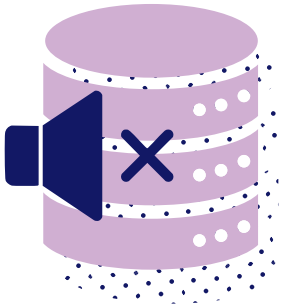
PROCHAIN ARRÊT

THE FORESIGHT SERIES BY KEOLIS



The silence of the servers

Cyberattack, blackout and the transport network

The Iberian precedent: 28 April 2025, 12:33

On 28 April 2025, at 12:33 local time, the Iberian electricity system blacked out. In the space of merely seconds, some 15 GW of generating capacity vanished from the grid — roughly 60% of demand at that moment. The peninsula automatically disconnected from the continental European network at 12:38. Spain, Portugal, Andorra and parts of south-west France experienced a major power cut lasting between ten and twenty hours depending on the area. The official human toll stood at seven deaths in Spain and one in Portugal, with more than 25 injured — this in an episode where the simultaneous shutdown of metros, trains, traffic lights, ATMs and telecommunications networks had paralysed the entire peninsula.

Successive reports from the expert group commissioned by ENTSO-E, ACER and national regulators conclude that there was no single cause: it was not a cyberattack, contrary to the rumours that circulated at first. It was a chain of technical failures — insufficiently effective voltage regulation, poor coordination between actors, badly configured protection systems — that could have been contained and was not. The event remains, regardless of its causes, the biggest European blackout of the past twenty years. It reveals a vulnerability that cybersecurity had largely masked until now: a highly digitalised transport network can fail without any help from a hacker. And it could be worse if someone decided to help it along.

Public transport as critical infrastructure

Modern public transport networks are stacks of information technology. IP-based signalling, remote supervision, cloud-based ticketing, contactless payment, passenger apps, traction energy management, passenger counting, video surveillance, depot management, bus geolocation, driver communications: every link in the chain depends on an IP network, servers, third-party APIs and external service providers. The EU NIS2 Directive (transposed into French law in October 2024) extended the status of operator of vital importance (OIV) or operator of essential services (OSE) to a much larger share of transport actors. This entails audit obligations, incident reporting to the national information system security agency ANSSI, and penalties for non-compliance. This status acknowledges a reality: if a major city's metro stops running, it is a public security incident.

There are an increasing number of attacks on transport networks, and here, the Polish incident of August 2023 is enlightening. Pro-Russian hacktivists disrupted a significant portion of the Polish rail network without any sophisticated ransomware, simply by exploiting an unsecured analogue VHF communications system and broadcasting emergency stop signals accompanied by excerpts from Vladimir Putin's speeches. The most emblematic attack remains NotPetya in June 2017: malware initially targeted at Ukraine that within hours paralysed banks and transport in Kyiv, then spread globally to companies including Maersk, Saint-Gobain and SNCF (causing collateral damage to certain computer systems). WannaCry in May 2017 had previously struck Telefónica in Spain and the British NHS, demonstrating that malware exploiting an unpatched Windows vulnerability could paralyse essential services within hours.

Recent figures offer cause for concern. According to ENISA analyses and sectoral reports, ransomware targeting the railway sector rose from 13% to 25% of all threats against that sector between 2021 and 2022 — almost a doubling in a single year. In France, ANSSI recorded 144 reported ransomware compromises in 2024, a level stable relative to 2023 but structurally high. The first quarter of 2025 saw an increase of 126% in the number of victims claimed by ransomware groups compared with Q1 2024 (Checkpoint report). The human factor remains the primary entry point: 82% of security officers (Proofpoint, 2024) regard human error — clicking on a booby-trapped link, using a shared password, failing to revoke access — as the leading vulnerability.

