sur l'apprentissage organisationnel documente depuis longtemps la dépréciation du savoir acquis en l'absence de pratique : à partir des données de production des chantiers navals américains de la Seconde Guerre mondiale, Argote, Beckman et Epple montrent que le savoir organisationnel se déprécie rapidement lorsque l'activité s'interrompt.[76] Ce résultat a été répliqué dans d'autres contextes organisationnels.[77] Au niveau individuel, la méta-analyse d'Arthur et al. établit que les compétences non exercées décroissent et que cette décroissance s'accentue avec la durée de non-utilisation. La récurrence obligatoire des exercices dans les dispositifs nationaux de préparation repose sur ce constat.[78] Cette observation est analytiquement distincte de la souveraineté : un mécanisme peut être souverain mais inopérant faute de compétence entretenue pour l'activer.

Le contraste empirique est net. Les exercices nationaux de préparation conduits par l'Ukraine en 2021 ont couvert une part significative des scénarios matérialisés en février 2022[79], et l'expérience des attaques de 2015-2016 contre le réseau électrique a permis la réponse qui a déjoué l'attaque d'avril 2022. La compétence y a été construite puis entretenue par la confrontation répétée.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

L'implication évaluative est directe : un exercice qui ne soumet pas l'activation des mécanismes de contention aux conditions du scénario mesure l'existence de ces mécanismes, sans mesurer la capacité à les opérer. Ce critère est repris en section 4.3.

Les considérations de maîtrise développées ici s'appliquent à tout nœud du graphe de dépendances. La présente note les traite là où leur défaillance est sans recours : les mécanismes de contention constituent la dernière ligne d'interruption d'une cascade, et leur indisponibilité laisse la propagation sans obstacle. L'analyse de la maîtrise des nœuds amont eux-mêmes relève de la cartographie des dépendances.[80]

3.2.4 - Coût observé de la réponse non planifiée

Les cas documentés dans cette note permettent d'observer partiellement le coût de mécanismes de contention déployés en urgence, après le déclenchement d'une dégradation, par opposition aux capacités pré-positionnées décrites en section 3.1.

A titre d’exemple, l'attaque contre Kyivstar a représenté un impact financier estimé à 3,6 milliards de hryvnias (environ 90 millions de dollars), sur les revenus 2024 de l'opérateur, couvrant les mesures de fidélisation, la gratuité temporaire du service et les réparations.[81] En regard, Kyivstar a investi 1,9 milliard de hryvnias (environ 47,5 millions de dollars) sur deux ans dans le renforcement pré-positionné de la redondance électrique de son réseau.

Ces chiffres visent à fournir un ordre de grandeur indicatif, mais leur citation appelle à trois précautions méthodologiques. Premièrement, le coût de l’installation de cette capacité de redondance électrique n’est pas à comparer directement avec l’impact financier de l’attaque contre Kyivstar, mais contre la part de cet impact que la redondance aurait permis d’éviter, ce qui est probablement irréalisable et contrefactuel, l’absence préalable de cette redondance ayant probablement orienté les choix de l’attaquant. Deuxièmement, l'impact financier de l'attaque ne se limite pas aux seuls revenus de l'entreprise mais s'étend aux activités qui dépendaient de son infrastructure. Enfin, un calcul honnête du coût de la planification devrait intégrer l'ensemble des dispositifs de résilience financés qui ne sont jamais activés. L'arbitrage entre le coût du pré-positionnement et celui de la réponse d'urgence relève d'un calcul de dimensionnement sous incertitude qui dépasse le périmètre de la présente note, comme l’explicite la troisième question identifiée en section 4.4.

3.2.5 - Résumé des enseignements empiriques sur les mécanismes de contention

Les données empiriques réunies dans cette section indiquent que les mécanismes de contention des cascades constituent eux-mêmes des surfaces de vulnérabilité, selon quatre modes distincts. Ils peuvent être ciblés délibérément, comme les sauvegardes de Kyivstar, ou défaillir silencieusement, comme le système d'alarme de FirstEnergy. Leur dimensionnement temporel peut être inférieur à la durée de la perturbation, auquel cas ils retardent la cascade sans l'interrompre. Leur disponibilité peut dépendre d'un tiers dont la coopération est révocable. Enfin, la compétence organisationnelle nécessaire à leur activation peut faire défaut, par non-acquisition ou par érosion.

DOI: https://doi.org/10.5281/zenodo.21285147

Ces quatre modes de défaillance ont une conséquence commune : l'existence d'un mécanisme de contention ne renseigne pas sur son efficacité dans les conditions réelles d'un incident. Un inventaire des mécanismes déployés, aussi complet soit-il, ne mesure ni leur résistance à un ciblage, ni leur autonomie face à une perturbation de durée inconnue, ni les conditions de leur disponibilité, ni la capacité de l'organisation à les activer. Évaluer la résilience d'un système impose donc de soumettre ses mécanismes de contention au même régime d'épreuve que le système lui-même. La section 4 traduit cette exigence en critères d'évaluation.

4 - Conclusions analytiques et cadre évaluatif

4.1 - Ce que les données empiriques révèlent

Les propagations inter-sectorielles documentées dans cette note présentent un caractère récurrent et des motifs qui permettent d'en tirer des enseignements généralisables. Les causes du blackout ibérique de 2025 sont similaires à celles d'un incident survenu dans le sud-est de l'Europe en 2024. La boucle de rétroaction entre électricité et gaz observée au Texas en 2021 est comparable à la boucle entre électricité et internet observée en Italie en 2003. Les cascades par dépendance numérique partagée (M.E.Doc en 2017, Change Healthcare en 2024) frappent des secteurs physiquement indépendants via le même vecteur : c'est le motif de divergence opérant hors de tout couplage physique. Ces propagations surviennent quelle que soit la nature du déclencheur (accident météorologique, défaillance interne, attaque criminelle ou opération étatique). Cette récurrence a une cause identifiable. Les quatre motifs décrits en section 1 existaient avant la numérisation partout où un couplage physique liait deux secteurs, comme entre le gaz et l'électricité au Texas. Ce que le substrat numérique a changé est l'étendue du graphe qui les porte : la numérisation a créé des chemins de propagation entre des secteurs qui n'en partageaient aucun, et les cascades M.E.Doc et Change Healthcare ont emprunté des liens qui n'existaient pas dix ans avant leur activation. Les motifs de propagation sont anciens mais la topologie qui les généralise est récente, et elle continue de s'étendre.

