The Digital Substrate of Cascading Failures

Cross-Sector Propagation in European Critical Infrastructure

Nicolas Roux, August 2026
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

Summary

The digitization of critical functions has transformed a set of co-existing systems into a single dependency graph, of which digital services form the common substrate, and in which energy and telecommunications occupy an upstream position on which nearly all other sectors depend. The analysis of major outages (Iberian Peninsula 2025, Texas 2021, Italy and North America 2003) and the systematic exploitation of interdependencies against Ukraine shows that failures propagate between sectors along recurring patterns: divergence of a failure from a node on which multiple sectors depend, convergence of multiple upstream failures towards the same downstream services, feedback loops preventing restoration, and transitive inheritance of dependencies. These propagations occur regardless of the trigger's nature, whether accidental or adversarial.

Six containment mechanisms capable of interrupting these propagations are identified from the case studies: separation, degraded-mode architecture, local redundancy, replication, substitution, and organizational competence. The analysis establishes that these mechanisms themselves constitute vulnerability surfaces: they can be targeted, under-dimensioned, dependent on a third party whose cooperation is revocable, or inoperative for lack of competence to activate them. The existence of a containment mechanism says nothing about its effectiveness under real incident conditions.

Projecting the documented cases onto existing frameworks (CER, NIS2, DORA) shows that each covers its perimeter with coherence and that the mechanism of cross-sector propagation falls into the gap between these perimeters, their sectoral partition mirroring a topology that predates digital unification. Documented public exercises simulate cross-sector environments without making propagation an evaluation object with its own criteria. Recent European political initiatives, from the Niinistö report to the Preparedness Union strategy, acknowledge the challenge without yet providing the tools to address it.

The note accordingly proposes an evaluation grid derived from the case studies, applicable both to exercise scenarios and to containment mechanisms, and usable by any reader with access to existing instruments, whether public or otherwise. The criteria it proposes are prescriptive at the level of exercise and plan design. The note proposes no change to the instruments it examines, and makes no claim about exercises whose documentation is not public.

The Digital Substrate of Cascading Failures : Cross-Sector Propagation in European Critical Infrastructure. Nicolas Roux, roux.nse@proton.me, August 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

Table of Contents

Summary....1
Introduction....3
1 - The dependency graph....4
2 - Case studies of cascading propagation....6
2.1 - Civil case studies....6
2.1.1 - Iberian power outage, 28 April 2025....6
2.1.2 - Texas winter storm, February 2021....7
2.1.3 - Italian power outage, 28 September 2003....8
2.1.4 - North American power outage, 14 August 2003....8
2.2 - Adversarial exploitation of interdependencies....8
2.2.1 - Exploitation of interdependencies against Ukraine....9
2.2.2 - Adversarial cross-sector cascade outside armed conflict: Change Healthcare....10
3 - What contains propagation....11
3.1 - Cascade containment mechanisms....11
3.1.1 - Mechanisms embedded in design....12
3.1.2 - Pre-positioned capabilities....12
3.1.3 - Failover to a third-party infrastructure....13
3.1.4 - Organizational competence conditions the usefulness of containment mechanisms….13
3.2 - Containment mechanisms are themselves vulnerable....13
3.2.1 - Mechanisms can be targeted and degraded....13
3.2.2 - The temporal dimensioning of containment mechanisms....14
3.2.3 - Control over containment mechanisms....14
3.2.4 - Observed cost of unplanned response....15
3.2.5 - Summary of empirical lessons on containment mechanisms....16
4 - Analytical conclusions and evaluative framework....16
4.1 - What the empirical data reveal....16
4.2 - Projection onto existing regulatory frameworks....18
4.3 - Evaluation criteria derived from documented cases....20
4.4 - Open questions....20
Conclusion....22

The Digital Substrate of Cascading Failures : Cross-Sector Propagation in European Critical Infrastructure. Nicolas Roux, roux.nse@proton.me, August 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

Introduction

Modern infrastructures exhibit cascading failure modes, as documented in cases from Spain, Italy and the United States, while the conflict in Ukraine has brought to light the deliberate adversarial exploitation of these same mechanisms. These case studies and cascading failure modes share common characteristics that emerge from the strong and still growing connectivity between different sectors of activity, notably through digital channels.

The widespread migration of industrial control systems to IP,[1] the digitization of healthcare[2] and the banking sector,[3] the increasing interconnection of the European power grid,[4] and more recently the mass adoption of AI[5] have transformed a set of co-existing systems into a single dependency graph linking all sectors of activity. This common digital layer is referred to throughout this note as the substrate of the graph: it is through this layer that sectors with no physical link now share propagation paths, and it is its continuing extension that makes the graph a moving object rather than a settled state. Section 1 sets out a description of this dependency graph.

Several international frameworks and large-scale cross-sector exercises aim to test the resilience of critical infrastructure. The principal frameworks include the Handbook for Cyber Stress Tests of the European Union Agency for Cybersecurity (ENISA),[6] the Sendai Framework for Action,[7] the European Digital Operational Resilience Act,[8] the CER Directive (EU 2022/2557) on the resilience of critical entities,[9] and the NATO Baseline Requirements for National Resilience.[10] On the exercise side, these include NATO's Locked Shields and Crisis Management Exercise, the United States' Cyber Storm, and the EU's Cyber Europe 2026. This concern has moreover reached the highest political level of the Union: the report submitted by Sauli Niinistö to the President of the European Commission in October 2024[11] recommends a whole-of-society preparedness approach covering all risks, and the Preparedness Union strategy published in March 2025[12] translates these orientations into thirty actions, including the regular conduct of Union-wide preparedness exercises.

However, examination of available public reports reveals a gap between the growing sophistication of simulated environments and the treatment of cross-sector propagation as an evaluation object. The most advanced technical exercises now simulate cross-sector systems within a single environment: Locked Shields integrates simulated industrial control systems covering the power grid, water treatment, telecommunications and the banking sector, including certain dependencies between systems such as the fuel supply of an air base controlled by programmable logic controllers.[13] [14] [15] Available public reports and academic analyses document the evaluation of defense tactics, national team preparedness and multi-actor coordination when multiple systems are attacked.[16] By contrast, none of these documents treats the causal propagation of a failure between interdependent sectors as an evaluation object in its own right, with its own success criteria: no feedback loop between simulated sectors, no degraded initial condition, no neutralization of containment mechanisms, no temporal dimension of the cascade. The trigger in these exercises remains predominantly cyber (with the exception of NATO's CMX), whereas the empirical data presented in this note show couplings operating in both directions between physical and digital failures. The ENISA handbook illustrates the same gap on the regulatory plane: it identifies

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

cascading effects and interdependencies among the objectives of stress tests, while defining the exercise as an individual assessment of entities, with a single developed example that is mono-sectoral.

Furthermore, the European framework itself structurally separates physical resilience from cybersecurity.[17] The CER Directive explicitly excludes from its scope matters covered by the NIS2 Directive (Article 1(2)), and prescribes their coordination through a general provision whose implementation is left to each Member State. The cases documented in this note, particularly the cyber-kinetic attacks against the Ukrainian power grid, illustrate why the coupling between these two domains is precisely what this separation struggles to capture.

The present analysis relies exclusively on publicly accessible documentation. Classified exercises or unpublished components may cover all or part of the propagation mechanisms documented here. The reader with access to such work is in a position to assess the extent to which the gaps identified in this note are effectively addressed. It remains the case that it is the accessible publications that guide the vast majority of organizations, including public ones, subject to these frameworks.

1 - The dependency graph

The terms characterizing this graph are understood here in the sense established in 2001 by Rinaldi, Peerenboom and Kelly:[18] a dependency is a directed relation by which the state of one sector conditions that of another, and an interdependency is the bidirectional relation formed by two dependencies of opposite direction.

The structure of this graph produces recurring propagations. The first is divergence: a node on which multiple sectors depend in parallel degrades all of them simultaneously when it fails. This pattern encompasses two phenomena that the literature distinguishes: the common-cause failure described by Rinaldi et al., where the common node is the trigger itself, as with the 2021 Texas storm striking both gas infrastructure and electricity generation capacity simultaneously, and the shared-dependency failure, where the common node is a service on which otherwise independent sectors depend, such as the Ukrainian accounting software M.E.Doc in 2017.

The second is convergence: multiple upstream failures, regardless of their origin, reach the same downstream service and produce a multiplying effect. During the 2025 Iberian power outage, the failure of the power grid and the resulting failure of telecommunications converged on emergency services, which were deprived of both their tools and their coordination capacity.

The third is the feedback loop, the activation of an interdependency in which two nodes mutually prevent each other from recovering: during the 2003 Italian power outage, internet routers went down with the power supply, making impossible the communication needed to restore electricity. This loop can be direct, as in the example cited, or indirect, transiting through one or more intermediate nodes.

