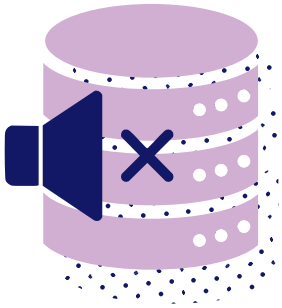
PROCHAIN ARRÊT

LA SÉRIE PROSPECTIVE DE KEOLIS



Le silence des serveurs

Cyberattaque, blackout et réseau de transport

Le précédent ibérique : 28 avril 2025, 12 h 33

Le 28 avril 2025, à 12 h 33 heure locale, le système électrique ibérique s'effondre. En quelques secondes, environ 15 GW de production électrique disparaissent du réseau — soit près de 60 % de la demande à cet instant. La péninsule se déconnecte automatiquement du réseau européen continental à 12 h 38. L'Espagne, le Portugal, l'Andorre et certaines régions du sud-ouest de la France connaissent une panne de courant majeure, qui dure entre dix et vingt heures selon les zones. Le bilan humain officiel s'établit à sept morts en Espagne et un au Portugal, plus de vingt-cinq blessés, dans un contexte où l'arrêt simultané des métros, des trains, des feux de signalisation, des distributeurs automatiques et des réseaux de télécommunications a paralysé toute la péninsule.

Les rapports successifs du groupe d'experts mandaté par ENTSO-E, l'ACER et les régulateurs nationaux concluent à l'absence de cause unique : ce n'est pas une cyberattaque, contrairement à la rumeur des premières heures. C'est un enchaînement de défaillances techniques — réglage de la tension insuffisamment efficace, mauvaise coordination entre acteurs, protections mal paramétrées —, qui aurait pu être contenu et qui ne l'a pas été. L'événement reste, indépendamment de ses causes, le plus important blackout européen des vingt dernières années. Il révèle une vulnérabilité que la cybersécurité avait jusque-là largement masquée : un réseau de transport hyper-numérisé peut tomber sans qu'aucun attaquant n'ait à faire quoi que ce soit. A fortiori si quelqu'un décide de l'aider à tomber.

Le transport public, infrastructure critique

Les réseaux de transport public modernes sont des empilements d'informatique. Signalisation IP, supervision à distance, billettique cloud, paiement dématérialisé, applications voyageurs, gestion de l'énergie de traction, comptage des passagers, vidéosurveillance, gestion des dépôts, géolocalisation des bus, communication avec les conducteurs : chaque maillon dépend d'un réseau IP, de serveurs, d'API tierces, de prestataires externes. La directive européenne NIS2 (transposée en France en octobre 2024) a élargi la qualification d'opérateur d'importance vitale (OIV) ou d'opérateur de services essentiels (OSE) à une part beaucoup plus grande des acteurs du transport. Cela signifie obligations d'audit, signalement des incidents à l'ANSSI, sanctions en cas de manquement. Le statut reconnaît une réalité : si le métro d'une grande ville s'arrête, c'est un événement de sécurité publique.

Les attaques se multiplient. L'incident polonais d'août 2023 est éclairant : des hacktivistes pro-russes ont paralysé une partie significative du réseau ferré polonais sans aucun ransomware sophistiqué, simplement en exploitant un système de communication VHF analogique non sécurisé, et en y diffusant des signaux d'arrêt d'urgence accompagnés d'extraits de discours de Vladimir Poutine. L'attaque la plus emblématique reste NotPetya en juin 2017 : un malware initialement ciblé sur l'Ukraine, qui a paralysé en quelques heures les banques et les transports de Kiev, puis s'est propagé mondialement à des entreprises comme Maersk, Saint-Gobain ou la SNCF (avec des dégâts collatéraux sur certains systèmes informatiques). WannaCry en mai 2017 avait préalablement frappé Telefónica en Espagne et le NHS britannique, démontrant qu'un malware exploitant une vulnérabilité Windows non patchée pouvait paralyser des services essentiels en heures.

Les chiffres récents sont préoccupants. Selon les analyses ENISA et les rapports sectoriels, les ransomwares ciblant le secteur ferroviaire sont passés de 13 % à 25 % de l'ensemble des menaces sur ce secteur entre 2021 et 2022, presque un doublement en un an. En France, l'ANSSI a recensé 144 compromissions par rançongiciel signalées en 2024, niveau stable par rapport à 2023 mais structurellement élevé. Le premier trimestre 2025 a vu une augmentation de 126 % du nombre de victimes revendiquées par les groupes ransomware par rapport au premier trimestre 2024 (rapport Checkpoint). Le facteur humain reste la porte d'entrée principale : 82 % des responsables sécurité (Proofpoint, 2024) considèrent l'erreur humaine — clic sur un lien piégé, mot de passe partagé, accès non révoqué — comme la première vulnérabilité.