The cyber + blackout combo: a credible scenario

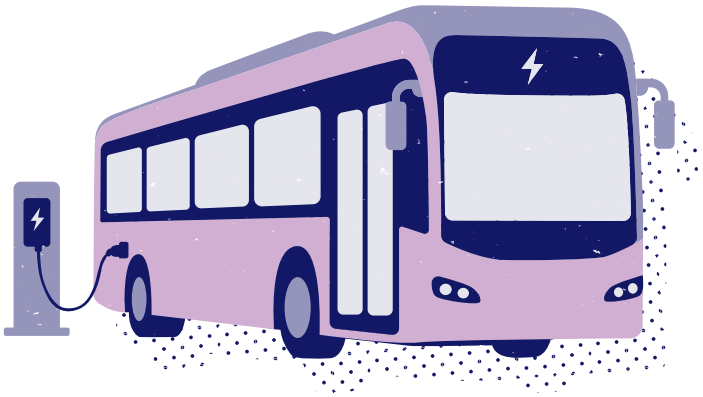
The scenario that most concerns national and European authorities is not that of an isolated cyberattack, nor that of a straightforward blackout. It is the combination of the two. A targeted cyberattack can trigger a localised or regional blackout, and conversely, a blackout can create a window of opportunity for an attack on systems operating in degraded mode and therefore less well defended. The available examples are few but striking: the attacks against Ukrenergo in December 2015 and December 2016 demonstrated that a patient attacker could penetrate the control system of an electricity operator, manually disconnect substations remotely and leave hundreds of thousands of homes in darkness for several hours. These attacks are attributed to the Russian group Sandworm and remain to this day the only documented cyberattacks to have caused a deliberate blackout.

For a public transport operator dependent on both power supply and IT systems, the combination is devastating. Without power: rail vehicles stop, electric buses cease to function once their battery reserves are depleted, traffic lights go down, lifts and escalators are stuck, tunnel ventilation stops. Without IT systems, emergency manual signalling is possible but drastically reduces service frequency; ticketing fails (free travel imposed by default, or checks impossible); passengers lose all real-time information; drivers lose contact with their controllers; surveillance cameras go dark. Both simultaneously: a complete service collapse, with a major safety risk for passengers trapped in underground tunnels, lifts or rolling stock without ventilation.

Looking ahead to 2044: accepted hyper-dependency

In 2044, the dependency of transport networks on computing and electricity will only have grown. The phasing out of diesel buses by around 2035 in most large French conurbations transforms electricity from a partial dependency into a total one. The widespread adoption of biometric payment, autonomous shuttles and algorithmic fleet supervision adds further layers of digital dependency. Public operators become targets for states (cyberwarfare, destabilisation), criminal groups (ransomware, extortion), hacktivists (political demands), and disgruntled insiders (sabotage). The attack surface multiplies with every API opened to a third-party provider.

Three consequences result from this. First, the cost of resilience becomes structural: redundancies must be funded — alternative power paths, off-cloud mirror servers, manually exercisable degraded modes — that are useful only in a crisis. This is expenditure that does not generate a single additional passenger journey. Second, cybersecurity expertise becomes a rare and critical asset: operators compete for a limited pool of qualified SOC (Security Operations Centre) analysts, with salaries rising sharply. Finally, the question of civil and criminal liability arises with every incident: who pays when a passenger dies in a tunnel following an unclaimed cyberattack? The operator, the transport authority, the state, the software vendor? Concession contracts will need to incorporate such clauses, failing which private operators may gradually withdraw from the most exposed contracts.



The story

Friday 24 June, 14:03

Lyon, june 2044

Jodie Vermeer had been staring at her main screen for fourteen seconds without blinking. Three processes had just gone down simultaneously on the supervision console for the Lyon conurbation's tram network. That in itself was not abnormal. What was abnormal was that the three failed processes were not located on the same server, nor on the same rack, nor in the same building. The first was at Lyon-Confluence, the second in the Vénissieux data centre, the third on the sovereign cloud hosted in Strasbourg. Three different physical locations. Three simultaneous failures. Statistically, impossible.

She was thirty-one and had been working for four years at the Keolis Lyon Security Operations Centre, in the basement of a commercial building in the Part-Dieu district. The windowless open-plan office, air-conditioned to 22 °C throughout the summer, hummed with the steady drone of the server racks lined up behind the glass partition. Six analysts on shift that Friday 24 June, from a team of fourteen. Outside, Lyon was registering 42 °C — a class 4 heatwave that had begun on Tuesday. Friday afternoon, July just around the corner, school holidays underway: the network was at that moment carrying around 80,000 passengers per hour off-peak, a figure that typically rose to 220,000 at the evening rush.