The fourth is transitive inheritance: a sector inherits the dependencies of the services on which it depends. During the Iberian power outage, it was not the healthcare sector that was struck but the

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

power grid, yet the chain of dependencies transmitted the failure all the way to patient care through digital medical records and the servers hosting them.

To these structural patterns is added a condition of state: Rinaldi et al. term escalating failure the situation where a disruption occurs while another, independent disruption is already degrading response capacity. The operations documented in section 2.2, where cyberattacks accompany campaigns of physical strikes, constitute the clearest illustration. This condition is incorporated as an evaluation criterion in section 4.3.

These characteristics render certain nodes in the graph particularly critical. The fact that the four civil case studies documented in this note involve the power grid as the central propagation vector is not a selection artefact: it reflects the position of electricity as an upstream node on which the operation of nearly all other sectors depends, notably through digital channels. Digital services occupy a dual position in this graph. They constitute one of its upstream nodes, on a par with energy: the failure of telecommunications or digital services degrades every sector that depends on them. Above all, they constitute its substrate: the common layer through which sectors become linked to one another, including where no material coupling exists between them. The M.E.Doc and Change Healthcare cases documented in section 2.2 belong to this second role: physically independent sectors there share failure modes because their functions transit through the same digital intermediaries. The distinction matters for the analysis, because each digitization of a function adds to the graph an edge that is declared nowhere and that becomes visible, most often, only upon its activation.

The present note focuses on the upstream nodes of the dependency graph (energy, telecommunications) and on the digital interfaces through which failures propagate between sectors. Downstream sectors (including water, food supply, transport, healthcare) appear in the case studies as recipients of the documented cascades. The analysis of their internal dependency structures and their specific containment mechanisms exceeds the scope of this note.

The level of granularity of the graph is to be adapted to the needs of the analysis and to the available data. The present note confines itself to a descriptive use of the graph. Its quantitative modelling and simulation constitutes an established research field[19] that lies outside its scope.

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

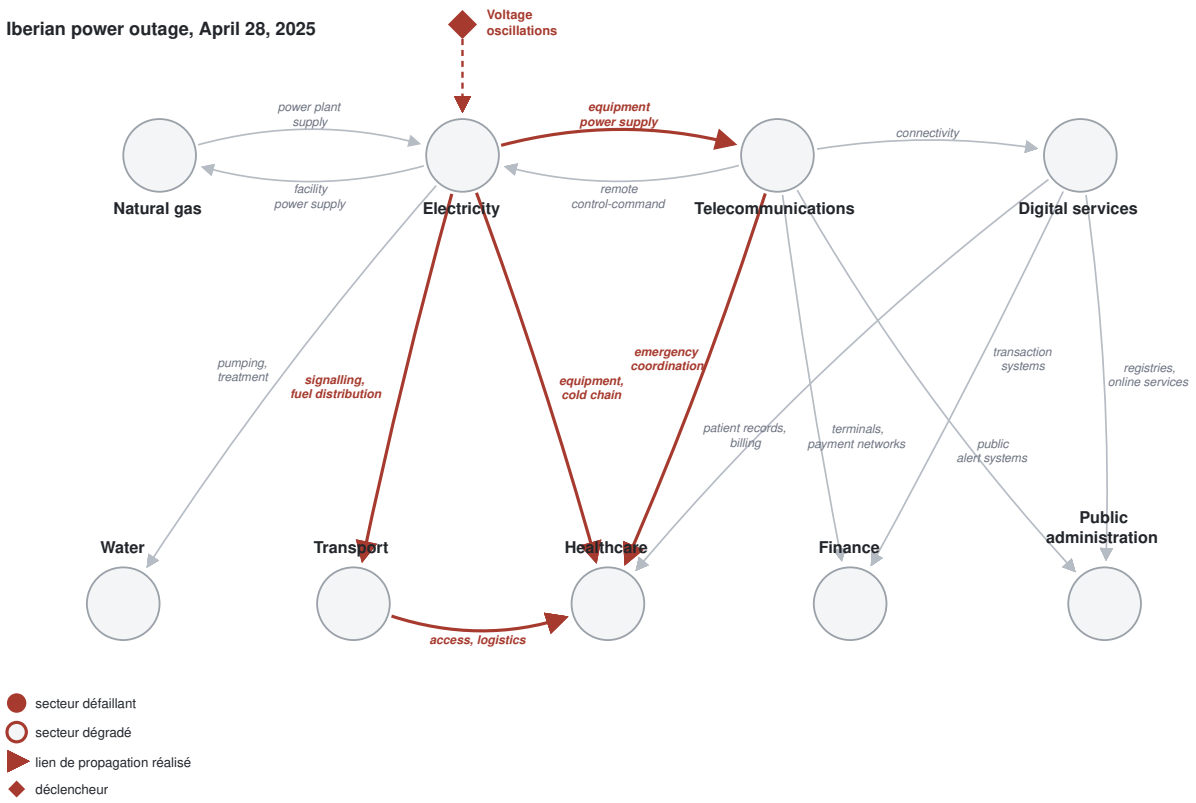

Figure 1: Simplified illustrative representation of the Iberian blackout (in red) projected onto the dependency graph.

2 - Case studies of cascading propagation

This section aims to identify how interdependencies between different sectors affect infrastructures in the event of unintentional occurrences (meteorological events, internal system failures) or intentional ones (attacks by a third-party entity).

2.1 - Civil case studies

The accidental or exogenous events listed here are examined through the lens of the failure modes described in section 1. The cascades, feedback loops and dependency chains presented here were revealed by their activation following an unforeseen event, as opposed to deliberate exploitation.

2.1.1 - Iberian power outage, 28 April 2025

This case is the most recent civil instance of cascading infrastructure failure, and it has benefited from an extensive analysis[20] conducted by an international panel of experts. The outage affected more than 50 million people and lasted over 10 hours.[21] The initial observed failure was a series of voltage oscillations in the power grid, leading to disconnections of renewable energy generation stations. The loss of power generation induced a collapse of network traffic to 10% of normal levels.[22]

The Digital Substrate of Cascading Failures : Cross-Sector Propagation in European Critical Infrastructure. Nicolas Roux, roux.nse@proton.me, August 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

These combined effects (power generation and telecommunications) reached, among others, hospital services, whose adaptation mechanisms (use of backup generators, equipment triage, paper-based records) rapidly reached their limits (backup generator capacity, restricted equipment use, threatened cold chain for medications). The impact on healthcare extended beyond hospital services alone: the volume of emergency calls collapsed, traffic lights and gas stations ceased to function,[23] creating a combined accident-generating effect and reducing the responsiveness of emergency services to this increased incidence of accidents. Eight deaths directly linked to the outage were reported, with excess mortality probably exceeding this direct toll,[24] for an outage that lasted 10 hours and in the absence of any degraded initial condition.

No affected region had a specific continuity plan for a prolonged power outage affecting emergency medical services. This fragility is not an isolated case: the causes are similar to an incident that occurred in south-eastern Europe in 2024.[25]

The impacts on the healthcare sector illustrate the fact that a sector inherits the dependencies of the sectors on which it itself depends: emergency services depend on access to fuel retail points and a functioning signalling system, which themselves depend on the proper functioning of the power grid, and therefore emergency services depend indirectly on the power grid. This analysis may seem self-evident in this particular case, but certain services have dependency chains that are both more complex and equally critical to their proper functioning, making it necessary to map and take into account the full dependency graph of an actor when frameworks or exercises aim to measure its resilience.

2.1.2 - Texas winter storm, February 2021

A winter storm struck the Texas power grid during the winter of 2021, depriving approximately 4.5 million households of electricity at peak outage, some for several days.[26] This case study illustrates the cross-sector feedback loops described in section 1.

The sequence of events began with a meteorological event (an episode of extreme cold) that led to the freezing of gas wellheads and certain natural gas processing facilities. Gas production consequently fell, and gas-fired power plants (which represented the primary source of Texas electricity generation) saw their supply fall in turn, forcing grid operators to carry out massive load shedding.

This load shedding deprived gas facilities of the electricity on which they depend to operate, which worsened the loss of gas production, and therefore once again worsened load shedding. The joint report of the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) explicitly mentions a mutual lock-in[27] and the associated press release indicates that 43.3% of gas production declines were due to freezing and weather conditions, and 21.5% to loss of power supply to production, gathering or processing facilities.[28] The strong interdependency between these two sectors produced a feedback loop that worsened the problem[29] and prevented both sectors from recovering.

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

The outage caused 246 deaths, a majority from hypothermia,[30] illustrating by comparison with the Iberian outage the fact that the duration of the outage and its context have a strong bearing on final outcomes.