L'adoption massive de l'IA, mentionnée en introduction, prolonge cette dynamique de formation du graphe : la concentration des modèles et des capacités d'inférence chez un petit nombre de fournisseurs installe un nouveau nœud amont dont la criticité croît avec l'intégration de ces services dans les processus opérationnels des secteurs aval. Aucune cascade inter-sectorielle majeure imputable à ce nœud n'est publiquement documentée à ce jour, cependant sa position est identique à celle des intermédiaires numériques partagés dont la défaillance a produit les cascades décrites en sections 2.2.1 et 2.2.2 : c'est un chemin de propagation commun entre des secteurs physiquement indépendants. Le mécanisme de désignation décrit en section 4.2, qui identifie un prestataire dont la défaillance serait systémique et dont la substitution serait difficile, constitue la réponse existante la plus proche de cette position, et il ne s'applique qu'à un seul secteur. Le rythme de cette extension est un paramètre en soi : entre l'adoption d'un cadre réglementaire et son entrée en application s'écoulent plusieurs années, quand l'intégration d'un nouvel intermédiaire numérique dans les processus opérationnels de secteurs entiers se mesure en mois. Le graphe se reconfigure plus vite que les instruments conçus pour l'évaluer.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

Les mécanismes de contention documentés en section 3, qu'ils soient intégrés à la conception (séparation, architecture en mode dégradé), pré-positionnés (redondance locale, réplication) ou fondés sur la bascule vers un tiers (substitution), ont fonctionné dans les cas étudiés. Ces mêmes cas montrent cependant que ces mécanismes constituent eux-mêmes des surfaces de vulnérabilité, selon les quatre modes identifiés en section 3.2 : ciblage délibéré ou défaillance silencieuse (destruction des sauvegardes des opérateurs télécom ukrainiens, panne muette du système d'alarme de FirstEnergy en 2003), sous-dimensionnement temporel (générateurs hospitaliers ibériques), dépendance à un tiers dont la coopération est révocable (limitations rapportées du service Starlink fourni à l'Ukraine), et défaut de compétence organisationnelle, par non-acquisition ou par érosion. La question de la maîtrise de ces mécanismes est analytiquement distincte de la question de leur existence.

La modélisation des infrastructures en graphe de dépendances avec nœuds de convergence, plutôt qu'en chaînes sectorielles indépendantes, change la nature de l'analyse de résilience. Dans ce graphe, un nœud amont hérite des exigences de résilience de l'ensemble des services aval qui dépendent de lui : l'allocation des investissements suit le graphe, non la classification sectorielle. Le corollaire est que toute fonction située sur le chemin critique de restauration d'une fonction vitale hérite des exigences de résilience de cette fonction, indépendamment de sa classification sectorielle propre. Le cas texan illustre concrètement ce principe : les infrastructures gazières n'avaient pas été identifiées par l'opérateur du réseau électrique comme charges critiques à maintenir en priorité lors des délestages, alors qu'elles alimentaient les centrales dont dépendait la restauration de la production. Le délestage des infrastructures gazières a aggravé la panne qu'il visait à contenir.

4.2 - Projection sur les cadres régulatoires existants

La partition de ces cadres reproduit la topologie qui précédait l'unification numérique : des systèmes coexistants, couplés en des points identifiables, dont la résilience pouvait s'évaluer secteur par secteur. Le décalage documenté dans cette section est un décalage de topologie. Les instruments évaluent des entités et des secteurs, quand la propagation opère sur un graphe dont les arêtes traversent leurs périmètres.

Les cadres CER et NIS2 couvrent individuellement la résilience physique et la cybersécurité des entités critiques avec un degré de granularité significatif : analyse de risques, plans de résilience, notification d'incidents, sécurité de la chaîne d'approvisionnement. CER impose aux entités critiques de prendre en compte leurs dépendances vis-à-vis d'autres secteurs dans leurs évaluations de risques. NIS2 ouvre la possibilité pour les États membres de désigner comme entité essentielle une entité ayant une importance spécifique pour d'autres secteurs interdépendants (article 2(2)(e)), ce qui autorise la constitution de chaînes de dépendances critiques au sein de son périmètre.

En revanche, CER exclut explicitement de son périmètre les matières couvertes par NIS2 (article 1(2)) et prescrit leur coordination par un article de principe dont la mise en œuvre est laissée à chaque État membre. La classification reste sectorielle et l'évaluation s'effectue au niveau de l'entité, sans considération du graphe de dépendances. Le mécanisme de désignation inter-sectorielle de NIS2 est discrétionnaire et ne repose sur aucune cartographie systématique.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

La même limite affecte les dispositions relatives à la chaîne d'approvisionnement. L'article 21(2)(d) de NIS2 impose aux entités de traiter les aspects de sécurité de leurs relations avec leurs fournisseurs directs et prestataires de services, et l'article 21(3) leur enjoint de prendre en compte les vulnérabilités propres à chacun de ces fournisseurs ainsi que la qualité globale de leurs pratiques[82]. L'obligation affecte chaque lien bilatéral et se trouve pleinement satisfaite par une entité qui a évalué chacun des fournisseurs avec lesquels elle contracte. Cependant, rien n'y impose à quiconque de constater qu'un grand nombre d'entités, réparties dans des secteurs sans rapport entre eux, dépendent du même fournisseur. L'article 22 ouvre le seul étage systémique, en permettant au groupe de coopération, avec la Commission et l'ENISA, de conduire des évaluations coordonnées des risques des chaînes d'approvisionnement critiques en TIC. Cet étage est une faculté et non une obligation, il porte sur des catégories de services, systèmes ou produits identifiées par la Commission, et il ne s'accompagne d'aucun pouvoir de supervision sur les fournisseurs examinés. La concentration sur un nœud partagé est ainsi un objet dont aucune de ces dispositions ne confie l'observation à un acteur.

La projection de chaque cas d'étude documenté dans cette note contre les cadres règlementaires rend visible des scénarios de défaillance qui tombent dans l'interstice entre les périmètres respectifs de ces cadres.

Lors de la panne électrique ibérique, la défaillance physique du réseau de transport relève du périmètre de CER. Les systèmes d'information des opérateurs de réseau relèvent de NIS2. La cascade par laquelle la perte simultanée de l'électricité et des télécommunications a privé les services d'urgence de leurs outils de coordination, dégradé l'accès aux stations-service et aux feux de signalisation, et propagé les effets jusqu'aux services hospitaliers via les dossiers numériques, échappe en tant que phénomène de propagation inter-sectorielle au périmètre de ces deux instruments. Chaque secteur aval relève individuellement de l'un ou de l'autre ; la cascade elle-même tombe dans l'interstice.

Le cas texan présente la même caractéristique. Les infrastructures gazières n'avaient pas été identifiées comme charges critiques lors des plans de délestage. La résilience sectorielle de chaque réseau pris isolément était traitée mais la cartographie inter-sectorielle des dépendances faisait défaut, et les entités responsables du secteur électrique ne disposaient d'aucune visibilité sur les dépendances gazières dont leur propre restauration dépendait.

Les attaques cyber-cinétiques les plus marquantes contre le réseau électrique ukrainien (2015, 2016, 2022) illustrent le cas le plus net : une attaque cyber relevant du périmètre NIS2 et produisant une défaillance physique relevant du périmètre CER, le couplage entre les deux étant le mécanisme même de l'attaque. La coordination entre les deux cadres est prescrite par des dispositions de principe dans chacun des deux cadres mais n'est testée en tant que vecteur de propagation dans aucun exercice documenté publiquement, à la connaissance de l’auteur.

Les cascades M.E.Doc et Change Healthcare exposent un troisième type d'interstice. Dans les deux cas, le nœud défaillant est un intermédiaire numérique partagé par des entités qui n'ont aucun autre lien entre elles : dans un cas un logiciel de comptabilité utilisé dans l'ensemble du tissu économique ukrainien en 2017, dans l’autre un service de compensation des transactions utilisé dans l'ensemble

DOI: https://doi.org/10.5281/zenodo.21285147

du système de santé américain en 2024. Chaque entité aval entretenait une relation bilatérale avec cet intermédiaire, et les dispositions relatives à la chaîne d'approvisionnement décrites plus haut portent précisément sur cette relation. Ce qui a produit la cascade est le nombre de ces relations convergeant vers un même nœud, propriété qui n'est visible depuis la position d'aucune entité prise isolément et qui ne relève d'aucun secteur en particulier.