La combinaison cyber + blackout : un scénario crédible

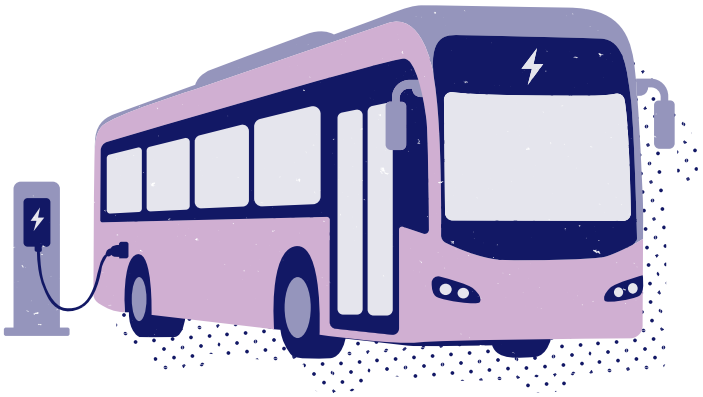
Le scénario qui inquiète le plus les autorités nationales et européennes n'est pas celui d'une cyberattaque isolée, ni celui d'un blackout pur. C'est la combinaison des deux. Une cyberattaque ciblée peut déclencher un blackout localisé ou régional, et inversement, un blackout peut créer une fenêtre d'opportunité pour une attaque sur les systèmes en mode dégradé, moins défendus. Les exemples disponibles sont peu nombreux mais frappants : l'attaque contre Ukrenergo en décembre 2015, puis en décembre 2016, a démontré qu'un attaquant patient pouvait pénétrer le système de contrôle d'un opérateur électrique, déconnecter manuellement des sous-stations à distance, et laisser plusieurs centaines de milliers de foyers dans l'obscurité pendant plusieurs heures. Ces attaques sont attribuées au groupe russe Sandworm, et restent à ce jour les seules attaques cyber documentées ayant causé un blackout délibéré.

Pour un opérateur de transport public dépendant à la fois du courant et de ses systèmes IT, la combinaison est dévastatrice. Sans courant : les rames ferroviaires s'arrêtent, les bus électriques cessent de fonctionner après leurs réserves d'autonomie, les feux tombent, les ascenseurs et escalators sont bloqués, la ventilation des tunnels s'arrête. Sans systèmes IT : la signalisation manuelle de secours est possible mais réduit drastiquement la fréquence ; la billettique tombe (paiement gratuit imposé par défaut, ou contrôle impossible) ; les voyageurs perdent toute information en temps réel ; les conducteurs perdent la liaison avec leurs régulateurs ; les caméras de surveillance s'éteignent. Les deux simultanément : c'est un effondrement complet du service, avec un risque sécuritaire majeur pour les voyageurs piégés dans des tunnels souterrains, des ascenseurs ou des rames sans ventilation.

À l'horizon 2044 : l'hyperdépendance assumée

À l'horizon 2044, la dépendance des réseaux de transport à l'informatique et à l'électricité ne fait que croître. La fin des bus diesel à l'horizon 2035 dans la plupart des grandes agglomérations françaises rend l'électricité non plus une dépendance partielle mais totale. La généralisation du paiement biométrique, des navettes autonomes et de la supervision algorithmique des flottes ajoute des couches de dépendance numérique. Les opérateurs publics deviennent des cibles à la fois d'États (cyberguerre, déstabilisation), de groupes criminels (ransomware, rançon), de hacktivistes (revendication politique) et d'acteurs internes mécontents (sabotage). La surface d'attaque se multiplie avec chaque API ouverte à un prestataire.