The FERC/NERC report shows that gas infrastructure had not been identified by the grid operator Electric Reliability Council of Texas (ERCOT) as "critical loads" to be kept active as a priority during load shedding plans. When load shedding was ordered, the operator cut power to the very facilities that were supposed to supply gas to the power generation plants.

This feedback loop therefore appears avoidable, or at least mitigable, but this requires having identified in advance the dependencies of critical systems and assigned responsibility to their suppliers, and may also depend on external factors as section 3 of this note shows.

2.1.3 - Italian power outage, 28 September 2003

This outage affected approximately 45 to 57 million people by various estimates in Italy and spread into the Swiss border areas, with restoration times of up to 19 hours depending on the region, and caused outages beyond Italian borders, in Switzerland (canton of Geneva, approximately 3 hours).[31]

Its distinctive feature is that it too exposed a feedback loop, this time between the energy sector and the telecommunications sector. The control systems used to operate the power grid rely on internet connectivity, but internet access requires the physical devices (routers) to be powered. Once these routers lost power, the restoration of the power grid was compromised. This case is the empirical foundation for the formalization by Buldyrev et al.[32] of the nonlinear fragility of coupled networks: the failure of a node in network A causes failures in network B which in turn worsen the failure of A.

2.1.4 - North American power outage, 14 August 2003

A few weeks before the Italian outage, a comparable outage struck the northeastern United States and Ontario (Canada), depriving approximately 50 million people of electricity. The joint United States/Canada investigation identified among the principal causes a loss of situational awareness by grid operators: the software alarm system of the control centre of FirstEnergy, the operator at the origin of the cascade, failed silently due to a software defect, depriving operators of all visual and audible alerts on the state of the grid for over an hour without their knowledge.[33]The operators continued to work believing they were observing a stable grid while overloaded transmission lines were failing in succession, propagating the failure until the cascading collapse of the regional grid. This case is used in section 3 of the present note to illustrate the vulnerability of detection mechanisms themselves.

2.2 - Adversarial exploitation of interdependencies

The civil cases of section 2.1 document the manifest existence of cascading and feedback failure modes in modern infrastructures. These failure modes, in the context of open conflicts or otherwise, constitute an exploitable means of action for an adversary. The empirical data show that in order to maximize the effects of an attack, an adversary can simultaneously target interdependent systems

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

and the means (see section 3) for interrupting the propagation of failure modes (backup generators, spare equipment stocks, logistics, alternative solutions, etc.), all within an initially difficult external context for the defender.

2.2.1 - Exploitation of interdependencies against Ukraine

Before even the Russian offensive in Ukraine, in June 2017, the update mechanism of an accounting software widely used in Ukraine (M.E.Doc) was compromised by Russian military intelligence and used to distribute destructive software to all its users.[34] [35] The attack propagated through the corporate networks of infected organizations to their business partners in at least 65 countries.[36] The affected sectors had no physical dependency between them yet were simultaneously impacted: port operations of the world's largest shipping company paralyzed for over a week, pharmaceutical production lines interrupted, patient records and radiology systems inaccessible in American hospitals, the Chernobyl radiation monitoring system taken offline.[37] What links these sectors is the digital substrate itself: their common dependency on shared services. The digitization of accounting, port logistics, industrial production and hospital management created the common propagation path through which an attack targeting a single country degraded critical functions in physically independent sectors on a global scale.

On 24 February 2022, Ukraine suffered a large-scale cyberattack targeting the modems and routers (internet access equipment) of the satellite access operator Viasat. The cybersecurity operator SentinelOne cites as a plausible motive an attempt to deprive the Ukrainian armed forces of part of their remote command and control capabilities. The attack had the collateral effect of depriving 5,800 wind turbines of internet access in Germany, interrupting their control and supervision capabilities and thereby rendering them temporarily inoperative.[38] Residential internet connections also suffered outages in France, Hungary, Greece, Italy and Poland.

In April 2022, a cyberattack targeted the Ukrainian power grid. The malware used targeted the control systems of high-voltage substations, with the objective of physically disconnecting substations supplying power to more than 2 million people.[39] The attack was thwarted by Ukrainian defenders assisted by the Ukrainian Computer Emergency Response Team (CERT-UA) and the cybersecurity firm ESET. It is part of a series begun in 2015[40] and 2016,[41] in which cyberattacks by the same actor affiliated with Russian military intelligence (GRU) had effectively caused power outages in Ukraine, establishing the capability to cross the boundary between the cyber domain and physical flows through industrial control systems.

This cyber-kinetic synergy has since been exploited on a continuous basis by the attacker. CERT-UA indicates, regarding Russian cyberattacks, that "These attacks are often observed in advance of missile strikes, suggesting a coordinated hybrid warfare strategy."[42] American cybersecurity researchers established explicitly in 2024 that cyberattacks and physical attacks are now used in conjunction to maximize their respective effectiveness.[43]

In December 2023, the Ukrainian telecommunications operator Kyivstar was in turn the target of a large-scale attack aimed at its digital infrastructure. The attack, orchestrated by a sub-entity of Russian intelligence,[44] affected (according to the group claiming responsibility) thousands of

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

workstations and servers, cloud storage systems and the backups intended to restore systems in the event of an outage. The attack disrupted the air-raid alert system in more than 80 localities in the Kyiv oblast alone as well as in large portions of the Cherkasy, Dnipropetrovsk, Kharkiv and Sumy oblasts, whose alert systems depended on Kyivstar infrastructure,[45] facilitating the campaign of physical strikes against Ukraine then underway. Mobile and internet access for 25 million people as well as certain banking terminals was cut. The head of the SBU's cybersecurity department noted that the attackers had been present in the system since at least May 2023, with total access probably achieved from November, which had allowed them to map the infrastructure and target backup systems simultaneously with the primary systems.[46]

The Ukrainian power grid constitutes a focal point of Russian attacks since the beginning of the war. The campaign of systematic strikes against energy infrastructure began in October 2022, initially targeting the transmission network (substations and distribution lines).[47] In spring 2024, a tactical shift targeted generation plants directly,[48] destroying or severely damaging approximately 9 GW of generation capacity, representing half the country's winter demand. By June 2024, 73% of thermal generation units were out of service.[49] The resulting load shedding exceeded twelve hours daily in certain cities,[50] propagating the failure to water supply, heating, sanitation systems, public health and education.[51] This attack model illustrates in an adversarial context the same mechanism documented in the civil cases of section 2.1: the position of electricity as an upstream node in the dependency graph transforms a strike targeting a single sector into cross-sector degradation.

2.2.2 - Adversarial cross-sector cascade outside armed conflict: Change Healthcare

In February 2024, a criminal group targeted Change Healthcare, a digital intermediary through which a significant share of transactions between insurers and healthcare providers in the United States transits.[52] The company was forced to take all its systems offline for several weeks.[53]

The effects propagated to the healthcare sector despite the absence of any attack on physical care infrastructure: pharmacies could no longer verify insurance coverage or process prescriptions, and hospitals could no longer submit reimbursement claims. Small practices were disproportionately affected, with 80% of respondents to the AMA survey reporting revenue losses more than one month after the attack.[54]

This case illustrates the same mode of healthcare sector degradation as the Iberian outage: physically functional care infrastructure unable to fulfil its mission because a digital dependency is broken. The failing node is here neither electricity nor telecommunications but a transactional intermediary whose digitization created the dependency link between the financial sector and the delivery of care. This link did not exist before the digitization of the billing chain. The fact that the actor is criminal rather than state-sponsored confirms that the exploitation of interdependencies requires neither the resources nor the strategic intent of a state: cascade mechanisms are an intrinsic property of the digital substrate, independent of the attacker's nature.

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

3 - What contains propagation

The case studies detailed in section 2 show the existence of feedback loops and cascades, as well as their accidental or intentional activation by adversarial conditions or attacks. Regarding adversarial attacks specifically, it appears that attackers with adequate resources map the dependencies of the systems they target before striking, as the Kyivstar and M.E.Doc cases illustrate. The United States has documented a case of pre-positioning maintaining dormant access to a system for at least five years.[55]

This in-depth knowledge of the dependencies of a system potentially targeted by an adversary raises a consequential problem: if the adversary knows the dependencies and vulnerabilities, it also knows the mechanisms in place to mitigate the dependencies and vulnerabilities, or to interrupt the propagation of failures through those dependencies. These mechanisms themselves become a target that attackers aim for to maximize the effect of their actions.[56] As a corollary, they also become an object to protect for the defender.

