Le BPA tenait au réseau : la cyberattaque comme révélateur

Le 8 septembre 2026, Boston Scientific a signé une déclaration réglementaire qui enchaîne, dans cet ordre, une panne réseau, l'arrêt partiel de la fabrication et des expéditions, puis l'abandon probable de ses prévisions de ventes et de bénéfice par action (BPA, le résultat net rapporté à chaque action). Son rapport annuel nommait cette dépendance sans jamais en donner la mesure. L'incident agit comme un révélateur, au sens photographique : il fait apparaître une architecture devenue indécomposable, construite par l'intégration et absente des documents de gouvernance, au moment même où l'obligation qui rend ce couplage public est contestée devant le régulateur.

Par Alexandre Berge · 20 octobre 2026 · 17 min de lecture · Chronique

Trois déclarations décrivent la même séquence, du réseau aux prévisions

Le 25 août 2026, Boston Scientific identifie un incident de cybersécurité qui, selon ses propres termes, provoque une perturbation mondiale de ses opérations. Le 8 septembre, le fabricant de dispositifs médicaux signe un formulaire 8-K (rapport courant qu'une société cotée aux États-Unis dépose lors d'un événement significatif) au titre de la rubrique 1.05, réservée aux incidents de cybersécurité jugés matériels. Le document décrit une chaîne causale d'une netteté rare. Une activité non autorisée sur certains systèmes a provoqué une panne réseau « affecting access to certain operating systems and business applications » (affectant l'accès à certains systèmes d'exploitation et applications métier), ce qui a atteint la capacité de l'entreprise à fabriquer, à traiter les commandes et à les expédier.

La conséquence financière suit dans le même texte. La société juge peu probable d'atteindre les fourchettes de croissance des ventes et de BPA ajusté communiquées le 29 juillet pour le troisième trimestre et l'exercice 2026. Elle indique que la distribution, la stérilisation et la plupart des sites de fabrication ont repris, compte récupérer une partie du chiffre d'affaires touché en résorbant les commandes en attente, renvoie la mise à jour chiffrée à sa conférence de résultats du 28 octobre 2026 et n'anticipe pas d'effet matériel sur sa situation financière à long terme.

Le schéma n'est pas isolé. West Pharmaceutical Services, fournisseur de composants pour médicaments injectables, détecte une intrusion le 4 mai 2026, conclut le 7 mai au caractère

matériel de l'attaque (données exfiltrées, systèmes chiffrés) et signe son 8-K le 11 mai. Pour contenir l'attaque, l'entreprise a mis ses systèmes hors ligne à l'échelle mondiale, puis redémarré expédition, réception et fabrication site par site. Son amendement du 20 mai la déclare pleinement opérationnelle et l'incident sans effet matériel sur ses prévisions. Son rapport trimestriel au 30 juin chiffre pourtant à environ 7 millions de dollars l'effet négatif de l'arrêt de production sur la croissance des ventes de son activité de fabrication sous contrat, dont la marge brute recule de 3,3 points sur le trimestre. Stryker, enfin, identifie un incident le 11 mars 2026. Son 8-K/A (version amendée) du 9 avril conclut à un impact matériel sur ses opérations et sur ses résultats du premier trimestre, tout en maintenant ses prévisions annuelles. Son rapport trimestriel décrit une perturbation de l'environnement réseau de l'entreprise et attribue la baisse de la marge brute (63,3 % contre 63,8 %) principalement au temps de production à l'arrêt, dans ses deux grands segments d'activité.

Trois sociétés, trois issues financières différentes, une même grammaire. Le réseau tombe, les applications deviennent inaccessibles, la fabrication et l'expédition s'arrêtent, et la prévision devient l'endroit où l'incident se lit dans la communication financière.