At 14:04, the fourth process went down. Contactless ticketing supervision across the entire bus network. At 14:05, the fifth: power supply management for the three tram lines. Jodie immediately dialled the number of Vincent Roca, director of operations. He picked up on the second ring. "Vincent. We've got something. Five critical systems down in two minutes, across three different sites. This is not a coincidence." Vincent asked how many. "Five for now. But it's climbing."

At 14:07, the alert screen flashed red: on the internal application, a short message had appeared. Not in the mailbox, not in the secure messaging system. Directly on the system notification banner — something technically impossible in a properly segmented infrastructure. The message was four words long: "First lesson. Signed: Mirror."

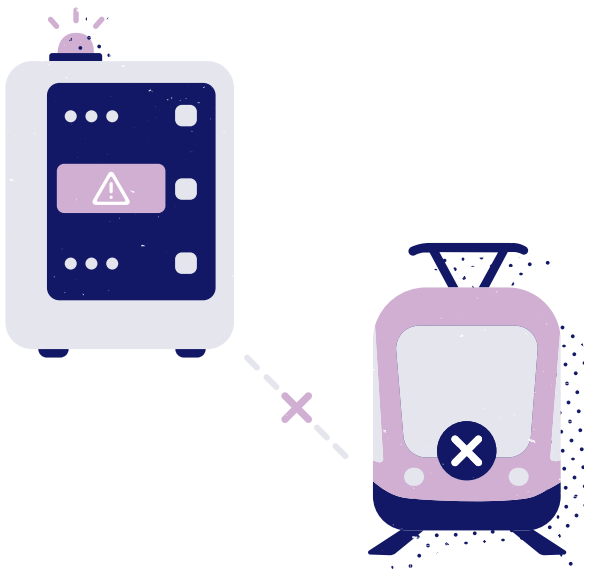
Jodie read it, then read it again. Then she picked up her phone again and called Anthony Schroeder. Anthony was fifty-eight, with twenty-two years at ANSSI behind him, seven of them in the technical division, and had been consulting for Keolis since 2041, two days a week, from his home in Villeurbanne. He had designed the current cyber crisis plan. He picked up on the first ring. "Jodie." She said: "Anthony. We have an attacker signing as Mirror. Five systems down in four minutes. A direct system notification on the internal screens."

A long silence at the other end. Then Anthony, in a low voice: "I'm on my way. Thirty minutes by motorbike. Don't touch anything except the level-1 defensive playbooks. Above all, no physical disconnection before I get there."

At 14:12, the Confluence control centre lost its air conditioning. Not the power — the air conditioning alone. But within ten minutes the temperature in the server room would climb from 22 to 35 degrees, and above 40 the machines would automatically shut down in protective mode. Jodie realised this when she looked at the environmental monitoring screen: everything had been calculated. The attacker did not want to cut the power abruptly. He wanted the servers to shut themselves down from overheating, in protected mode, preserving the logs. An elegant attack. An attack by heat. An attack that hated its victims enough to give them time to watch it coming.

At 14:18, the first passenger called the contact centre. An elderly lady, Bellecour station, stranded in a T1 tram that had been standing at the stop for ten minutes, air conditioning off, doors open, with no word from the driver. At 14:21, the second: a man in Vaulx-en-Velin stuck in an electric bus that had lost all power, stranded in the bus lane, driver requesting an evacuation. By 14:25, the contact centre was saturated. At 14:29, Jodie's phone emitted a sharp whistle and froze. The 6G network was overloaded. By 14:30, no calls were getting out of the building.

Anthony arrived at 14:34, helmet under his arm, his face ashen. He glanced at the screens, the log console, the message "First lesson. Signed: Mirror." And uttered, sotto voce, to no one in particular: "Fuck."



Vincent Roca burst into the room at 14:36. He had run down from the 12th floor by the stairs — the lifts were out. He was sweating. “Situation?” Jodie: “Eleven systems down. Trams stopped on all three lines. Electric buses 60% halted through loss of supervision. Ticketing inoperative. Contact centres saturated. Outgoing phones cut. Control room air conditioning progressively failing. CCTV: we’re losing feeds one by one. And there is a hacker attacker who has identified himself.” Vincent: “Sandworm? Lockbit? Cl0p?” Anthony, calmly: “No. None of those. This is someone I know.”