Le droit de l'Union comporte pourtant un mécanisme conçu pour cette propriété. Les articles 31 à 44 de DORA permettent aux autorités européennes de surveillance de désigner un prestataire tiers de services TIC comme critique pour le secteur financier, de lui affecter un superviseur principal et d'exercer directement sur lui des pouvoirs d'information, d'enquête et d'inspection, alors même qu'il n'est pas lui-même une entité régulée[83]. Les critères de désignation incluent l'impact systémique d'une défaillance du prestataire et son caractère substituable, ce qui constitue un test de concentration conduit à l'échelle de l'Union. La première liste de prestataires désignés a été publiée en 2025. Le modèle de supervision existe donc et fonctionne. Son périmètre est le secteur financier, et la position qu'occupait Change Healthcare dans la chaîne de facturation du système de santé américain ne dispose d'aucun mécanisme de désignation équivalent dans un autre secteur, dans l'Union comme ailleurs. La cascade a franchi une frontière que les instruments tracent entre secteurs, à un nœud dont la criticité n’est pas intrinsèque mais tient au nombre de secteurs qu'il dessert.

Les instruments nationaux présentent la même partition. En France, la directive générale interministérielle 320 du 23 janvier 2023, qui fixe le cadre de la planification de défense et de sécurité nationale entre ministères, propose une lecture de cette transversalité avec une matrice croisant facteurs de crise majeure et activités-clés constituant les centres de gravité de la Nation. Sa section « Stratégie de réponse » prévoit toutefois que la mise en œuvre de chaque levier relève du seul ministère de tutelle[84]. La transversalité est présente dans la matrice d'analyse et absente de la partie prescriptive de la directive, qui reste sectorielle et cloisonnée. Cette illustration nationale (un exemple parmi vingt-sept), met en lumière le fait qu’un cadrage par fonctions vitales peut coexister avec une exécution cadrée par secteur, bien que la transversalité reste ici incomplète.

Au-dessus de cette couche réglementaire, la reconnaissance politique du phénomène est désormais acquise au niveau européen. Le rapport Niinistö recommande une approche de préparation globale inspirée des modèles nordiques et identifie explicitement les crises en cascade : il propose la transformation du Centre de coordination de la réaction d'urgence (ERCC) en un centre de crise transversal servant de point d'entrée unique pour les crises majeures transfrontalières et en cascade, ainsi qu'une meilleure articulation entre niveaux politique et technique via les arrangements IPCR. La stratégie d'Union de la préparation reprend ces orientations en trente actions, dont la conduite régulière d'exercices de préparation complets à l'échelle de l'Union. Ces textes établissent au niveau politique le constat que documente la présente note, jusqu'à nommer les cascades comme objet de coordination. Le traitement proposé porte toutefois sur la réponse : le centre de crise envisagé coordonne la gestion d'une cascade en cours, et les exercices annoncés visent la prise de décision et la coordination. Aucune méthodologie publique ne définit à ce jour à la connaissance de l’auteur les critères permettant de tester ex ante la propagation inter-sectorielle, ses boucles de rétroaction ou la neutralisation des mécanismes de contention. Cette absence d'outillage contraste avec la maturité de

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

la recherche : la modélisation et la simulation des infrastructures interdépendantes constituent un champ établi, dont la revue de référence distinguait dès 2014 six familles d'approches.[85] Le savoir analytique existe mais son transfert vers les cadres et les exercices en tant qu'objet d'évaluation reste à opérer. L'écart entre reconnaissance et traitement, documenté en introduction pour les exercices techniques, se retrouve ainsi au niveau politique sous une forme précise : la cascade y est constituée en objet de gestion de crise, pas encore en objet d'évaluation. Les critères proposés en section 4.3 se situent dans cet interstice.

La lecture des dépendances proposée dans la présente note ne prétend donc pas se substituer aux cadres existants sur leur périmètre propre. Son apport recherché est de rendre visible ce qu'aucun d'entre eux ne prend pour objet, c’est à dire le mécanisme de propagation inter-sectorielle lui-même. L'écart entre la topologie que ces cadres présupposent et celle que documentent les cas étudiés croît avec chaque fonction nouvellement numérisée.

4.3 - Critères d'évaluation dérivés des cas documentés

L'anatomie des propagations décrite dans cette note permet de formuler des questions auxquelles un exercice de *stress testing* inter-sectoriel devrait pouvoir répondre. Ces questions dérivent des modes de défaillance identifiés dans les cas étudiés dans la présente note et de leur propagation à travers le graphe de dépendances décrit en section 1. Ces critères sont prescriptifs. Chacun affirme qu'un exercice ou un plan de résilience gagne à le satisfaire, et chaque affirmation repose sur un cas documenté dans lequel l'absence de la propriété a contribué à une cascade ou à la défaillance d'un mécanisme de contention. Deux limites en découlent. La présente note ne propose aucune modification des instruments réglementaires examinés en section 4.2, l'appréciation de leur suffisance supposant un accès à leur application. Et elle ne traduit pas ces critères en conception d'exercice, les exercices concernés n'étant pour une large part pas documentés publiquement. Ce qu'elle fait est expliciter ce qu'implique chaque critère, de sorte qu'un lecteur disposant de cette documentation puisse déterminer si la condition est déjà remplie. La formulation des réponses lui appartient.

Critères portant sur le scénario :

- Le scénario teste-t-il la propagation causale entre au moins deux secteurs interdépendants, plutôt que chaque secteur isolément ? Ce qu'il faut vérifier est si le second secteur défaille parce que le premier a défailli, ou parce que le scénario l'a décrété. Au Texas en 2021, les délestages ont coupé l'alimentation des installations gazières qui approvisionnaient les centrales, ce qui a aggravé les délestages. Un scénario qui déclare le gaz et l'électricité hors service à l'heure zéro éprouve la réponse à une double panne et laisse la boucle qui l'a produite hors du champ d'évaluation.
- Le scénario couvre-t-il la convergence de plusieurs nœuds amont défaillants vers les mêmes services aval ? Ce qu'il faut vérifier est, pour chaque solution de repli dont dispose le service aval, si ses propres dépendances figurent parmi les nœuds que le scénario a déjà mis hors service. Les services d'urgence ibériques ont perdu leurs outils de coordination et les télécommunications qui les portaient sous l'effet d'une même défaillance amont.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

