The Digital Substrate of Cascading Failures

Cross-Sector Propagation in European Critical Infrastructure

Executive Summary

Nicolas Roux - Independent analyst, strategic resilience and digital dependencies, August 2026.

Analytical note, DOI : https://doi.org/10.5281/zenodo.21285147, Licence CC BY 4.0

Full note : nicolasroux.eu/publications · Contact : nr@nicolasroux.eu

Purpose

This note analyses cascading failures across critical infrastructure sectors, drawing on six documented cases: the Iberian (2025), Texan (2021), Italian and North American (2003) power outages, the systematic exploitation of interdependencies against Ukraine (2017–2024), and the attack on Change Healthcare (2024). It establishes that these cascades share a common substrate: the digital layer through which failures cross sectoral boundaries. From these cases, it derives an evaluation grid to assess whether a given instrument (existing framework, regulatory regime or exercise) takes cross-sector propagation as its object. The analysis relies exclusively on public documentation. The criteria it derives are prescriptive at the level of exercise and plan design, and it proposes no change to the instruments it examines.

Findings

1. Digitization has unified critical infrastructures into a single dependency graph with recurring propagation patterns. Energy and telecommunications occupy an upstream position on which nearly all other sectors depend, increasingly through digital channels. Four patterns recur across the cases studied: divergence (a failing node simultaneously degrades multiple sectors that depend on it), convergence (multiple upstream failures reach the same downstream service, such as the simultaneous loss of electricity and telecommunications for Iberian emergency services), feedback loop (two sectors mutually prevent each other from recovering, as with electricity and gas in Texas), and transitive inheritance (a sector inherits the dependencies of the services on which it depends). These propagation patterns occur regardless of the trigger's nature: meteorological, accidental, criminal, or state-sponsored. Cascades through shared digital dependency (M.E.Doc 2017, Change Healthcare 2024) travel along links that did not exist before the digitization of the functions concerned.

2. Containment mechanisms capable of arresting these propagation patterns exist, but their existence says nothing about their effectiveness. Six containment mechanisms are identified from

the empirical data: separation, degraded-mode architecture, local redundancy, replication, substitution, and the organizational competence that conditions the activation of the other five. The documented cases show that these mechanisms themselves constitute vulnerability surfaces, along four failure modes: they can be deliberately targeted or fail silently (destruction of Kyivstar's backups, silent failure of the alarm system during the 2003 North American blackout); their temporal dimensioning can fall short of the disruption's duration (Iberian hospital generators); their availability can depend on a third party whose cooperation is revocable (the reported limitations of the Starlink service in Ukraine); and the competence required for their activation can be lacking, whether through non-acquisition or erosion. An inventory of deployed mechanisms, however complete, measures none of these four failure modes of containment mechanisms.

3. Cross-sector propagation escapes existing frameworks, whose sectoral partition predates digital unification. Projecting the documented cases onto the CER, NIS2, DORA frameworks and, in France, the DGI 320 shows that each instrument covers its perimeter with coherence, and that the mechanism of propagation between sectors escapes each of them. Classification remains sectoral, assessment is conducted at entity level, and the coordination between physical resilience and cybersecurity relies on provisions of principle whose implementation is left to the Member States.

The supply chain provisions run along each bilateral link between an entity and its suppliers, and leave the concentration of many entities on a single shared intermediary unobserved. DORA is the one instrument that supervises such an intermediary directly, but it does so for the financial sector alone.

The DGI 320 illustrates the same configuration at national level: cross-sector analysis features in its risk matrix and disappears from its prescriptive section, which remains sectoral. Documented public exercises, including the most advanced such as Locked Shields, simulate cross-sector environments without making propagation an evaluation object with its own criteria. Recent political initiatives, from the Niinistö report to the Preparedness Union strategy, explicitly acknowledge cascading crises. The proposed treatment, however, bears on the coordination of the response, and no public methodology defines to date the criteria for testing propagation ex ante.

Deliverable: an empirically derived evaluation grid

The note proposes ten criteria, applicable by any reader with access to existing instruments, whether public or otherwise. Five bear on the scenario: does it test causal propagation between at least two interdependent sectors; does it cover the convergence of multiple upstream failures towards the same downstream services; does it integrate the temporal dimension of the cascade (speed, intervention window, irreversibility threshold); does it include a degraded initial condition; does it test propagation beyond the national or jurisdictional perimeter of the assessed entity. Five bear on containment mechanisms: are they themselves subjected to the scenario's stress; does the scenario provide for their neutralization (destruction of backups, silent failure of detection, feedback loop blocking restoration); does the assessment identify dependencies on actors whose cooperation is revocable, and the jurisdiction under which those actors fall; and has the organization demonstrated,

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

under scenario conditions, the capacity to activate them; and does their activation depend on a detection or orchestration layer that the scenario includes in its scope.

Applying these criteria to existing exercises, plans and architectures is the responsibility of the actors who have both charge and access. Non-public work may cover all or part of the gaps identified, and only the reader with access is in a position to judge.

Scope and limitations

The note focuses on illustrating propagation patterns and containment mechanisms through the best-documented nodes in the case studies (energy, telecommunications). The internal dependency structures of these upstream nodes, or of the downstream sectors, are equally relevant for any private or public actor operating within one of these nodes or sectors, but their analysis exceeds the scope of this note, whose sole objective is to make manifest the existence of the dependency graph and associated mechanisms. Three open questions are identified for further work: the design of critical systems for degraded-mode operation, the absence of a bilateral European digital continuity framework, and the allocation of resilience effort across the graph (balanced between hardening the nodes where inherited resilience requirements concentrate and raising the baseline that propagation through the weakest link demands).

Suggested citation: Roux, N., "The Digital Substrate of Cascading Failures: Cross-Sector Propagation in European Critical Infrastructure", August 2026, DOI 10.5281/zenodo.21285147, CC BY 4.0.