He sat down at Jodie’s console, asked for the logs, and studied them for two minutes in silence. Then he said: “Mirror is a signature I saw three times between 2032 and 2035 at ANSSI. Three attacks against European transport operators — Lisbon, Düsseldorf, Naples. Each time: no responsibility claimed, never any ransom demanded, never any communication. Just a short message at the end. In Lisbon in 2033 it was: you had not listened. In Düsseldorf in 2034: you had not seen. In Naples in 2035: you had not understood. We never identified the perpetrator. The profiling suggested someone who had worked in offensive cybersecurity, who was bored or playing a game. Not a state actor, not a cybercriminal. Someone who wanted to teach us something.”Jodie: “Teach us what?” Anthony looked at her. “That we are not ready. And that no amount of regulation will make us ready if we continue to think this is a technical problem.”

At 14:51, the SOC lighting switched to emergency power. The white LEDs turned red. The hum of the servers behind the glass partition shifted in pitch, dropped an octave, then began to pulse in bursts. A smell of warm plastic began to rise from the raised floor. Vincent ordered all non-critical teams to evacuate the building. Jodie, Anthony, and two other analysts stayed. The main room’s air conditioning gave out at 14:58. The temperature began to rise by one degree every four minutes.

At 15:12, the preliminary evacuation report came back from the network: an elderly passenger had died at Saxe-Gambetta station, apparently from a heat-related heart attack in a train that was at a standstill with its doors closed (the driver, in shock, had forgotten the manual door-opening override). A pregnant woman had been evacuated from a line C7 bus by emergency services for an urgent Caesarean. Forty-seven passengers were trapped in a lift between two levels at Vieux-Lyon station, their cries audible in the shaft through the still-active audio sensors. Anthony read the report, looked up, and said quietly to Jodie: “First lesson.”

At 16:22, using an emergency analogue radio channel (purchased three years earlier at Anthony’s insistence, against the advice of financial management), they managed to coordinate with SNCF Réseau and Enedis on a manual re-segmentation strategy. At 17:47, the first tram restarted on line T2, in secure manual mode, speed limited to 15 km/h, without centralised signalling, driving on sight. By 21:15, the bus network was running at 35% of normal capacity. The metro remained entirely shut down. Ticketing would remain inoperative for six weeks: everyone would travel free, by default.

The internal report drawn up on Monday 27 June put the human toll at three deaths — the man from Saxe-Gambetta, plus two people who died of heat stroke in poorly ventilated metro tunnels, whose bodies were not found until Saturday morning. There were forty-seven direct casualties, of whom eighteen were serious. The direct financial cost was estimated at €47 million for the operator, not counting losses for Lyon businesses (estimated at between €80 and €120 million), compensation payments that would be spread over years, and the costs of rebuilding the cyber infrastructure (estimated at €30 million over eighteen months). Mirror never made itself known in Lyon again. Anthony Schroeder resigned from his consultancy contract on 1 September 2044, without public explanation. Jodie Vermeer still holds her post at the SOC.

The silence of the servers, that Friday 24 June at 14:03, had lasted exactly nine seconds before Jodie noticed it. Nobody had heard the servers go quiet. Nobody ever would.

Three forward-looking scenarios

WHITE SCÉNARIO

Institutionalised resilience

In the optimistic scenario, the 2030s are a decade of widespread awakening. Transport operators have been recognised as operators of vital importance across Europe, with strict obligations for annual audit, penetration testing, redundancy, and exercisable continuity plans. Public transport authorities explicitly fund cyber resilience in contracts, with a dedicated envelope representing 4 to 6% of operators' IT budgets. Shared SOC centres across operators (Keolis, Transdev, SNCF, RATP Dev, etc., in sectoral consortia) become the norm, sharing threat intelligence and indicators of compromise in real time. Degraded modes are regularly exercised, including through planned multi-hour outages under real conditions. Attacks continue — they do not disappear — but they can no longer paralyse a network for more than a few hours, and they no longer cause human casualties. Cybersecurity becomes just another profession in public transport, with its own career paths, training and unions.