- Le scénario intègre-t-il la dimension temporelle des cascades, c'est-à-dire la vitesse de propagation, la fenêtre d'intervention disponible et la durée au-delà de laquelle la dégradation devient difficilement réversible ? La durée d'une panne n'est pas connaissable tant qu'elle dure, ce qui la rend inutilisable comme cible de dimensionnement d'une réserve bornée. La grandeur mesurable est le délai de réapprovisionnement dans les conditions de la crise. Pour un générateur hospitalier ibérique, c'est le délai de décision, prise par des responsables qui peuvent être empêchés de se réunir, sur une information incomplète et face à des priorités concurrentes, puis le délai d'exécution d'une livraison de carburant avec une signalisation éteinte, une circulation désorganisée et des stations-service dont le paiement par carte dépend des télécommunications hors service. Une réserve est dimensionnée lorsque son autonomie excède ce délai.
- Le scénario inclut-il une « défaillance aggravante », une condition initiale dégradée dans laquelle un secteur est déjà affaibli lorsque le déclencheur survient ? Ce qu'il faut vérifier est que la dégradation préalable soit indépendante du déclencheur, une condition produite par le déclencheur lui-même n'étant qu'une phase du même évènement, et qu'elle porte sur la capacité de réponse et pas seulement sur l'infrastructure. Le CERT-UA rapporte des cyberattaques observées en amont des frappes de missiles : quand les frappes arrivent, les systèmes d'alerte et les équipes sont déjà dégradés.
- Le scénario teste-t-il la propagation au-delà du périmètre national ou juridictionnel de l'entité évaluée ? Ce qu'il faut vérifier est le sens de la propagation. Un évènement étranger qui atteint l'entité évaluée est communément simulé mais l'entité évaluée comme vecteur vers d'autres juridictions est un cas de figure rarement éprouvé. L'attaque Viasat visait un opérateur desservant l'Ukraine et a laissé 5 800 éoliennes allemandes sans supervision, ainsi que des accès résidentiels dans cinq autres pays européens.

Critères portant sur les mécanismes de contention :

- Les mécanismes identifiés en section 3.1 (séparation, architecture en mode dégradé, redondance locale, réplication, substitution) sont-ils eux-mêmes soumis au stress du scénario ? Ce qu'il faut vérifier est si l'exercice exige un résultat ou accepte une déclaration. Dans le cas cité en section 3.1.2, des sauvegardes vendues comme physiquement isolées se trouvaient dans le même bâtiment que le serveur qu'elles protégeaient, l'isolement étant présumé du contrat jusqu'à ce qu'un incendie le démente.
- Le scénario prévoit-il la neutralisation du mécanisme de contention lui-même, comme la destruction du système de sauvegarde, la défaillance silencieuse du système d'alarme, ou la boucle de rétroaction empêchant la restauration ? Le ciblage, le sous-dimensionnement et l'indisponibilité d'un tiers peuvent être injectés en cours d'exercice. La défaillance silencieuse doit être prévue à la conception, puisqu'il faut présenter aux participants une lecture fausse mais plausible plutôt qu'un instrument qui s'arrête. En 2003, les opérateurs de FirstEnergy ont observé un réseau stable pendant plus d'une heure alors que les lignes de transmission tombaient successivement.
- Le mécanisme de contention dépend-il d'un acteur dont la coopération est révocable, et si c'est le cas, cet acteur relève-t-il d'une juridiction permettant de contraindre cette coopération

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

? Lorsque la coopération est contraignable, la voie juridique comporte un délai, qui se mesure contre le même intervalle que le critère de dimensionnement temporel ci-dessus. Ce qu'il faut vérifier est si ce délai a été mesuré ou supposé. Le partage d'infrastructure entre opérateurs ukrainiens après l'attaque contre Kyivstar et la substitution par Starlink après Viasat illustrent les deux positions.

- L'organisation a-t-elle démontré, dans les conditions du scénario, la capacité à activer le mécanisme de contention ? Deux éléments sont observables sans historique d'incident : si l'exercice se conduit avec les outils que le scénario laisse disponibles, et si la personne qui active le mécanisme est celle qui serait effectivement joignable plutôt que le titulaire désigné de la fonction. Aucune région ibérique ne disposait d'un plan de continuité pour une panne prolongée affectant les services médicaux d'urgence : les générateurs existaient, et ce qui n'avait jamais été éprouvé était l'adéquation de leur autonomie aux besoins des services qui en dépendaient. Ce qu'un tel exercice mesure est la préparation, et la question de ce à quoi ressemble un test de compétence en conditions réalistes dans une organisation sans historique d'incident reste ouverte.
- L'activation du mécanisme dépend-elle d'une couche de détection ou d'orchestration, et cette couche est-elle incluse dans le périmètre du scénario ? Ce qu'il faut vérifier est une liste des mécanismes couverts et de ce qui déclenche chacun d'eux : tout déclencheur apparaissant deux fois est une dépendance partagée qu'aucune cartographie ne déclare. Une bascule automatique qui dépend d'un système de supervision tombe avec lui et laisse la capacité redondante disponible et inutilisée.

4.4 - Questions ouvertes

L'empirie et le cadre évaluatif de cette note font apparaître trois questions qui dépassent son périmètre. Ces questions relèvent du champ étudié, dans ses architectures, ses cadres et ses doctrines, et non des limites méthodologiques de la présente analyse, qui établit leur pertinence sans les instruire.[86]

La première porte sur l'architecture des systèmes critiques. Les cas documentés montrent que les systèmes conçus pour un fonctionnement nominal perdent leur utilité lorsque leurs dépendances (connectivité, électricité) sont interrompues. L'approche inverse, concevoir les systèmes dont dépend la continuité des fonctions vitales pour un fonctionnement en mode dégradé et sur des communications indépendantes du transport réseau, constitue un axe de travail identifié.

La deuxième porte sur l'absence de cadre bilatéral de continuité numérique entre États membres. Le droit de l'Union pratique déjà, dans le secteur de l'énergie, l'articulation entre l'échelon commun et l'échelon bilatéral : le mécanisme de solidarité gazière du règlement (UE) 2017/1938 repose sur des accords bilatéraux entre États membres pour ses modalités techniques, juridiques et financières,[87] et des règles par défaut ont été introduites en 2024[88] pour couvrir les cas où ces accords n'ont pas été conclus.[89] La coopération nordique procède de la même architecture : les déclarations de Haga organisent depuis 2009 la préparation civile entre pays nordiques, en articulation explicite avec les initiatives de l'Union et de l'OTAN.[90] À la connaissance de l'auteur au moment de la rédaction de cette note, aucun accord bilatéral entre États membres ne couvre la continuité des services

DOI: https://doi.org/10.5281/zenodo.21285147

numériques en contexte de crise, et les initiatives issues du rapport Niinistö et de la stratégie d'Union de la préparation portent sur la coordination de la réponse à l'échelle de l'Union. Une couche bilatérale viendrait compléter cet échelon commun, comme dans les deux domaines cités, et en réduirait la criticité en tant que point de passage unique de coordination, selon la logique de divergence décrite en section 1. Les propagations transfrontalières documentées dans cette note en illustrent le besoin.

La troisième porte sur l'allocation de l'effort de résilience à travers le graphe. La section 4.1 établit que les exigences de résilience se transmettent par héritage : un nœud amont hérite de celles de l'ensemble des services aval qui en dépendent, et toute fonction du chemin critique de restauration d'une fonction vitale hérite de celles de cette fonction. Le renforcement des nœuds où ces exigences héritées se concentrent découle directement de cette logique. Cette approche par « nœuds critiques » ne suffit toutefois pas à elle seule : l'opacité intrinsèque du renseignement sur les intentions et capacités adversariales, combinée à la propriété documentée des cascades de se propager par le maillon le plus faible du graphe, implique qu'au-delà d'un certain point la valeur marginale d'un renforcement supplémentaire d'un nœud déjà durci devient inférieure à celle de l'élimination d'une vulnérabilité connue sur un nœud faible. L'allocation suit donc le graphe dans ses deux dimensions, à savoir la concentration des exigences héritées, qui désigne les nœuds à durcir, et le chemin de moindre résistance, qui appelle une élévation du niveau de base sur l'ensemble. L'instruction de cet arbitrage, en particulier la localisation du point de bascule entre les deux, dépasse le périmètre de cette note.