Le rapport annuel nommait la dépendance sans en donner la mesure

Le rapport annuel (formulaire 10-K) de Boston Scientific pour l'exercice 2025, signé le 17 février 2026, ne passait pas la dépendance informatique sous silence. Un facteur de risque dédié indique que l'entreprise s'appuie sur ses systèmes d'information et ses technologies opérationnelles « to manufacture and ship our products » (pour fabriquer et expédier nos produits). Le même texte envisage l'échec des plans de réponse aux incidents, de reprise après sinistre et de continuité d'activité, et les effets qu'il aurait sur les opérations et les résultats.

Le diagnostic qualitatif était donc juste. Ce qui manque, dans les rubriques 1A (facteurs de risque) et 1C (cybersécurité), c'est une grandeur. Aucune durée d'indisponibilité tolérable, aucune part du chiffre d'affaires dépendant d'un socle réseau commun, aucun ordre de grandeur des ventes différées par jour d'arrêt n'y figure. La rubrique 1C décrit la gouvernance (supervision par le conseil, points annuels sur la cybersécurité, remontée immédiate des sujets susceptibles d'effets matériels) et affirme qu'aucun risque cyber n'a affecté matériellement l'entreprise, ni n'est raisonnablement susceptible de le faire, à la date du rapport. L'arithmétique que le document ne fait pas est pourtant simple : avec 20,074 milliards de dollars de ventes nettes en 2025, chaque jour calendaire représente en moyenne environ 55 millions de dollars de chiffre d'affaires.

L'écart entre les deux documents constitue l'angle mort. Le facteur de risque énonce une possibilité valable pour toute grande entreprise. Le 8-K donne un ordre de causalité, du réseau aux prévisions, que la gouvernance n'avait pas traduit en unités de compte de résultat. Le discours dominant sur la cybersécurité, centré sur la description des dispositifs et la

conformité, produit exactement ce type de texte : exact, prudent, et inutilisable pour répondre à la seule question qu'un conseil se pose au premier jour d'une panne, à savoir combien de chiffre d'affaires trimestriel cesse d'être facturable si l'annuaire ou le réseau reste indisponible dix jours.

Les documents d'après incident font d'ailleurs surgir un vocabulaire absent des rapports annuels. Les 8-K de Boston Scientific et de Stryker rangent parmi leurs facteurs d'incertitude l'adéquation des processus pendant la perturbation et le recours à des solutions de remplacement des systèmes. Le mode dégradé (la manière de continuer à produire et facturer sans les outils habituels), invisible tant que tout fonctionne, devient un sujet de communication financière dès qu'il est mobilisé.

L'intégration a effacé les frontières à l'intérieur desquelles une panne reste locale

> **Concept : la quasi-décomposabilité (Herbert A. Simon, 1962)**
>
> Dans « The Architecture of Complexity » (*Proceedings of the American Philosophical Society*, décembre 1962), l'économiste et théoricien des organisations Herbert A. Simon décrit les systèmes complexes durables comme *quasi décomposables* : des sous-systèmes dont les interactions mutuelles sont « weak, but not negligible » (faibles, mais pas négligeables). À court terme, chaque sous-système se comporte de façon à peu près indépendante des autres. À long terme, il ne dépend d'eux que de manière agrégée. Simon en tire une propriété de résistance : un système bâti en sous-ensembles stables absorbe une interruption en ne perdant que le sous-ensemble en cours.

Simon illustre la thèse par une parabole. Deux horlogers, Hora et Tempus, fabriquent des montres d'environ mille pièces. Tempus les assemble d'une seule traite, si bien qu'une interruption (un appel de client) fait tomber en morceaux la montre inachevée, qu'il doit reprendre depuis les pièces élémentaires. Hora assemble des sous-ensembles stables d'une dizaine de pièces, eux-mêmes regroupés en ensembles plus larges, et une interruption ne lui coûte que quelques gestes. Avec une probabilité d'interruption de 1 % à chaque pièce ajoutée, Simon calcule que Tempus met en moyenne quelque quatre mille fois plus longtemps qu'Hora à achever une montre.