Trois conséquences se dessinent. D'abord, le coût de la résilience devient structurel : il faut financer des redondances (chemins électriques alternatifs, serveurs miroir hors-cloud, modes dégradés exerçables manuellement) qui ne servent qu'en cas de crise. C'est une dépense qui ne génère aucun voyageur supplémentaire. Ensuite, l'expertise cybersécurité devient un actif rare et critique : les opérateurs se disputent un vivier limité d'analystes SOC (Security Operations Center) qualifiés, à des salaires qui s'envolent. Enfin, la question de la responsabilité civile et pénale se pose à chaque incident : qui paie quand un voyageur meurt dans un tunnel après une attaque cyber non revendiquée ? L'opérateur, l'AOM, l'État, l'éditeur de logiciel ? Les contrats de délégation devront intégrer ces clauses, sous peine de désengagement progressif des opérateurs privés des contrats les plus exposés.



Le récit

Vendredi 24 juin, 14 h 03

Lyon, juin 2044

Jodie Vermeer regardait son écran principal depuis quatorze secondes, sans cligner. Trois processus venaient de tomber simultanément sur la console de supervision du réseau Tramway de l'agglomération lyonnaise. Ce n'était pas anormal. Ce qui l'était, c'est que les trois processus tombés n'étaient pas situés sur le même serveur, ni sur le même rack, ni dans le même bâtiment. Le premier était à Lyon-Confluence, le deuxième dans le datacenter de Vénissieux, le troisième sur le cloud souverain hébergé à Strasbourg. Trois lieux physiques différents. Trois failles simultanées. Statistiquement, impossible.

Elle avait trente et un ans et travaillait depuis quatre ans au Security Operations Center de Keolis Lyon, dans le sous-sol d'un immeuble tertiaire de la Part-Dieu. L'open space sans fenêtres, climatisé à 22 °C tout l'été, vibrait du bourdonnement régulier des baies de serveurs alignées derrière la cloison vitrée. Six analystes en poste ce vendredi 24 juin, sur un effectif de quatorze. Dehors, Lyon affichait 42 °C, vague de chaleur classe 4 démarrée le mardi. Vendredi après-midi, début juillet imminent, vacances scolaires lancées : le réseau transportait à cette heure environ 80 000 voyageurs en heure creuse, ce qui montait habituellement à 220 000 au pic du retour.

À 14 h 04, le quatrième processus tomba. La supervision de la billettique sans contact sur l'ensemble du réseau bus. À 14 h 05, le cinquième : la gestion de l'alimentation électrique des trois lignes de tramway. Jodie composa immédiatement le numéro de Vincent Roca, directeur des opérations. Il décrocha à la deuxième sonnerie. « Vincent. On a quelque chose. Cinq systèmes critiques tombés en deux minutes, sur trois sites différents. Ce n'est pas une coïncidence. » Vincent demanda combien. « Cinq pour l'instant. Mais ça monte. »

À 14 h 07, l'écran d'alerte clignota en rouge : sur l'application interne, un message court venait d'apparaître. Pas dans la boîte mail, pas dans la messagerie sécurisée. Directement sur le bandeau de notification système — chose techniquement impossible dans une infrastructure correctement segmentée. Le message tenait en six mots : « Première leçon. Signé : Mirror. »

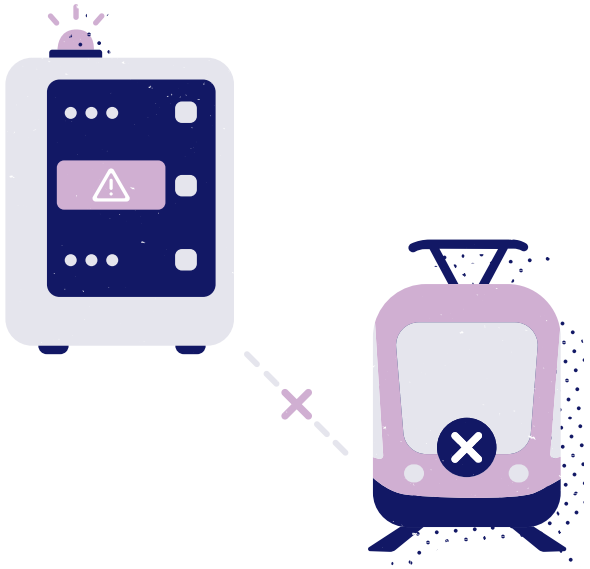
Jodie le lut deux fois. Puis elle décrocha à nouveau son téléphone et appela Anthony Schroeder. Anthony avait cinquante-huit ans, vingt-deux ans d'ANSSI derrière lui dont sept à la direction technique, et il consultait pour Keolis depuis 2041, deux jours par semaine, depuis sa maison de Villeurbanne. C'est lui qui avait conçu le plan de crise cyber actuel.