Deux considérations éclairent la composante d'élévation du niveau de base. La première tient à la temporalité : une élévation cohérente du niveau de base se construit sur des années voire des décennies, quand une menace peut émerger et s'activer en quelques mois. Un dispositif de résilience conditionné à l'identification préalable de la menace arrive donc potentiellement trop tard. Sa robustesse impose qu'il soit permanent et agnostique quant à la nature du déclencheur, propriété que les cas documentés dans cette note confirment, les mêmes cascades étant activées indifféremment par des évènements météorologiques, des défaillances internes ou des attaques. La seconde tient à la valeur des investissements sous incertitude : la littérature sur la décision robuste en matière d'adaptation climatique établit que les mesures produisant des bénéfices dans un large éventail de scénarios, y compris en l'absence de crise, dominent les mesures dont la valeur est conditionnée à la matérialisation d'un scénario spécifique[91]. Les modèles de défense totale nordiques (*Kokonaisturvallisuus* finlandais[92], *Totalförsvar*[93] suédois) reposent sur cette double logique de permanence et d'élévation systématique du niveau de base, en intégrant l'ensemble des acteurs, administrations, entreprises, organisations et citoyens, dans le dispositif de résilience. Cette orientation trouve une convergence dans la stratégie opérationnelle déclarée par l'autorité française compétente en cybersécurité (ANSSI), dont le directeur général Vincent Strubel explicite le focus comme visant à relever le niveau de sécurité général pour réduire le volume d'attaques réussies.[94]

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

Conclusion

Les infrastructures dont dépendent les fonctions vitales des sociétés européennes formaient des systèmes coexistants. Leur numérisation en a fait un graphe de dépendances unique, dont les propriétés de propagation sont documentées, récurrentes et indifférentes à la nature du déclencheur. Les mécanismes capables d'interrompre ces propagations existent et ont fait leurs preuves, mais leur existence ne renseigne ni sur leur résistance à un ciblage, ni sur leur dimensionnement face à une perturbation de durée inconnue, ni sur les conditions de leur disponibilité, ni sur la capacité des organisations à les activer. Les cadres réglementaires et les exercices qui définissent aujourd'hui l'évaluation de la résilience couvrent chacun leur périmètre avec cohérence, mais cette cohérence est celle d'une partition sectorielle que le substrat numérique traverse désormais de part en part. Le mécanisme de propagation inter-sectorielle n'est l'objet d'évaluation d'aucun d'entre eux, et l'écart croît à mesure que le substrat s'étend.

Cette note propose au lecteur un instrument pour combler cet écart : une grille de critères dérivés de l'empirie, applicables aux dispositifs (cadres et exercices) existants, y compris ceux dont la documentation n'est pas publique. La confrontation de ces critères aux exercices, plans et architectures en place relève des acteurs qui en ont la charge et l'accès.

Les adversaires qui ont frappé les infrastructures documentées dans cette note avaient cartographié les dépendances de leurs cibles avant d'agir, jusqu'aux mécanismes prévus pour contenir les défaillances. Le graphe de dépendances existe et produit ses effets, que les dispositifs d'évaluation le prennent pour objet ou non.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

Remerciements

L'auteur remercie Vincent Giraud (chaire Souveraineté numérique et cyber de l'IHEDN), Tim Clements (Purpose and Means, Copenhague) et Christian Sommade (délégué général du Haut Comité Français pour la Résilience Nationale) pour leurs commentaires sur des versions préliminaires de cette note. Son contenu n'engage que son auteur.

Le substrat numérique des cascades de défaillance : Propagation inter-sectorielle dans les infrastructures critiques européennes. Nicolas Roux, roux.nse@proton.me, août 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

1 "Widely available, low-cost Ethernet, Internet Protocol (IP), and wireless devices are now replacing the older proprietary technologies, which increases the likelihood of cybersecurity vulnerabilities and incidents." Stouffer K., Pease M., Tang C.Y., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. (2023). *Guide to Operational Technology (OT) Security*. NIST SP 800-82r3. DOI : 10.6028/NIST.SP.800-82r3

2 Protogiros D, Tsitsi T, Cloconi C, Nicolaidou I, Kyriacou E, Couespel N, Moreno-Alonso D, Carrión C, Claveria A, Charalambous A. *Mapping and Assessing Existing Digital Skills Training Programs for Health Care Professionals and Health Managers in Europe: Expert-Based Survey for Investigating the Landscape, Accessibility, and Effectiveness of Training Initiatives.* J Med Internet Res 2025;27:e71657. URL:https://www.jmir.org/2025/1/e71657 DOI: 10.2196/71657

3 « Banking has fundamentally become an IT business. » Montagner, p., *"Information and Communications Technology resilience and reliability"*, discours au Frankfurt Banking Summit (Fitch Ratings / PwC Strategy&), Francfort, 2 juillet 2025. URL : https://www.bankingsupervision.europa.eu/press/speeches/date/2025/html/ssm.sp250702~3f15a64e12.en.html

4 Geneletti G, Cremona E, *Money on the line: scaling electricity interconnection for Europe's energy future.* Ember Energy citant le *Ten-Year Network Development Plan* d'ENTSO-E. https://ember-energy.org/latest-insights/money-on-the-line-scaling-electricity-interconnection-for-europes-energy-future/

5 Stanford HAI, *AI Index 2026 Annual Report*, avril 2026. https://hai.stanford.edu/ai-index/2026-ai-index-report

6 European Union ENISA : Handbook for Cyber Stress Tests https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests

7 Cadre d'action de Sendai pour la réduction des risques de catastrophe 2015 - 2030 https://www.unisdr.org/files/43291_frenchsendaiframeworkfordisasterris.pdf

8 « The Digital Operational Resilience Act (DORA) is a regulation introduced by the European Union to strengthen the digital resilience of financial entities. » https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

9 Commission Européenne, « Critical infrastructure resilience at EU-level », 13 janvier 2026. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

10 OTAN, « Resilience, civil preparedness and Article 3 », mis à jour le 13 November 2024. https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3

11 Sauli Niinistö, 2024, « Safer Together, Strengthening Europe's Civilian and Military Preparedness and Readiness », https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

12 Commission européenne et Haut représentant, 26 mars 2025, « Joint Communication on the European Preparedness Union Strategy », https://commission.europa.eu/document/download/526806b6-c4e1-43d1-81b7-947308efbab1_en?filename=Joint%20Communication.pdf

13 Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCDCOE), annonce LS17. https://ccdcoe.org/news/2017/the-largest-international-technical-cyber-defence-exercise-launched-this-week/

14 Armée des Etats-Unis d'Amérique, LS18, « 2d TSB Cybersecurity Division at the forefront of the world's largest live-fire cyber exercise » https://www.army.mil/article/208855/