3.1 - Cascade containment mechanisms

The civil and armed conflict case studies presented in section 2 allow the identification of six containment mechanisms, one of which is cross-cutting, that have contained or interrupted propagation. The examples illustrating these mechanisms in section 3.1 are concentrated on Ukraine not by editorial choice but by a selection bias stemming directly from data availability, the Ukrainian computer emergency response team (CERT-UA) publishing prolifically on the attacks sustained by the country. These containment mechanisms are distinguished along three axes: their operating regime (the mechanism operates by design, without activation; it relies on a pre-positioned resource whose effect requires activation; or it mobilizes ex post a non-pre-positioned capability), their location (the mobilized resource is internal to the protected system or provided by a third party), and the object they preserve (the function delivered, the data, or the capacity to activate the other mechanisms). The activation of a pre-positioned mechanism may be operator-driven or automatic. The distinction bears on the response delay and on the object to be protected: an automatic activation removes the latency of human detection and decision, and transfers the condition of the mechanism's effectiveness to the layer that performs it. Section 3.2 addresses the consequences. The following table positions each mechanism along these axes and the subsequent subsections group them by mode of operation.

Mechanism	Operating regime	Location	Object preserved
Separation	By design	Internal	The function, through absence of propagation link
Degraded-mode architecture	By design	Internal	A partial function
Local redundancy	Pre-positioned, activation required	Internal, on site	The function, for a bounded duration
Replication	Pre-positioned, activation required	External in most cases	The data and system state

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

Mechanism	Operating regime	Location	Object preserved
Substitution	Ex post mobilization	External	The function, via a third-party infrastructure
Organizational competence	Cross-cutting	Organizational	The capacity to activate the other five

3.1.1 - Mechanisms embedded in design

Separation and degraded-mode architecture operate by design: they require no activation at the time of the incident, and their cost is borne entirely up front.

Two separated systems have, by definition, no link through which the failure of one could propagate to the other. The communications network of the Ukrainian armed forces remained functional during the December 2023 attack against Kyivstar, because it relies on protocols and infrastructure distinct from the attacked civilian operator.[57] Similarly, the final report of the ENTSO-E expert panel on the Iberian outage recommends that voice communications between key actors and critical remote control functions remain operational when public telecommunications networks are down,[58] which amounts to prescribing an architectural separation between power grid control communications and the public network.

Degraded-mode architecture provides, from the design stage, restricted but operational functioning when the system's dependencies (connectivity, electricity) are interrupted. The Ukrainian digital identity management service Diia offers a partial example: the local storage of documents allows use without connectivity, although verification and transactional services remain network-dependent.[59] The distinction from separation lies in the object: separation suppresses the dependency link while degraded-mode architecture preserves the link but bounds the consequences of its rupture.

3.1.2 - Pre-positioned capabilities

Local redundancy and replication rely on resources deployed before the incident whose effect materializes only upon activation. A critical variable common to mechanisms mobilizing a bounded resource is dimensioning: temporal for redundancy, scope of coverage for replication. Temporal dimensioning is the subject of section 3.2.2.

Local redundancy is a backup capability physically available on site, allowing a function to be maintained for a limited duration without network dependency. Ukraine has allocated substantial resources to give its telecommunications network resilience against power outages, with more than 4,000 generators and 230,000 batteries deployed at the telecommunications towers of operators Lifecell-Datagroup-Volia[60] and Kyivstar.[61] The backup generators of Iberian hospitals fall under the same mechanism although their dimensioning proved insufficient against the duration of the outage.

Replication consists of copying data or systems to an alternative environment, such that the destruction of the original does not destroy the function. The emergency migration of Ukrainian state registries to the cloud constitutes the most documented example: 161 national registries and

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

approximately 15 petabytes of government data were replicated outside the territory starting in February 2022.[62] PrivatBank, the country's largest bank, migrated all its operations in under 45 days.[63]
Replication does not necessarily imply a subsequent failover operation. Distributed architectures maintain a service simultaneously across several sites, so that the loss of one node leaves the function available without operator action at the time of the incident. This mode of operation is native to the large cloud providers, and it is also implemented outside them, on open-source software running on geographically dispersed and heterogeneous hardware.[64]

Where the failover is operator-driven, the mechanism depends on detection, decision and execution, whose latency adds to the propagation window. Where it is automatic, the mechanism depends on the layer that detects the failure and reroutes traffic, which becomes a component of the containment mechanism in its own right. In neither case is redundancy a property acquired without design: it presupposes a dimensioning of the surviving capacity and a configuration whose conformity to the intended behaviour has been verified and tested. A deployment presumed to be replicated but configured within a single availability zone (or physical site) provides the appearance of the mechanism without its properties.[65]

3.1.3 - Failover to a third-party infrastructure

Substitution consists of the failover of a service to an alternative infrastructure after the failure. This mechanism, activated ex post, is the most likely to be externalized to a third-party entity, making it the mechanism most exposed to the control risks addressed in section 3.2.3.

The deployment of Starlink after the neutralization of Viasat on 24 February 2022 is the primary illustration: although representing a small share of Ukrainian internet traffic,[66] the network provided a rapidly deployable replacement capability in a crisis situation. The infrastructure sharing between competing operators after the attack on Kyivstar (Vodafone Ukraine, Lifecell) falls under the same mechanism, in a configuration where the third party is a domestic peer rather than a foreign provider.

3.1.4 - Organizational competence conditions the usefulness of containment mechanisms

Organizational competence is different in nature from the five preceding mechanisms: it does not interrupt a propagation by itself, but determines whether pre-positioned capabilities are activated in time, whether the failover to a third party is executed correctly, and whether the dimensioning of the whole corresponds to actual needs. It conditions the effectiveness of the mechanisms of sections 3.1.1 to 3.1.3 without substituting for them. The experience acquired by Ukrainian services during the attacks against their power grid in 2015 and 2016 enabled the response that thwarted the April 2022 attack.[67] Its own failure modes, non-acquisition and erosion, are addressed in section 3.2.3.

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

3.2 - Containment mechanisms are themselves vulnerable

As noted in the introduction to section 3, the containment mechanisms for failure propagation are not exempt from failing themselves, for intentional, accidental, or negligent reasons. These mechanisms are an integral part of the system concerned from the standpoint of its capacity to maintain or restore its functioning, and they must therefore be subjected to resilience criteria as well.

3.2.1 - Mechanisms can be targeted and degraded

During the campaign against Ukrainian telecommunications operators, CERT-UA reports a targeting of Kyivstar's backups, with the explicit purpose of making recovery more difficult. The replication mechanism was here targeted as such.

Also in the Kyivstar case, the destruction of the customer registration system prevented the failover of subscribers to competing operators via national roaming.[68] The substitution mechanism did not function because the system on which it depended had been destroyed.

During the 2003 North American outage, the software alarm system (forming part of the containment mechanism) of the operator's control centre failed silently. The mechanism whose function is precisely to detect grid degradation and signal the emergency was the first point of failure, and it failed without signalling itself. The operators continued to work believing they were observing a stable grid while the cascade was propagating.

During the 2003 Italian outage, the power grid restoration mechanism (communication via the internet to control reconnection) depended on the very network whose restoration was the objective. The feedback loop coupling energy and the internet prevented each network from restoring the other.

Automatic activation displaces this exposure without removing it. The detection and orchestration layer that triggers the failover conditions the effectiveness of the mechanism it operates: its own failure, silent or otherwise, leaves redundant resources available and unused. The silent failure of the FirstEnergy alarm system in 2003 illustrates this mode on a mechanism whose function was detection. Where this layer is shared by several services, its failure degrades them simultaneously, which is the divergence pattern described in section 1 applied to the containment mechanism itself. A containment mechanism is itself a node in the dependency graph: it carries its own dependencies and inherits the resilience requirements of the function it preserves.

3.2.2 - The temporal dimensioning of containment mechanisms

A vulnerability cutting across all containment mechanisms mobilizing a bounded resource is that of their temporal reach. The Iberian hospital generators failed because they had a capacity of a few hours and had to face an outage lasting over 10 hours.[69] A containment mechanism whose runtime is shorter than the duration of the disruption merely delays the cascade, and since the disruption's duration is a priori unknown before the triggering event, the dimensioning of each runtime reserve deserves particular attention. The conceptual distinction between interrupting a cascade and

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

delaying it is obvious but its consequences are non-trivial: the temporal runtime that a cascade containment mechanism (backup generator, battery, food stocks, water or medication supplies, etc.) provides must be calculated against the needs of dependent services, which implies a precise mapping of these services and their requirements.

For example, the runtime of a generator on which refrigerated stocks and life-support equipment depend is to be measured against the resupply lead time under degraded conditions.

3.2.3 - Control over containment mechanisms

Containment mechanisms present risks related to their control. In particular, two dimensions of this control can call into question their operational usefulness: sovereignty and organizational competence.