Il décrocha à la première sonnerie. « Jodie. » Elle dit : « Anthony. On a un attaquant qui signe Mirror. Cinq systèmes tombés en quatre minutes. Une notification système directe sur les écrans internes. » Long silence à l'autre bout. Puis Anthony, voix basse : « J'arrive. Trente minutes en moto. Ne touchez à rien que les playbooks défensifs niveau 1. Surtout pas de débranchement physique avant que je sois là. »

À 14 h 12, le poste central de Confluence vit tomber sa climatisation. Pas l'électricité — la climatisation, seulement. Mais en dix minutes la température dans la salle des serveurs allait monter de 22 à 35, et au-delà de 40 les machines basculeraient automatiquement en arrêt protection. Jodie le comprit en regardant l'écran d'environnement : c'était calculé. L'attaquant ne voulait pas couper le courant brutalement. Il voulait que les serveurs s'éteignent eux-mêmes pour cause de surchauffe, en mode protégé, en gardant les logs. Une attaque élégante. Une attaque par chaleur. Une attaque qui détestait ses victimes assez pour leur donner le temps de regarder venir.

À 14 h 18, le premier voyageur appela le centre d'appel. Une dame âgée, station Bellecour, dans un tramway T1 immobilisé en station depuis dix minutes, climatisation à l'arrêt, portes ouvertes, conducteur silencieux. À 14 h 21, le deuxième : un homme à Vaulx-en-Velin coincé dans un bus électrique qui avait perdu toute puissance, sur la voie réservée, conducteur en train de demander une évacuation. À 14 h 25, le centre d'appel saturait. À 14 h 29, le téléphone de Jodie se mit à émettre un sifflement aigu et se figea. Réseau 6G saturé. À 14 h 30, plus aucun appel ne sortait du bâtiment.

Anthony arriva à 14 h 34, son casque sous le bras, le visage couleur de cendre. Il jeta un coup d'œil aux écrans, à la console des logs, au message « Première leçon. Signé : Mirror. » Et il dit, à voix très basse, pour personne : « Putain. »



Vincent Roca déboula dans la salle à 14 h 36. Il avait couru depuis le 12e étage par les escaliers — les ascenseurs étaient tombés. Il transpirait. « Bilan ? » Jodie : « Onze systèmes tombés. Tramway à l'arrêt sur les trois lignes. Bus électriques 60 % à l'arrêt par perte de supervision. Billettique inopérante. Centres d'appel saturés. Téléphonie sortante coupée. Climatisation des postes de contrôle en perte progressive. Vidéosurveillance : on perd les flux les uns après les autres. Et il y a un attaquant qui s'est annoncé. » Vincent : « Sandworm ? Lockbit ? Cl0p ? » Anthony, calmement : « Non. Ce n'est aucun de ceux-là. C'est quelqu'un que je connais. »

Il s'installa devant la console de Jodie, demanda les logs, les regarda pendant deux minutes en silence. Puis il dit : « Mirror, c'est une signature que j'ai vue trois fois entre 2032 et 2035 à l'ANSSI. Trois attaques contre des opérateurs de transport européens — Lisbonne, Düsseldorf, Naples. À chaque fois, jamais revendiquée, jamais d'argent demandé, jamais de communication. Juste un message court à la fin. À Lisbonne en 2033 c'était : vous n'aviez pas écouté. À Düsseldorf en 2034 : vous n'aviez pas vu. À Naples en 2035 : vous n'aviez pas compris. On n'a jamais identifié l'auteur. Le profilage suggérait quelqu'un qui avait travaillé dans le milieu de la cybersécurité offensive, qui s'ennuyait ou qui jouait. Ni groupe étatique, ni cybercriminel. Quelqu'un qui voulait nous apprendre quelque chose. » Jodie : « Apprendre quoi ? » Anthony la regarda. « Que nous ne sommes pas prêts. Et qu'aucun montant de réglementation ne nous rendra prêts si nous continuons à penser que c'est un problème technique. »

À 14 h 51, la lumière du SOC bascula sur l'éclairage de secours. Les LED blanches devinrent rouges. Le bourdonnement des serveurs derrière la cloison vitrée changea de note, descendit d'une octave, puis se mit à clignoter par à-coups. Une odeur de plastique chaud commença à monter du faux plancher. Vincent ordonna à toutes les équipes non-critiques d'évacuer le bâtiment. Jodie, Anthony et deux autres analystes restèrent. Le climatiseur de la salle principale lâcha à 14 h 58. La température commença à monter de un degré toutes les quatre minutes.