15 SANS, LS25, « SANS Powers Critical Training for Locked Shields 2025 - World's Largest Live-Fire Cyber Exercise » https://www.sans.org/press/announcements/sans-powers-critical-training-for-locked-shields-2025-worlds-largest-live-fire-cyber-exercise

16 C. Ramezan, L. Schaupp, E. Vitullo, W. Walker. 23 février 2026, Kennesaw State University, « Simulating Cyber-Resilience: The Strategic Role of the Locked Shields Exercise in Enhancing International Cyber Preparedness », https://digitalcommons.kennesaw.edu/jcerp/vol2026/iss1/5/

17 Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, article 1(2), Journal officiel de l'Union européenne, L 333, 27.12.2022, p. 164-198, https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

18 Rinaldi, S M, et al. "Identifying, understanding, and analyzing critical infrastructure interdependencies.." IEEE Control Syst. Mag., vol. 21, no. 6 ; Dec. 2001, Dec. 2001. https://doi.org/10.1109/37.969131

19 Ouyang, M., « Review on modeling and simulation of interdependent critical infrastructure systems », Reliability Engineering & System Safety, vol. 121, 2014, p. 43-60. https://doi.org/10.1016/j.ress.2013.06.040

20 ENTSO-E, « 28 April 2025 Blackout », https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/

21 Aaron Larson pour Powermag, « Anatomy of a Blackout: Findings from the Spain-Portugal Grid Collapse Final Report » https://www.powermag.com/anatomy-of-a-blackout-findings-from-the-spain-portugal-grid-collapse-final-report/

22 David Belson pour Cloudflare, « How the April 28, 2025, power outage in Portugal and Spain impacted Internet traffic and connectivity » https://blog.cloudflare.com/how-power-outage-in-portugal-spain-impacted-internet/

23 Castro-Delgado R, Azeli Y, Pardo Ríos M, et al. Blackout in Spain: Urgent Analysis of Impact on Emergency Medical Services. Prehospital and Disaster Medicine. 2025 Dec;40(6):319-323. DOI: 10.1017/s1049023x25101556. PMID: 41384383; PMCID: PMC12818971. https://portalinvestigacion.uniovi.es/documentos/6987d95671f47e7e0ac0fab1?lang=en

24 Konstantinoudis, G. & Riou, J. (2025), « Excess mortality attributable to the 2025 Iberian Peninsula blackout », surmortalité estimée à +167 décès en Espagne dans les deux jours suivant la panne (intervalle de crédibilité à 95 % : +28 à +300), prépublication medRxiv (non révisée par les pairs), prépublication medRxiv (non révisée par les pairs), doi:10.1101/2025.06.03.25328877 https://www.medrxiv.org/content/10.1101/2025.06.03.25328877v1

25 ENTSO-E, « Grid incident in south-eastern part of the Continental Europe power system - Update », 15 juillet 2024 https://www.entsoe.eu/news/2024/07/15/grid-incident-in-south-eastern-part-of-the-continental-europe-power-system-update/

26 *Federal Energy Regulatory Commission* (FERC) et *North American Electric Reliability Corporation* (NERC), « The February 2021 Cold Weather Outages in Texas and the South Central United States | FERC, NERC and Regional Entity Staff Report », 8 décembre 2021. https://www.ferc.gov/media/february-2021-cold-weather-outages-texas-and-south-central-united-states-ferc-nerc-and

27 Ibid. p.155-156

28 Communiqué FERC, « Final Report on February 2021 Freeze Underscores Winterization Recommendations », https://www.ferc.gov/news-events/news/final-report-february-2021-freeze-underscores-winterization-recommendations

29 « "Freezing and power outage issues at both gathering and processing facilities for natural gas caused limited natural gas supply for generators. Firm load shed affected power supply to various natural gas production and processing facilities that in turn led to further forced outages for natural gas generators. », *February 2021 Cold Weather Event: Winter Storm Uri* du NERC 2021-2022 Winter Reliability Assessment, p. 6 https://www.nerc.com/globalassets/programs/rapa/ra/nerc_wra_2021.pdf

30 Health Services, décembre 2021, « February 2021 Winter Storm-Related Deaths – Texas », https://www.dshs.texas.gov/sites/default/files/news/updates/SMOC_FebWinterStorm_MortalitySurvReport_12-30-21.pdf

31 Sforna, M., « Overview of the events and causes of the 2003 Italian blackout », IEEE Power and Energy Magazine, vol. 4, no. 5, septembre-octobre 2006.

32 Sergey V. Buldyrev, Roni Parshani, Gerald Paul, H. Eugene Stanley, Shlomo Havlin, 15 avril 2010, « Catastrophic cascade of failures in interdependent networks », Nature, vol. 464, p. 1025-1028, https://www.nature.com/articles/nature08932

33 US-Canada Power System Outage Task Force, « Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations », avril 2004, chapitre 5 (Phase 2: FE's Computer Failures). https://www.nerc.com/globalassets/our-work/reports/event-reports/august_2003_blackout_final_report.pdf

34 Peter Sayer (IDG NS), adaptation Jean Elyan, 6 Juillet 2017, « Petya : La police ukrainienne saisit les PC de l'éditeur M.E.Doc ». https://www.lemondeinformatique.fr/actualites/lire-petya%C2%A0-la-police-ukrainienne-saisit-les-pc-de-l-editeur-medoc-68743.html

35 U.S. Department of Justice, 19 octobre 2020, « Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace ». https://www.justice.gov/archives/opa/press-release/file/1328521/dl

36 Microsoft Defender Research (MSTIC), 27 juin 2017, « New ransomware, old techniques: Petya adds worm capabilities » : « We saw the first infections in Ukraine, where more than 12,500 machines encountered the threat. We then observed infections in another 64 countries ». https://www.microsoft.com/en-us/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

37 Andrew Powell (CISO, A.P. Moller-Maersk), présentation Black Hat Europe 2019. Rapporté par Tara Seals, Dark Reading, 11 décembre 2019. https://www.darkreading.com/cyber-risk/maersk-ciso-says-notpeyta-devastated-several-unnamed-us-firms

38 Juan Andrés Guerrero-Saade pour SentinelLabs, « AcidRain | A Modem Wiper Rains Down on Europe » https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

39 Idaho National Laboratory, « PRECURSOR ANALYSIS REPORT: INDUSTROYER2 AND WIPER MALWARE TARGETING UKRAINIAN ENERGY PROVIDER 2022 », page 5 : « Had the Industroyer2 attack been successful, it could have caused a blackout for more than two million people during the early stages of Russia’s invasion of Ukraine. ». https://cyote.inl.gov/content/uploads/24/2025/12/CyOTE-Case-Study_Industroyer2.pdf

40 CISA, 2021, « Cyber-Attack Against Ukrainian Critical Infrastructure » https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

41 ESET, 2017, « Industroyer : la plus importante menace de type malware pour les systèmes de contrôle industriels depuis Stuxnet. » https://www.eset.com/be-fr/industroyer/

42 Rapport CERT-UA H2 2024, p.3 : « The threat of hostile attacks targeting Ukraine’s energy infrastructure and other critical infrastructure remains a pressing concern. These attacks are often observed in advance of missile strikes, suggesting a coordinated hybrid warfare strategy. », p.9 : « Russian hackers systematically attempt to disrupt the operations of Ukraine’s energy sector, coordinating cyberattacks with mass missile strikes on the energy system. » https://cip.gov.ua/services/cm/api/attachment/download?id=68768