Sovereignty. A containment mechanism owned and operated by the actor that depends on it carries risks (failures, under-dimensioning, design error), all mitigable by its owner. When the mechanism belongs to a third party, its availability, scope of use and conditions of access are decided by an actor whose cooperation is revocable, as reported by Reuters in the case of the Starlink service provided to Ukraine,[70] subject to pricing, conditional[71] or instrumentalized[72]. The jurisdictional position of this third party modulates the risk. A service provided by a third party falling under the jurisdiction of the dependent actor remains revocable in intent, but remains in principle compellable through legal instruments such as service obligations or requisition,[73] at the cost of a delay and execution uncertainty that fall under the same temporal dimensioning requirements as other mechanisms (section 3.2.2). A third-party service provider situated outside that jurisdiction is accessible only through contractual or diplomatic levers.[74] The infrastructure sharing between Ukrainian operators after the attack on Kyivstar and the substitution by Starlink after the neutralization of Viasat illustrate these two positions (section 3.1.3). This distinction does not call into question the usefulness of a third-party mechanism, but it characterizes its availability (compellable in one case, negotiable in the other, and without guarantee in either case).

The degree of autonomy afforded by a given capability is intrinsically linked to the degree of sovereignty over that capability. This sovereignty is a continuous and shifting spectrum, requiring analysis proportionate to the criticality of the capability or containment mechanism.[75]

Competence. The organizational capacity to activate containment mechanisms under the real conditions of an incident conditions their effectiveness as much as their existence. A mechanism present but activated too late, poorly dimensioned or never tested produces a result close to that of an absent mechanism.

This capacity fails by two paths. Non-acquisition, first, when the organization has never confronted the scenario: no region affected by the Iberian outage had a continuity plan for a prolonged power outage affecting emergency medical services. Although generators existed, their articulation with the needs of dependent services had never been tested.

Erosion, second, when organizational competence degrades for lack of practice. Competence is a perishable asset. The literature on organizational learning has long documented the depreciation of

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

acquired knowledge in the absence of practice: drawing on production data from American shipyards during the Second World War, Argote, Beckman and Epple show that organizational knowledge depreciates rapidly when activity ceases.[76] This finding has been replicated in other organizational contexts.[77] At the individual level, the meta-analysis by Arthur et al. establishes that skills not exercised decline and that this decline increases with the duration of non-use. The mandatory recurrence of exercises in national preparedness frameworks rests on this observation.[78] This observation is analytically distinct from sovereignty: a mechanism may be sovereign yet inoperative for lack of maintained competence to activate it.

The empirical contrast is clear. The national preparedness exercises conducted by Ukraine in 2021 covered a significant share of the scenarios that materialized in February 2022,[79] and the experience of the 2015–2016 attacks against the power grid enabled the response that thwarted the April 2022 attack. Competence was built and then maintained through repeated confrontation.

The evaluative implication is direct: an exercise that does not subject the activation of containment mechanisms to scenario conditions measures the existence of these mechanisms, without measuring the capacity to operate them. This criterion is taken up in section 4.3.

The control considerations developed here apply to every node in the dependency graph. The present note addresses them where their failure is without recourse: containment mechanisms constitute the last line of interruption of a cascade, and their unavailability leaves propagation without obstacle. The analysis of control over the upstream nodes themselves falls under dependency mapping.[80]

3.2.4 - Observed cost of unplanned response

The cases documented in this note allow partial observation of the cost of containment mechanisms deployed as an emergency, after the onset of degradation, as opposed to the pre-positioned capabilities described in section 3.1.

As an example, the attack on Kyivstar represented an estimated financial impact of 3.6 billion hryvnias (approximately 90 million dollars) on the operator's 2024 revenues, covering customer retention measures, temporary free service and repairs.[81] By comparison, Kyivstar invested 1.9 billion hryvnias (approximately 47.5 million dollars) over two years in the pre-positioned reinforcement of the electrical redundancy of its network.

These figures aim to provide an indicative order of magnitude, but their citation calls for three methodological caveats. First, the cost of installing this electrical redundancy capability is not to be compared directly with the financial impact of the attack on Kyivstar, but against the share of that impact that the redundancy would have made it possible to avoid. Calculating that hypothetical impact is probably unfeasible and counterfactual, the prior absence of this redundancy having probably influenced the attacker's choices. Second, the financial impact of the attack is not limited to the company's revenues alone but extends to the activities that depended on its infrastructure. Finally, an honest calculation of the cost of planning should integrate all funded resilience measures that are never activated. The trade-off between the cost of pre-positioning and that of emergency

DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

response falls under a dimensioning calculation under uncertainty that exceeds the scope of the present note, as the third question in section 4.4 makes explicit.

3.2.5 - Summary of empirical lessons on containment mechanisms

The empirical data gathered in this section indicate that cascade containment mechanisms themselves constitute vulnerability surfaces, along four distinct modes. They can be deliberately targeted, as with Kyivstar's backups, or fail silently, as with FirstEnergy's alarm system. Their temporal dimensioning can fall short of the disruption's duration, in which case they delay the cascade without interrupting it. Their availability can depend on a third party whose cooperation is revocable. Finally, the organizational competence required for their activation can be lacking, through non-acquisition or erosion.

These four failure modes share a common consequence: the existence of a containment mechanism says nothing about its effectiveness under real incident conditions. An inventory of deployed mechanisms, however complete, measures neither their resistance to targeting, nor their runtime against a disruption of unknown duration, nor the conditions of their availability, nor the organization's capacity to activate them. Assessing the resilience of a system therefore requires subjecting its containment mechanisms to the same testing regime as the system itself. Section 4 translates this requirement into evaluation criteria.

4 - Analytical conclusions and evaluative framework

4.1 - What the empirical data reveal

The cross-sector propagations documented in this note are recurring and exhibit patterns from which generalizable lessons can be drawn. The causes of the 2025 Iberian blackout are similar to those of an incident in south-eastern Europe in 2024. The feedback loop between electricity and gas observed in Texas in 2021 is comparable to the loop between electricity and the internet observed in Italy in 2003. The cascades through shared digital dependency (M.E.Doc in 2017, Change Healthcare in 2024) strike physically independent sectors through the same vector: this is the divergence pattern operating outside any physical coupling. These propagation occur regardless of the trigger's nature (meteorological accident, internal failure, criminal attack or state operation). This recurrence has an identifiable cause. The four patterns described in section 1 existed before digitization wherever a physical coupling linked two sectors, as between gas and electricity in Texas. What the digital substrate has changed is the extent of the graph that carries them: digitization has created propagation paths between sectors that previously shared none, and the M.E.Doc and Change Healthcare cascades travelled along links that did not exist ten years before their activation. The patterns are old but the topology that generalizes them is recent, and it continues to extend.

The mass adoption of AI, mentioned in the introduction, extends this dynamic of graph formation: the concentration of models and inference capabilities with a small number of providers establishes a new upstream node whose criticality grows with the integration of these services into the

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

operational processes of downstream sectors. No major cross-sector cascade attributable to this node has been publicly documented to date, yet its position is identical to that of the shared digital intermediaries whose failure produced the cascades described in sections 2.2.1 and 2.2.2: The designation mechanism described in section 4.2, which identifies a provider whose failure would be systemic and whose substitution would be difficult, is the closest existing answer to this position, and it applies to one sector only.

The pace of this extension is a parameter in itself: several years elapse between the adoption of a regulatory framework and its entry into application, whereas the integration of a new digital intermediary into the operational processes of entire sectors is measured in months. The graph reconfigures itself faster than the instruments designed to assess it.

The containment mechanisms documented in section 3, whether embedded in design (separation, degraded-mode architecture), pre-positioned (local redundancy, replication) or based on failover to a third party (substitution), functioned in the cases studied. These same cases show, however, that these mechanisms themselves constitute vulnerability surfaces, along the four modes identified in section 3.2: deliberate targeting or silent failure (destruction of Ukrainian telecom operators' backups, silent failure of FirstEnergy's alarm system in 2003), temporal under-dimensioning (Iberian hospital generators), dependency on a third party whose cooperation is revocable (the reported limitations of the Starlink service to Ukraine), and lack of organizational competence, through non-acquisition or erosion. The question of control over these mechanisms is analytically distinct from the question of their existence.

Modelling infrastructures as a dependency graph with convergence nodes, rather than as independent sectoral chains, changes the nature of resilience analysis. In this graph, an upstream node inherits the resilience requirements of all downstream services that depend on it: the allocation of investments follows the graph, not the sectoral classification. The corollary is that every function situated on the critical restoration path of a vital function inherits the resilience requirements of that function, regardless of its own sectoral classification. The Texas case concretely illustrates this principle: gas infrastructure had not been identified by the power grid operator as critical loads to be kept active as a priority during load shedding, even though they supplied the generation plants on which production restoration depended. The load shedding of gas infrastructure worsened the very outage it was intended to contain.

4.2 - Projection onto existing regulatory frameworks

The partition of these frameworks reproduces the topology that preceded digital unification: co-existing systems, coupled at identifiable points, whose resilience could be assessed sector by sector. The gap documented in this section is a gap of topology. The instruments assess entities and sectors, while propagation operates on a graph whose edges cross their perimeters.