À 15 h 12, le rapport préliminaire des évacuations remonta du réseau : un voyageur âgé décédé à la station Saxe-Gambetta, vraisemblablement d'un malaise cardiaque lié à la chaleur dans la rame immobilisée portes fermées (la commande d'ouverture manuelle avait été oubliée par le conducteur sous le coup du stress). Une femme enceinte évacuée par les secours d'un bus de la ligne C7 en cours de césarienne d'urgence. Quarante-sept passagers piégés dans un ascenseur entre deux niveaux à la station Vieux-Lyon, dont on entendait les cris dans la cage par les capteurs audio encore actifs. Anthony lut le rapport, leva les yeux, dit doucement à Jodie : « Première leçon. »

À 16 h 22, en utilisant un canal radio analogique de secours (acheté trois ans plus tôt sur insistance d'Anthony, contre l'avis du contrôle de gestion), ils réussirent à coordonner avec SNCF Réseau et Enedis une stratégie de re-segmentation manuelle. À 17 h 47, le premier tramway redémarra sur la ligne T2, en mode manuel sécurisé, vitesse limitée à 15 km/h, sans signalisation centralisée, conducteur en visu directe. À 21 h 15, le réseau bus fonctionnait à 35 % de son régime nominal. Le métro restait totalement à l'arrêt. La billettique resterait inopérante pendant six semaines : tout le monde voyagerait gratuitement, par défaut.

Le rapport interne établi le lundi 27 juin chiffra le bilan humain à trois décès — l'homme de Saxe-Gambetta, plus deux personnes décédées de coup de chaleur dans des tunnels de métro mal ventilés, dont les corps ne furent retrouvés que le samedi matin. Les blessés directs étaient au nombre de quarante-sept, dont dix-huit graves. Le coût financier direct fut estimé à 47 millions d'euros sur l'opérateur, sans compter les pertes pour les commerces lyonnais (estimées entre 80 et 120 millions), les indemnisations qui s'étaleraient sur des années, et les coûts de reconstruction de l'infrastructure cyber (estimés à 30 millions sur dix-huit mois). Mirror ne s'est plus jamais manifesté Lyon. Anthony Schroeder a démissionné de son contrat de consultant le 1er septembre 2044, sans explication publique. Jodie Vermeer occupe toujours son poste au SOC.

Le silence des serveurs, ce vendredi 24 juin à 14 h 03, avait duré exactement neuf secondes avant que Jodie ne s'en aperçoive. Personne n'avait entendu les serveurs se taire. Personne ne les entendrait jamais.

Trois scénarios prospectifs

SCÉNARIO BLANC

La résilience institutionnalisée

Dans l'hypothèse optimiste, la décennie 2030 a été celle d'une prise de conscience généralisée. Les opérateurs de transport ont été reconnus comme opérateurs d'importance vitale dans toute l'Europe, avec des obligations strictes d'audit annuel, de tests d'intrusion, de redondance, de plans de continuité exerçables. Les autorités organisatrices financent explicitement la résilience cyber dans les contrats, avec une enveloppe dédiée représentant 4 à 6 % du budget IT des opérateurs. Les centres SOC mutualisés entre opérateurs (Keolis, Transdev, SNCF, RATP Dev, etc., dans des consortiums sectoriels) deviennent la norme, partageant la veille et les indicateurs de compromission en temps réel. Les modes dégradés sont régulièrement exercés, y compris avec des coupures planifiées de plusieurs heures en condition réelle. Les attaques continuent — elles ne disparaissent pas — mais elles n'arrivent plus à paralyser un réseau plus de quelques heures, et n'occasionnent plus de victimes humaines. La cybersécurité devient un métier de transport public comme un autre, avec ses carrières, ses formations, ses syndicats.