GRAY SCÉNARIO

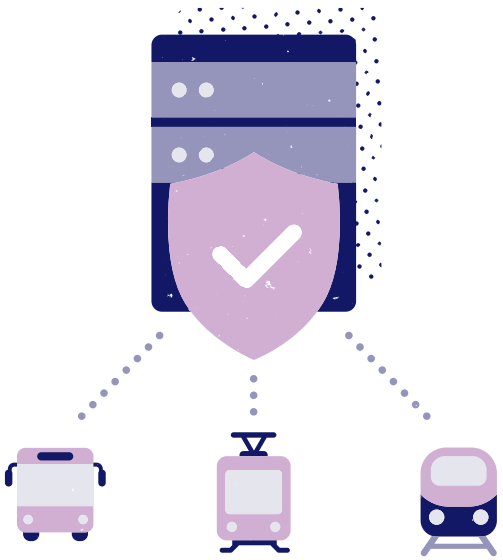
Vulnerability managed case-by-case

In the intermediate trajectory, cybersecurity remains a serious but under-funded issue. Operators invest what they can — that is, what their contracts allow — which is often insufficient. Attacks multiply: five to ten per year in France affecting the transport sector, with one or two paralysing an urban network for 48 to 72 hours. Human casualties remain rare but not zero: one to three deaths per year at national level on average, in combined cyber and operational degradation incidents. The state tightens regulation after each major crisis, without budgets truly following. Cyber insurance becomes prohibitive or withdraws from the sector. Operators learn to live with a level of risk that none would have accepted ten years earlier, for want of any alternative.

BLACK SCÉNARIO

The network remotely dismantlable

In the pessimistic scenario, the combined cyber + blackout scenario becomes the weapon of choice in hybrid conflicts. By 2044, one major European conurbation every year suffers a significant attack that brings the entire network to a halt for more than 24 hours. Deaths run into the dozens per incident in the worst cases (heatwave + tunnel + ventilation shutdown). Wealthier passengers durably turn away from public transport, perceiving it as exposed and unpredictable. Private autonomous pods, perceived as less vulnerable (wrongly, but perception is enough), capture a growing share of journeys. Public operators become unsaleable to private actors, who withdraw one by one from tender processes. Public transport authorities find themselves directly operating, without cyber expertise and without financial capacity, networks that are permanent targets. The geopolitics of cybersecurity becomes a matter of national sovereignty — but also a structural factor in urban quality of life. The social contract of public transport — universal, reliable, safe — unravels under the effect of attacks that no one claims and no state can deter.



Sources

ENTSO-E, Factual Report on the Grid Incident in Spain and Portugal on 28 April 2025, 3 October 2025; final report identifying root causes, 20 March 2026.

RTE, Foire aux questions : black-out du 28 avril 2025 sur la péninsule ibérique, updated 25 March 2026.

Red Eléctrica de España (REE), official statement of the Spanish government dated 17 June 2025 on the causes of the 28 April 2025 blackout.

Sfen, «28 semaines plus tard, premières réponses sur le blackout ibérique», October 2025.

ENISA, Threat Landscape 2024, European Union Agency for Cybersecurity, June 2024.

ANSSI, Panorama de la cybermenace 2024, Agence nationale de la sécurité des systèmes d'information, 2025 .

Checkpoint Software Technologies, Cyber Security Report Q1 2025.

Proofpoint, Voice of the CISO 2024 Report.

Directive (EU) 2022/2555 (NIS2) of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, transposed into French law in October 2024.

Cybermalveillance.gouv.fr, Annual Activity Report 2024 and 2025, GIP ACYMA.

Zataz, "Hacktivistes pro-russes : paralysie d'une partie du réseau ferré polonais", August 2023.

Greenberg, A., Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, Doubleday, 2019 (on the Ukrenergo 2015–2016 attacks and NotPetya 2017).

Bodet-Time, "Les enjeux d'une cyberattaque dans le secteur des transports", 2025

LeMagIT, "Ransomware : 2025, l'année de la reprise en France", 2026.

Formind, Panorama de la menace cyber : premier semestre 2025, October 2025.

Harris, T., The Silence of the Lambs, St. Martin's Press, 1988