The CER and NIS2 frameworks individually cover the physical resilience and cybersecurity of critical entities with a significant degree of granularity: risk analysis, resilience plans, incident notification, supply chain security. CER requires critical entities to take into account their dependencies on other sectors in their risk assessments. NIS2 opens the possibility for Member

DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

States to designate as an essential entity an entity having specific importance for other interdependent sectors (Article 2(2)(e)), which allows for the constitution of critical dependency chains within its scope.

By contrast, CER explicitly excludes from its scope matters covered by NIS2 (Article 1(2)) and prescribes their coordination through a provision of principle whose implementation is left to each Member State. Classification remains sectoral and assessment is conducted at entity level, without consideration of the dependency graph. The NIS2 cross-sector designation mechanism is discretionary and does not rest on any systematic mapping. Projecting each case study documented in this note against the regulatory frameworks makes visible what falls into the gap between their respective perimeters.

The same limitation affects the supply chain provisions. Article 21(2)(d) of NIS2 requires entities to address the security aspects of their relationships with their direct suppliers and service providers, and Article 21(3) directs them to weigh the vulnerabilities specific to each of those suppliers and the overall quality of their practices[82]. The obligation runs along each bilateral link and is discharged in full by an entity that has assessed every supplier it contracts with. Nothing in it requires any party to observe that a large number of entities across unrelated sectors depend on the same supplier. Article 22 opens the only systemic tier, allowing the Cooperation Group, together with the Commission and ENISA, to conduct coordinated security risk assessments of critical ICT supply chains. That tier is a faculty rather than an obligation, it is scoped to categories of services, systems or products identified by the Commission, and it carries no supervisory power over any provider it examines. Concentration on a shared node is therefore an object that neither provision makes any party responsible for observing.

During the Iberian power outage, the physical failure of the transmission network falls under the CER perimeter. The information systems of grid operators fall under NIS2. The cascade by which the simultaneous loss of electricity and telecommunications deprived emergency services of their coordination tools, degraded access to gas stations and traffic lights, and propagated effects to hospital services through digital records, escapes as a phenomenon of cross-sector propagation the perimeter of both instruments. Each downstream sector individually falls under one or the other; the cascade itself falls into the gap.

The Texas case presents the same characteristic. Gas infrastructure had not been identified as critical loads in load shedding plans. The sectoral resilience of each network taken in isolation was addressed but the cross-sector mapping of dependencies was lacking, and the entities responsible for the electricity sector had no visibility over the gas dependencies on which their own restoration depended.

The most notable cyber-kinetic attacks against the Ukrainian power grid (2015, 2016, 2022) illustrate the clearest case: a cyber attack falling under the NIS2 perimeter and producing a physical failure falling under the CER perimeter, the coupling between the two being the very mechanism of the attack. Coordination between the two frameworks is prescribed by provisions of principle in each of them but is not tested as a propagation vector in any publicly documented exercise, to the author's knowledge.

The Digital Substrate of Cascading Failures : Cross-Sector Propagation in European Critical Infrastructure. Nicolas Roux, roux.nse@proton.me, August 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

The M.E.Doc and Change Healthcare cascades expose a third type of gap. In both, the failing node is a digital intermediary shared by entities that have no other connection to one another: an accounting package used across Ukrainian business in 2017, a transaction clearing service used across American healthcare in 2024. Each downstream entity held a bilateral relationship with that intermediary, and the supply chain provisions described above address precisely that relationship. What produced the cascade was the number of such relationships converging on a single node, a property visible from no individual entity's position and belonging to no sector.

European law does contain a mechanism built for this property. Articles 31 to 44 of DORA allow the European Supervisory Authorities to designate an ICT third party as critical for the financial sector, to appoint a Lead Overseer for it, and to exercise powers of information, investigation and inspection directly over a provider that is not itself a regulated entity[83]. The designation criteria include the systemic impact of a failure of the provider and the degree to which it can be substituted, which is a concentration test conducted at Union level. The first list of designated providers was published in 2025. The supervisory model therefore exists and operates. Its perimeter is the financial sector, and the position that Change Healthcare occupied in the American healthcare billing chain has no equivalent designation mechanism in any other sector, in the Union or elsewhere. The cascade crossed a boundary that the instruments draw between sectors, at a node whose criticality derives from the number of sectors it serves.

National instruments show the same partition. In France, the Interministerial General Directive 320 of 23 January 2023, which sets the framework for defence and national security planning across ministries, offers a reading of this cross-cutting dimension through a matrix crossing major crisis factors with the key activities constituting the centres of gravity of the Nation. Its "Response Strategy" section provides, however, that the implementation of each lever falls under the sole responsibility of the lead ministry.[84] Cross-cutting analysis features in the risk matrix and is absent from the prescriptive section of the directive, which remains sectoral and siloed. The instrument is cited here as one national illustration among twenty-seven, and what it illustrates is that a framing by vital functions can coexist with an execution framed by sector.

Above this regulatory layer, political recognition of the phenomenon is now established at the European level. The Niinistö report recommends a comprehensive preparedness approach covering all risks inspired by Nordic models and explicitly identifies cascading crises: it proposes the transformation of the Emergency Response Coordination Centre (ERCC) into a cross-cutting crisis centre serving as a single point of entry for major cross-border and cascading crises, as well as better articulation between political and technical levels through the IPCR arrangements. The Preparedness Union strategy translates these orientations into thirty actions, including the regular conduct of comprehensive Union-wide preparedness exercises. These texts establish at the political level the observation that the present note documents, going so far as to name cascades as an object of coordination. The proposed treatment, however, bears on response: the envisaged crisis centre coordinates the management of an ongoing cascade, and the announced exercises target decision-making and coordination. No public methodology defines to date, to the author's knowledge, the criteria for testing cross-sector propagation ex ante, its feedback loops or the neutralization of containment mechanisms. This absence of tooling contrasts with the maturity of the research: the

DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

modelling and simulation of interdependent infrastructures constitute an established field, whose reference review distinguished six families of approaches as early as 2014.[85] The analytical knowledge exists, but its transfer into frameworks and exercises as an evaluation object has yet to occur. The gap between recognition and treatment, documented in the introduction for technical exercises, is thus found at the political level in a precise form: the cascade is constituted as an object of crisis management, not yet as an object of evaluation. The criteria proposed in section 4.3 are situated in this gap.

The reading of dependencies proposed in the present note does not therefore claim to substitute for existing frameworks on their own perimeter. Its intended contribution is to make visible what none of them takes as its object, which is the mechanism of cross-sector propagation itself. The gap between the topology these frameworks presuppose and the topology the documented cases reveal widens with each newly digitized function.

4.3 - Evaluation criteria derived from documented cases

The anatomy of propagation described in this note allows the formulation of questions to which a cross-sector stress testing exercise should be able to respond. These questions derive from the failure modes identified in the cases studied in the present note and from their propagation through the dependency graph described in section 1. These criteria assert that an exercise or a resilience plan is better for satisfying it, and each assertion rests on a documented case in which the absence of the property contributed to a cascade or to the failure of a containment mechanism. Two limits follow. This note proposes no change to the instruments examined in section 4.2, since assessing their sufficiency would require access to their application. And it does not translate these criteria into exercise design, since the exercises concerned are in large part not publicly documented. What it does is make explicit what each criterion implies, so that a reader holding that documentation can determine whether the condition is already met. The formulation of the answers is theirs.

Criteria bearing on the scenario:

- Does the scenario test causal propagation between at least two interdependent sectors, rather than each sector in isolation? What to check is whether the second sector fails because the first did, or because the scenario declared it. In Texas in 2021, load shedding cut power to the gas facilities supplying the generation plants, which deepened the shedding. A scenario declaring gas and electricity down at hour zero exercises the response to a double outage and leaves the loop that produced it untested.
- Does the scenario cover the convergence of multiple failing upstream nodes towards the same downstream services? What to check is each fallback available to the downstream service, and whether its own dependencies appear among the nodes the scenario has already brought down. Iberian emergency services lost their coordination tools and the telecommunications carrying them to a single upstream failure.
- Does the scenario integrate the temporal dimension of cascades, that is to say the speed of propagation, the available intervention window and the duration beyond which degradation

DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

becomes difficult to reverse? The duration of an outage cannot be known while it lasts, which makes it unusable as a design target for a bounded reserve. The measurable quantity is the time a replenishment takes under the conditions of the crisis. For an Iberian hospital generator, that is the time to reach a decision, taken by people who may be unable to convene, on incomplete information and against competing priorities, followed by the time to complete a fuel delivery over dead traffic lights, disorganised traffic and filling stations whose card payment depends on the same telecommunications that are down. A reserve is dimensioned when its runtime exceeds that.