43 Alvaro Cardenas, « It’s not an isolated event, these events in the cyber world and physical world are reinforcing each other to create the most damage they can. ». https://news.ucsc.edu/2024/05/ukraine-cybersecurity/

44 Sergiu Gatlan, BleepingComputer, « Russian hackers wiped thousands of systems in KyivStar attack », 4 janvier 2024. Cite la revendication Solntsepek, la confirmation Vitiuk/SBU, et le rapport CERT-UA sur les 11 opérateurs. https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/

45 OCHA, « Ukraine Humanitarian Response 2023 Winter Attacks: Humanitarian Impact of Intensified Strikes and Hostilities - Flash Update #1 (13 Dec 2023) ». https://reliefweb.int/report/ukraine/ukraine-humanitarian-response-2023-winter-attacks-humanitarian-impact-intensified-strikes-and-hostilities-flash-update-1-13-dec-2023-enuk

46 Illia Vitiuk, 27 décembre 2023, cité par Reuters : « For now, we can say securely, that they were in the system at least since May 2023 […] I cannot say right now, since what time they had ... full access: probably at least since November. » https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

47 OSW, "Russia is destabilising the energy system in Ukraine", 11 octobre 2022. osw.waw.pl/en/publikacje/analyses/2022-10-11/russia-destabilising-energy-system-ukraine

48 OSW, "Russia's new large-scale attacks on Ukraine's energy infrastructure", 17 avril 2024. osw.waw.pl/en/publikacje/analyses/2024-04-17/russias-new-large-scale-attacks-ukraines-energy-infrastructure

49 Rapport HRMMU, septembre 2024 : « these assaults have destroyed around 9 gigawatts of electricity generation capacity — equivalent to half of what Ukraine requires during winter months. By June, 73 per cent of the country's thermal power generating units had been rendered inoperative. » ukraine.ohchr.org/en/Attacks-On-Ukraines-Electricity-Infrastructure

50 Ibid. HRMMU : « The damage has caused rolling power cuts across the country, with some cities experiencing blackouts for 12 hours or more a day during a heat wave over the summer. »

51 Ibid. HRMMU : « The destruction of energy infrastructure has compromised essential services, including water distribution, sewage and sanitation systems, heating and hot water, public health, education, and the economy. »

52 Andrew Witty (CEO, UnitedHealth Group), témoignage devant le Congrès américain, mai 2024. Synthèse : BlackFog, « The Change Healthcare Ransomware Attack: A Landmark Cybersecurity Breach ». https://www.blackfog.com/change-healthcare-landmark-cybersecurity-breach/

53 Congressional Research Service, « The Change Healthcare Cyberattack and Response Considerations for Policymakers », IN12330, 24 avril 2024. https://www.congress.gov/crs-product/IN12330

54 AMA, « Physicians struggle to keep practices afloat after Change cyberattack », 10 avril 2024. https://www.ama-assn.org/press-center/ama-press-releases/physicians-struggle-keep-practices-afloat-after-change-cyberattack

55 CISA, NSA, FBI, « PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure », Advisory AA24-038A, 7 février 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

56 BleepingComputer, Ionut Ilascu, « Russian hackers wiped thousands of systems in KyivStar attack », 4 janvier 2024, https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/. « This has led to service interruptions after the hackers deployed scripts during the final stages of the attacks to wipe Mikrotik equipment and backups to make recovery more challenging. »

57 Daryna Antoniuk, 4 janvier 2024, The Record : « The hack did not impact the communication systems of the Ukrainian armed forces, which according to Vitiuk do not rely on telecom operators and made use of what he described as "different algorithms and protocols". » https://therecord.media/russians-infiltrated-kyivstar-months-before

58 ICS Investigation Expert Panel, le 20 mars 2026, « Grid Incident in Spain and Portugal on 28 April 2025 », Final Report, p. 393, section recommendations : « Ensuring that blackout-proof voice communication between key actors and critical remote control functions is available when public telecommunication networks are down. » https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/

59 Istanbul Innovation Days, « Kyiv Digital and Diia - Reinvention in the face of war ». Mentionnant eDocument, un des outils de l’écosystème Diia : « One of its most significant innovations was єДокумент (eDocument), a digital ID that remained operational offline, allowing individuals to verify their identity even when networks were disrupted. » https://istanbulinnovationdays.org/kyiv-digital-and-diia-reinvention-in-the-face-of-war/

60 Developing Telecoms, « Resilience in connectivity: Ukraine's digital battlefront », 20 novembre 2024 https://developingtelecoms.com/telecom-business/telecom-regulation/17644-resilience-in-connectivity-ukraine-s-digital-battlefront.html

61 Developing Telecoms, John Tanner, « Kyivstar starts next phase of network backup-power upgrades », 31 octobre 2024, https://developingtelecoms.com/telecom-technology/energy-sustainability/17551-kyivstar-starts-next-phase-

of-network-backup-power-upgrades.html

62 Liam Maxwell (AWS), 29 novembre 2023, cité par Nextgov/FCW : « Since the beginning of the war with Russia, Maxwell said Ukraine has moved 161 state registries and 356 organizations to the cloud, along with 15 petabytes of critical government data. » https://www.nextgov.com/modernization/2023/11/how-push-cloud-helped-ukrainian-bank-keep-faith-customers-amid-war/392375/

63 PrivatBank, 29 avril 2022, communiqué officiel, https://privatbank.ua/en/news/2022/4/29/financial-safety-above-everything-privatbank-completed-migration-to-cloud

64 Association Deuxfleurs, Garage, logiciel libre de stockage objet distribué compatible S3 : « An S3 object store so reliable you can run it outside datacenters ». Chaque fragment de données est répliqué sur trois zones, sur l'internet public et sur du matériel hétérogène, la résilience aux défaillances de nœud, de site et de réseau constituant un objectif de conception. Le projet a bénéficié de financements du programme Next Generation Internet de la Commission européenne (NGI POINTER, convention n° 871528 ; NGI Zero Entrust, n° 101069594 ; NGI Zero Commons, n° 101135429). https://garagehq.deuxfleurs.fr/

65 Tribunal de commerce de Lille Métropole, jugement du 26 janvier 2023, France Bati Courtage c/ OVH. À la suite de l'incendie de mars 2021 sur le site strasbourgeois d'OVH, le tribunal retient un manquement contractuel à l'offre de sauvegarde automatisée : les sauvegardes étaient stockées dans le même bâtiment que le serveur du client, alors que le prestataire s'était engagé à ce qu'elles soient physiquement isolées de l'infrastructure hébergeant celui-ci. OVH est condamné à 93 000 euros de dommages et intérêts. La présomption d'isolement reposait ici sur l'engagement contractuel lui-même, en l'absence de vérification de sa mise en œuvre effective. https://www.legalis.net/jurisprudences/tribunal-de-commerce-de-lille-metropole-jugement-du-26-janvier-2023/

66 Chatham House, « The internet under attack », août 2024, section 04, note 142, https://www.chathamhouse.org/2024/08/internet-under-attack/04-internet-resilience-ukraine - citant Madory, Doug, « Ukraine's wartime internet from the inside », Kentik, 11 avril 2023.