SCÉNARIO GRIS

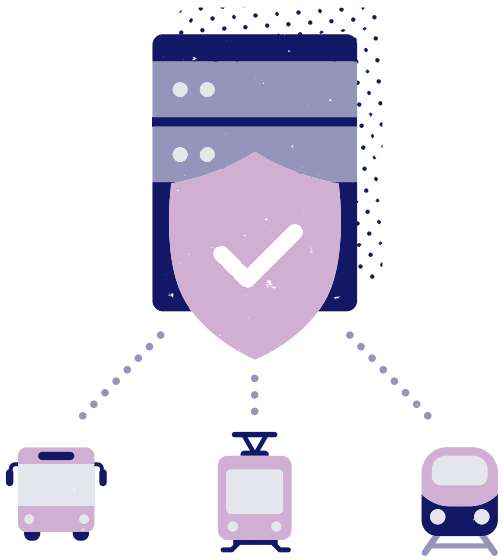
La vulnérabilité gérée au coup par coup

Dans la trajectoire intermédiaire, la cybersécurité reste un sujet sérieux mais sous-financé. Les opérateurs investissent ce qu'ils peuvent, c'est-à-dire ce que les contrats leur permettent — souvent insuffisant. Les attaques se multiplient : on en compte cinq à dix par an en France touchant le secteur transport, dont une ou deux paralysent un réseau urbain pour 48 à 72 heures. Les victimes humaines restent rares mais non nulles : un à trois morts par an au niveau national, en moyenne, dans des incidents combinés cyber + dégradation opérationnelle. L'État durcit la réglementation après chaque crise majeure, sans que les budgets suivent vraiment. Les assurances cyber deviennent prohibitives ou se retirent du secteur. Les opérateurs apprennent à vivre avec un niveau de risque qu'aucun n'aurait accepté dix ans plus tôt, faute d'alternative.

SCÉNARIO NOIR

Le réseau démantelable à distance

Dans l'hypothèse pessimiste, le scénario combiné cyber + blackout devient l'arme de prédilection des conflits hybrides. À l'horizon 2044, une grande agglomération européenne subit chaque année une attaque majeure entraînant un arrêt total du réseau pendant plus de 24 heures. Les morts se comptent en dizaines par incident dans les pires cas (vague de chaleur + tunnel + ventilation à l'arrêt). Les voyageurs aisés se détournent durablement du transport public, qu'ils perçoivent comme exposé et imprévisible. Les capsules autonomes privées, perçues comme moins vulnérables (à tort, mais la perception suffit), captent une part croissante des trajets. Les opérateurs publics deviennent invendables pour les acteurs privés, qui se retirent un à un des appels d'offres. Les autorités organisatrices se retrouvent à exploiter directement, sans expertise cyber et sans capacité financière, des réseaux qui sont des cibles permanentes. La géopolitique de la cybersécurité devient un sujet de souveraineté nationale, mais aussi un facteur structurant de la qualité de vie urbaine. Le contrat social du transport public — service universel, fiable, sûr — se délite sous l'effet d'attaques que personne ne revendique et qu'aucun État n'arrive à dissuader.



Bibliographie

ENTSO-E, Factual Report on the Grid Incident in Spain and Portugal on 28 April 2025, 3 octobre 2025 ; rapport final identifiant les causes racines, 20 mars 2026.

RTE, Foire aux questions : black-out du 28 avril 2025 sur la péninsule ibérique, mise à jour 25 mars 2026.

Red Eléctrica de España (REE), communiqué officiel du gouvernement espagnol du 17 juin 2025 sur les causes du blackout du 28 avril 2025.

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

ENISA, Threat Landscape 2024, Agence européenne de la cybersécurité, juin 2024.

ANSSI, Panorama de la cybermenace 2024, Agence nationale de la sécurité des systèmes d'information, 2025 (144 compromissions par rançongiciel signalées).

Checkpoint Software Technologies, Cyber Security Report Q1 2025 (augmentation de 126 % des attaques par rançongiciel par rapport à Q1 2024).

Proofpoint, Voice of the CISO 2024 Report (82 % des RSSI considèrent l'erreur humaine comme la principale source de vulnérabilité).

Directive (UE) 2022/2555 (NIS2) du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, transposée en France en octobre 2024.

Cybmalveillance.gouv.fr, Rapport d'activité annuel 2024 et 2025, GIP ACYMA.

Zataz, « Hacktivistes pro-russes : paralysie d'une partie du réseau ferré polonais », août 2023.

Greenberg, A., Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, Doubleday, 2019 (sur les attaques Ukrenergo 2015-2016 et NotPetya 2017).

Bodet-Time, « Les enjeux d'une cyberattaque dans le secteur des transports », 2025 (ransomware 13 % → 25 % des attaques ferroviaires entre 2021 et 2022).

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

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

Harris, T., Le Silence des agneaux, éditions Albin Michel, 1989 (1re éd. The Silence of the Lambs, St. Martin's Press, 1988).