- Does the scenario include an "escalating failure," a degraded initial condition in which a sector is already weakened when the trigger occurs? What to check is that the prior degradation is independent of the trigger, since a condition the trigger itself produces is a phase of the same event, and that it bears on response capacity rather than on infrastructure alone. CERT-UA reports cyberattacks observed in advance of missile strikes: when the strikes arrive, the alert systems and the teams are already degraded.
- Does the scenario test propagation beyond the national or jurisdictional perimeter of the assessed entity? What to check is the direction. A foreign event reaching the assessed entity is the case usually simulated; the assessed entity acting as the vector towards others is the case rarely tested. The Viasat attack targeted an operator serving Ukraine and left 5,800 wind turbines in Germany without supervision, along with residential connections in five other European countries.

Criteria bearing on containment mechanisms:

- Are the mechanisms identified in section 3.1 (separation, degraded-mode architecture, local redundancy, replication, substitution) themselves subjected to the stress of the scenario? What to check is whether the exercise requires a result or accepts a declaration. In the case cited in section 3.1.2, backups sold as physically isolated sat in the same building as the server they protected, and the isolation was presumed from the contract until a fire disproved it.
- Does the scenario provide for the neutralization of the containment mechanism itself, such as the destruction of the backup system, the silent failure of the alarm system, or the feedback loop preventing restoration? Targeting, under-dimensioning and third-party unavailability can be injected once the exercise is under way. Silent failure has to be built in beforehand, since participants must be shown a plausible false reading rather than an instrument that stops. In 2003, FirstEnergy operators watched a stable grid for over an hour while transmission lines failed in succession.
- Does the containment mechanism depend on an actor whose cooperation is revocable, and if so, does that actor fall under a jurisdiction allowing this cooperation to be compelled? Where cooperation can be compelled, the legal route carries a delay, measured against the same interval as the criterion on temporal dimensioning above. What to check is whether that delay has been measured or assumed. Infrastructure sharing between Ukrainian

DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

operators after the Kyivstar attack and the substitution by Starlink after Viasat illustrate the two positions.

- Has the organization demonstrated, under scenario conditions, the capacity to activate the containment mechanism? Two things are observable without any incident history: whether the exercise runs on the tools the scenario leaves standing, and whether the person activating the mechanism is the one who would be reachable in fact rather than the designated holder of the role. No Iberian region had a continuity plan for a prolonged outage affecting emergency medical services: the generators existed, and what had never been tested was whether their runtime matched what the services depending on them required. What such an exercise measures is preparation, and the question of what a realistic test of competence looks like in an organization with no incident history remains open.
- Does the activation of the mechanism depend on a detection or orchestration layer, and is that layer included in the scope of the scenario? What to check is a list of the mechanisms in scope alongside what triggers each one: any trigger appearing twice is a shared dependency that no dependency map declares. An automatic failover depending on a monitoring system fails with it and leaves the redundant capacity available and unused.

4.4 - Open questions

The empirical evidence and evaluative framework of this note bring to light three questions that exceed its scope. These questions pertain to the field studied, in its architectures, its frameworks and its doctrines, and not to the methodological limitations of the present analysis, which establishes their relevance without answering them.[86]

The first concerns the architecture of critical systems. The documented cases show that systems designed for nominal operation lose their usefulness when their dependencies (connectivity, electricity) are interrupted. The inverse approach, designing the systems on which the continuity of vital functions depends for degraded-mode operation and on communications independent of network transport, constitutes an identified line of work.

The second concerns the absence of a bilateral digital continuity framework between Member States. Union law already practises, in the energy sector, the articulation between the common tier and the bilateral tier: the gas solidarity mechanism of Regulation (EU) 2017/1938 rests on bilateral agreements between Member States for its technical, legal and financial modalities,[87] and default rules were introduced in 2024[88] to cover cases where such agreements have not been concluded.[89] Nordic cooperation proceeds from the same architecture: the Haga declarations have organized civil preparedness among Nordic countries since 2009, in explicit articulation with Union and NATO initiatives.[90] To the author's knowledge at the time of writing, no bilateral agreement between Member States covers the continuity of digital services in a crisis context, and the initiatives stemming from the Niinistö report and the Preparedness Union strategy bear on the coordination of the response at Union scale. A bilateral layer would complement this common tier, as in the two domains cited, and would reduce its criticality as a single coordination gateway, following the divergence logic described in section 1. The cross-border propagations documented in this note illustrate the need.

The Digital Substrate of Cascading Failures : Cross-Sector Propagation in European Critical Infrastructure. Nicolas Roux, roux.nse@proton.me, August 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

The third concerns the allocation of resilience effort across the graph. Section 4.1 establishes that resilience requirements are transmitted by inheritance: an upstream node inherits those of all downstream services that depend on it, and every function on the critical restoration path of a vital function inherits those of that function. The reinforcement of nodes where these inherited requirements concentrate follows directly from this logic. This "critical nodes" approach does not, however, suffice on its own: the intrinsic opacity of intelligence on adversarial intentions and capabilities, combined with the documented property of cascades to propagate through the weakest link of the graph, implies that beyond a certain point the marginal value of additional reinforcement of an already hardened node becomes lower than that of eliminating a known vulnerability on a weak node. Allocation therefore follows the graph in both its dimensions: the concentration of inherited requirements, which identifies the nodes to harden, and the path of least resistance, which calls for raising the baseline across the whole. The adjudication of this trade-off, in particular the location of the tipping point between the two, exceeds the scope of this note.

Two considerations shed light on the baseline-raising component. The first pertains to temporality: a coherent raising of the baseline is built over years or decades, whereas a threat can emerge and activate within months. A resilience framework conditional on the prior identification of the threat therefore potentially arrives too late. Its robustness requires it to be permanent and agnostic as to the trigger's nature, a property that the cases documented in this note confirm, with the same cascades being activated indifferently by meteorological events, internal failures or attacks. The second pertains to the value of investments under uncertainty: the literature on robust decision-making in climate adaptation establishes that measures producing benefits across a broad range of scenarios, including in the absence of a crisis, dominate measures whose value is conditional on the materialization of a specific scenario.[91] The Nordic total defense models (Finnish kokonaisturvallisuus,[92] Swedish totalförsvar[93]) rest on this dual logic of permanence and systematic baseline elevation, integrating the full range of actors (administrations, businesses, organizations and citizens) into the resilience framework. This orientation finds convergence in the operational strategy declared by the competent French authority on cybersecurity (ANSSI), whose director general Vincent Strubel states the focus as aiming to raise the general security level in order to reduce the volume of successful attacks.[94]

Conclusion

The infrastructures on which the vital functions of European societies depend used to form co-existing systems. Their digitization has turned them into a single dependency graph whose propagation properties are documented, recurring and indifferent to the trigger's nature. The containment mechanisms capable of interrupting these propagations exist and have proven themselves, but their existence says nothing about their resistance to targeting, their dimensioning against a disruption of unknown duration, the conditions of their availability, or the capacity of organizations to activate them. The regulatory frameworks and exercises that define resilience assessment today each cover their perimeter with coherence, but that coherence is the coherence of a sectoral partition which the digital substrate now runs straight through. The mechanism of cross-

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

sector propagation is the evaluation object of none of them, and the gap widens as the substrate extends.

This note offers the reader an instrument to bridge this gap: an evaluation grid of criteria derived from empirical evidence, applicable to existing instruments (frameworks and exercises), including those whose documentation is not public. Applying these criteria to existing exercises, plans and architectures is the responsibility of the actors who have both charge and access.

The adversaries who struck the infrastructures documented in this note had mapped the dependencies of their targets before acting, down to the mechanisms intended to contain failures. The dependency graph exists and produces its effects, whether or not evaluation frameworks take it as their object.

The Digital Substrate of Cascading Failures : Cross-Sector Propagation in European Critical Infrastructure. Nicolas Roux, roux.nse@proton.me, August 2026.
DOI: https://doi.org/10.5281/zenodo.21285147 - CC BY 4.0

Acknowledgements

The author thanks Vincent Giraud (IHEDN Chair on Digital Sovereignty and Cyber), Tim Clements (Purpose and Means, Copenhagen) and Christian Sommade (General Delegate, French High Committee for National Resilience) for their comments on earlier drafts of this note. Responsibility for its content rests solely with the author.