67 Victor Zhora, vice-président du Service spécial ukrainien des communications, dans une interview donnée à Numerama : « N*ous sommes attaquées depuis 2014. La cyber défense ukrainienne a eu le temps d'apprendre et de se former au fil des attaques ».* https://www.numerama.com/cyberguerre/957249-ukraine-peut-on-dire-que-les-hackers-russes-ont-ete-surevalues.html

68 NTT Security, « Russian hacker claims responsibility for massive cyberattack in Ukraine », février 2024, https://web.archive.org/web/20250716050527/http://se.security.ntt/en/russian-hacker-claims-responsibility-for-massive-cyberattack-in-ukraine/

69 Goiana-da-Silva F, Madureira-Fonseca D, Tude Graça D, Moitinho De Almeida M, Cabral Pinho M, Sá J, Moreira R, Cabral L, Pereira N, Nunes AM, Lourenço A, Branco J, Ashrafian H, Araújo F, Darzi A. « When the lights went out: impacts of the April 2025 Iberian blackout on the Portuguese National Health Service sovereignty - a reflection on national defence, health sovereignty, risk, and infrastructural dependency ». Front Public Health. 2025 Jul 9;13:1630933. doi: 10.3389/fpubh.2025.1630933. PMID: 40703176; PMCID: PMC12283781. https://researchportal.ulisboa.pt/en/publications/when-the-lights-went-out-impacts-of-the-april-2025-iberian-blacko/

70 Joey Roulette, Cassell Bryan-Low et Tom Balmforth pour Reuters, juillet 2025, « Musk ordered shutdown of Starlink satellite service as Ukraine retook territory from Russia » https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/

71 USAID OIG, « USAID Did Not Fully Mitigate the Risk of Misuse of the Starlink Satellite Terminals It Delivered to Ukraine », août 2025, https://oig.usaid.gov/node/7845

72 Sauli Niinistö, 30 octobre 2024, « Safer Together », op. cit., section sur les menaces hybrides et la sécurité économique, p.24 : « Supply chain dependencies, future digital infrastructure, foreign direct investment, research security, and new clean technologies are leveraged by competing and malicious global powers to create the potential for weaponisation as part of coercive strategies. ».

73 « Réquisitions pour les besoins de la défense et de la sécurité nationale » du Livre II de la Partie 2 du code de la défense (article L2211-1 à L2212-11) https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071307/LEGISCTA000006151492/

74 Shalal, Andrea; Roulette et Joey pour Reuters ; 22 février 2025, « Exclusive: US could cut Ukraine's access to Starlink internet services over minerals, say sources » https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/

75 Roux, N., « European Digital Dependencies », mars 2026, https://nicolasroux.eu/publications/european-digital-dependencies/, https://doi.org/10.5281/zenodo.19358627

76 Argote L., Beckman S., Epple D., « The Persistence and Transfer of Learning in Industrial Settings », Management Science, 36(2), 1990, p. 140-154. https://pubsonline.informs.org/doi/10.1287/mnsc.36.2.140

77 Eric D. Darr, Linda Argote, Dennis Epple. « The Acquisition, Transfer, and Depreciation of Knowledge in Service Organizations: Productivity in Franchises », *Management Science*, https://pubsonline.informs.org/doi/10.1287/mnsc.41.11.1750

78 Arthur Jr. W., Bennett Jr. W., Stanush P., McNelly T. (1998), « Factors That Influence Skill Decay and Retention: A Quantitative Review and Analysis », *Human Performance*, 11(1), p. 57-101.

https://gwern.net/doc/psychology/spaced-repetition/1998-arthur.pdf

79 RNBO, « Ukraine's First Grid NetWars Cyber Training Has Started in Kyiv », 2 décembre 2021, https://www.rnbo.gov.ua/en/Diialnist/5170.html

80 Roux, N., « European Digital Dependencies », op. cit.

81 VEON, 18 janvier 2024, « Kyivstar Completes Preliminary Assessment of the Financial Impact of the Cyberattack », https://www.veon.com/newsroom/press-releases/kyivstar-completes-preliminary-assessment-of-the-financial-impact-of-the-cyberattack

82 Directive (UE) 2022/2555 (NIS2), articles 21(2)(d), 21(3) et 22. Journal officiel de l'Union européenne, L 333, 27.12.2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

83 Règlement (UE) 2022/2554 (DORA), articles 31 à 44, relatifs à la désignation des prestataires tiers critiques de services TIC et au cadre de supervision associé. Sur le fonctionnement du cadre et la liste des prestataires désignés : Autorité bancaire européenne, « DORA oversight ». https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/dora-oversight

84 Directive générale interministérielle n°320/SGDSN/PSE/PSN du 23 janvier 2023 relative à la planification de défense et de sécurité nationale, https://www.legifrance.gouv.fr/circulaire/id/45441

85 Ouyang, Op. cit.

86 Ces trois questions font l'objet de travaux en cours de l'auteur.

87 Règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz naturel et abrogeant le règlement (UE) n° 994/2010, article 13, JO L 280 du 28.10.2017. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32017R1938

88 Règlement (UE) 2024/1789 (paquet marché gaz et hydrogène), présenté dans la synthèse EUR-Lex « Sécurité de l'approvisionnement en gaz dans l'Union européenne », https://eur-lex.europa.eu/FR/legal-content/summary/gas-supply-security-in-the-eu.html JO *L, 2024/1789, 15.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1789/oj*

89 Conseil de l'Union européenne, infographie « Gas market: measures to secure and share supply in the EU » : six accords bilatéraux de solidarité conclus (Allemagne-Danemark, Finlande-Estonie, Estonie-Lettonie, Lettonie-Lituanie, Allemagne-Autriche, Italie-Slovénie) sur une quarantaine attendus au titre du règlement de 2017. https://www.consilium.europa.eu/en/infographics/gas-market-share-supply-eu/

90 Déclaration Haga III, réunion des ministres nordiques chargés de la protection civile et de la préparation, 27-28 novembre 2024, qui s'inscrit dans la continuité des déclarations Haga I (2009) et Haga II (2013) et prévoit de « bring forward common initiatives taking into account relevant NATO and EU policies/initiatives ». https://www.mcf.se/siteassets/dokument/om-msb/internationella-samarbeten/haga-iii-declaration.pdf

91 Stéphane Hallegatte, 2009, « Strategies to adapt to an uncertain climate change », Global Environmental Change, 19(2), p. 240-247, https://doi.org/10.1016/j.gloenvcha.2008.12.003

92 Gouvernement Finlandais, 16 janvier 2025, « Security Strategy for Society », https://julkaisut.valtioneuvosto.fi/items/0126122a-1e8a-4ffa-9868-6286292efc01

93 Gouvernement Suédois, 4 mai 2026, « The Strategic Environment and Planning Assumptions for Swedish Total Defence 2025-2030 », https://www.mcf.se/siteassets/dokument/publikationer/english-publications/the-strategic-environment-and-planning-assumptions-for-swedish-total-defence.pdf

94 Vincent Strubel, interviewé par Guillaume Belfiore pour Clubic, 28 juin 2026 : « Notre activité et notre focus principal, aujourd'hui plus que jamais, c'est la prévention. Il s'agit de faire en sorte de relever le niveau de sécurité pour limiter le volume des attaques, en tout cas celles qui réussissent. » https://www.clubic.com/dossier-618682-interview-anssi.html