The Digital Substrate of Cascading Failures : Cross-Sector Propagation in European Critical Infrastructure. Nicolas Roux, roux.nse@proton.me, August 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 theolder 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 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

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." J Med Internet Res 2025;27:e71657. DOI: 10.2196/71657. https://www.jmir.org/2025/1/e71657

3 "Banking has fundamentally become an IT business." Montagner, P., "Information and Communications Technology resilience and reliability," speech at the Frankfurt Banking Summit (Fitch Ratings / PwC Strategy&), Frankfurt, 2 July 2025. 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, citing the ENTSO-E Ten-Year Network Development Plan. 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, April 2026. https://hai.stanford.edu/ai-index/2026-ai-index-report

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

7 Sendai Framework for Disaster Risk Reduction 2015–2030. https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030

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 European Commission, "Critical infrastructure resilience at EU-level," 13 January 2026. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

10 NATO, "Resilience, civil preparedness and Article 3," updated 13 November 2024. https://www.nato.int/en/what-we-do/deterrence-and-defense/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 European Commission and High Representative, 26 March 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 NATO Cooperative Cyber defense Centre of Excellence (CCDCOE), LS17 announcement. https://ccdcoe.org/news/2017/the-largest-international-technical-cyber-defense-exercise-launched-this-week/

14 United States Army, 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 February 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 (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities, Article 1(2), Official Journal of the European Union, L 333, 27.12.2022, pp. 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. 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 for 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 for 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. https://portalinvestigacion.uniovi.es/documentos/6987d95671f47e7e0ac0fab1?

lang=en
24 Konstantinoudis, G. & Riou, J. (2025), "Excess mortality attributable to the 2025 Iberian Peninsula blackout," excess mortality estimated at +167 deaths in Spain within two days of the outage (95% credibility interval: +28 to +300), medRxiv preprint (not peer-reviewed). 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 July 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) and 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 December 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 FERC press release, "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." NERC 2021–2022 Winter Reliability Assessment, February 2021 Cold Weather Event: Winter Storm Uri, p. 6. https://www.nerc.com/globalassets/programs/rapa/ra/nerc_wra_2021.pdf
30 Texas Department of State Health Services, December 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, September–October 2006. https://www.researchgate.net/publication/224686365_Overview_of_the_events_and_causes_of_the_2003_Italian_blackout
32 Sergey V. Buldyrev, Roni Parshani, Gerald Paul, H. Eugene Stanley, Shlomo Havlin, 15 April 2010, "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, pp. 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," April 2004, chapter 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), adapted by Jean Elyan, 6 July 2017, "Petya: La police ukrainienne saisit les PC de l'éditeur M.E.Doc" [Petya: Ukrainian police seizes M.E.Doc publisher's PCs]. Le Monde Informatique. 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 October 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 June 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), presentation at Black Hat Europe 2019. Reported by Tara Seals, Dark Reading, 11 December 2019. https://www.darkreading.com/cyber-risk/maersk-ciso-says-notpeyta-devastated-several-unnamed-us-firms
38 Juan Andrés Guerrero-Saade for 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," p. 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: the biggest threat to industrial control systems since Stuxnet." https://www.eset.com/industroyer/

42 CERT-UA H2 2024 Report, 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 January 2024. Citing the Solntsepek claim, the Vitiuk/SBU confirmation, and the CERT-UA report on the 11 operators. 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 December 2023, cited by 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 October 2022. https://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 April 2024. https://osw.waw.pl/en/publikacje/analyses/2024-04-17/russias-new-large-scale-attacks-ukraines-energy-infrastructure

49 HRMMU Report, September 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." https://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), testimony before the United States Congress, May 2024. Summary: 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 April 2024. https://www.congress.gov/crs-product/IN12330

54 AMA, "Physicians struggle to keep practices afloat after Change cyberattack," 10 April 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 February 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 January 2024: "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." https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/

57 Daryna Antoniuk, 4 January 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, 20 March 2026, "Grid Incident in Spain and Portugal on 28 April 2025," Final Report, p. 393, recommendations section: "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": "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 November 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 October 2024. https://developingtelecoms.com/telecom-technology/energy-sustainability/17551-kyivstar-starts-next-phase-of-network-backup-power-upgrades.html

62 Liam Maxwell (AWS), 29 November 2023, cited by 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 April 2022, official communiqué. https://privatbank.ua/en/news/2022/4/29/financial-safety-above-everything-privatbank-completed-migration-to-cloud

64 Deuxfleurs association, Garage, an S3-compatible distributed object storage software: "An S3 object store so reliable you can run it outside datacenters." Each chunk of data is replicated across three zones, over the public internet and on heterogeneous hardware, resilience to node, site and network failures being a design objective. The project has received funding from the European Commission's Next Generation Internet programme (NGI POINTER, grant agreement No 871528; NGI Zero Entrust, No 101069594; NGI Zero Commons, No 101135429). https://garagehq.deuxfleurs.fr/

65 *Tribunal de commerce de Lille Métropole*, judgment of 26 January 2023, France Bati Courtage v. OVH. Following the March 2021 fire at OVH's Strasbourg site, the court found the provider in breach of its automated backup offer: the backups had been stored in the same building as the customer's server, whereas the provider had undertaken that they would be physically isolated from the infrastructure hosting it. OVH was ordered to pay 93,000 euros in damages. The presumption of isolation rested here on the contractual commitment itself, in the absence of any verification of its effective implementation. Judgment (in French): https://www.legalis.net/jurisprudences/tribunal-de-commerce-de-lille-metropole-jugement-du-26-janvier-2023/

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

67 Victor Zhora, Deputy Chairman of the State Service of Special Communications and Information Protection of Ukraine, interview with Numerama: "We have been attacked since 2014. Ukrainian cyber defense has had time to learn and train through the attacks." [Translated from French.] 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," February 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 defense, health sovereignty, risk, and infrastructural dependency." Front Public Health. 2025 Jul 9;13:1630933. DOI: 10.3389/fpubh.2025.1630933. https://researchportal.ulisboa.pt/en/publications/when-the-lights-went-out-impacts-of-the-april-2025-iberian-blacko/

70 Joey Roulette, Cassell Bryan-Low and Tom Balmforth for Reuters, July 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," August 2025. https://oig.usaid.gov/node/7845

72 Sauli Niinistö, 30 October 2024, Safer Together, op. cit., section on hybrid threats and economic security, 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 "Requisitions for the needs of national defense and security," Book II of Part 2 of the French defense Code (Articles L2211-1 to L2212-11). https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071307/LEGISCTA000006151492/

74 Shalal, Andrea and Roulette, Joey for Reuters, 22 February 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, March 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, pp. 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), pp. 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 December 2021. https://www.rnbo.gov.ua/en/Diialnist/5170.html
80 Roux, N., European Digital Dependencies, op. cit.
81 VEON, 18 January 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 (EU) 2022/2555 (NIS2), Articles 21(2)(d), 21(3) and 22. Official Journal of the European Union, L 333, 27.12.2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
83 Regulation (EU) 2022/2554 (DORA), Articles 31 to 44, on the designation of critical ICT third-party service providers and the associated oversight framework. On the operation of the framework and the list of designated providers: European Banking Authority, "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 of 23 January 2023 on the planning of national defense and security. https://www.legifrance.gouv.fr/circulaire/id/45441
85 Ouyang, op. cit.
86 These three questions are the subject of ongoing work by the author.
87 Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010, Article 13, OJ L 280, 28.10.2017. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R1938
88 Regulation (EU) 2024/1789 (gas and hydrogen market package), presented in the EUR-Lex summary "Gas supply security in the EU." https://eur-lex.europa.eu/EN/legal-content/summary/gas-supply-security-in-the-eu.html - OJ L, 2024/1789, 15.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1789/oj
89 Council of the European Union, infographic "Gas market: measures to secure and share supply in the EU": six bilateral solidarity agreements concluded (Germany-Denmark, Finland-Estonia, Estonia-Latvia, Latvia-Lithuania, Germany-Austria, Italy-Slovenia) out of approximately forty expected under the 2017 regulation. https://www.consilium.europa.eu/en/infographics/gas-market-share-supply-eu/
90 Haga III Declaration, meeting of Nordic ministers responsible for civil protection and preparedness, 27–28 November 2024, in the continuity of the Haga I (2009) and Haga II (2013) declarations, providing to "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), pp. 240–247. https://doi.org/10.1016/j.gloenvcha.2008.12.003
92 Government of Finland, 16 January 2025, Security Strategy for Society. https://julkaisut.valtioneuvosto.fi/items/0126122a-1e8a-4ffa-9868-6286292efc01
93 Government of Sweden, 4 May 2026, The Strategic Environment and Planning Assumptions for Swedish Total defense 2025–2030. https://www.mcf.se/siteassets/dokument/publikationer/english-publications/the-strategic-environment-and-planning-assumptions-for-swedish-total-defense.pdf
94 Vincent Strubel, interviewed by Guillaume Belfiore for Clubic, 28 June 2026: "Our activity and our primary focus, today more than ever, is prevention. It is about raising the security level to limit the volume of attacks, at least those that succeed." [Translated from French.] https://www.clubic.com/dossier-618682-interview-anssi.html