Un système d'information d'entreprise est quasi décomposable lorsqu'un incident dans un domaine (un site, une fonction, une application) laisse les autres fonctionner. Il cesse de l'être lorsque tous les domaines partagent le même annuaire d'identités, le même réseau et le même progiciel de gestion. Les interactions ne sont plus faibles, elles sont constitutives. Les trois déclarations en portent la trace. Boston Scientific décrit une perturbation mondiale née d'une panne réseau. Stryker impute la baisse de marge de ses deux grands segments, MedSurg et Neurotechnologie d'une part, Orthopédie de l'autre, au même arrêt de production. Chez West, l'unité de confinement retenue a été le monde entier : quand l'architecture n'offre

pas de frontière intermédiaire, isoler revient à tout éteindre.

Le 10-K de Boston Scientific signale d'ailleurs la dynamique d'intégration en cours, sans qu'aucun document public ne la relie à l'incident. L'entreprise indique avoir déjà subi, et pouvoir subir encore, des interruptions opérationnelles liées au déploiement de son progiciel de gestion intégré (ERP) mondial. L'ERP est précisément l'outil qui remplace une constellation de systèmes faiblement couplés par une plateforme unique. Son discours de justification compte la visibilité, la standardisation et l'efficience. Il ne compte jamais la décomposabilité perdue, c'est-à-dire la taille de la montre que la prochaine interruption fera tomber en morceaux. Là où les chroniques consacrées à Tchap et à Hélios demandaient, avec Charles Perrow, pourquoi l'accident survient, le présent article demande pourquoi la perte qu'il entraîne n'a pas de frontière.

Maersk, 2017 : la facturation comme dernier maillon de la chaîne

Le précédent le plus proche est celui d'A.P. Møller-Mærsk, frappé par une cyberattaque en juin 2017. Le rapport annuel 2017 du groupe, publié le 9 février 2018, estime l'effet sur la rentabilité entre 250 et 300 millions de dollars, concentré pour l'essentiel sur Maersk Line au troisième trimestre. Il relie aussi le flux de trésorerie opérationnel négatif de Damco, sa filiale de commission de transport (moins 101 millions de dollars, contre plus 4 millions un an plus tôt), à l'effet temporaire de l'attaque sur ses opérations et ses processus de facturation, et note la dégradation du coût unitaire de Maersk Line au même trimestre.

La proximité structurelle tient à trois traits. L'attaque frappe un réseau partagé par des activités physiques mondiales, l'impact se concentre sur le trimestre qui suit, et la facturation apparaît comme le maillon où l'arrêt informatique devient perte de trésorerie. La différence tient au véhicule de publication : Maersk chiffre l'incident dans ses rapports périodiques, quand les sociétés cotées aux États-Unis doivent désormais le déclarer dans un format dédié. Le rapport 2017 fixe d'ailleurs comme priorité le renforcement de la colonne vertébrale informatique et de la cyberrésilience, autrement dit la prise en compte, après coup, d'une dépendance que les documents antérieurs ne mesuraient pas.

L'instrument qui rend le couplage visible est contesté au nom de son coût

La rubrique 1.05 du formulaire 8-K et l'item 106 du règlement S-K (description annuelle, dans le 10-K, de la gestion et de la gouvernance du risque cyber) résultent de la règle adoptée par la SEC (Securities and Exchange Commission, l'autorité fédérale américaine des marchés) le 26 juillet 2023. L'émetteur doit déclarer l'incident dans les quatre jours ouvrés qui suivent sa conclusion sur la matérialité, conclusion à tirer sans retard déraisonnable, en décrivant sa nature, son étendue, son calendrier et son impact matériel. La rubrique s'applique depuis le 18 décembre 2023 aux émetteurs autres que les petites sociétés.

Le 13 janvier 2026, le président de la SEC, Paul Atkins, a ouvert une consultation sur la réforme

du règlement S-K. Le 2 octobre 2026, CTIA, association professionnelle du secteur américain des communications sans fil, y dépose une lettre signée par Avonne S. Bell qui demande l'abrogation de l'item 106 et de la rubrique 1.05, et le retour à une déclaration volontaire des incidents. L'argument de coût y est explicite : la déclaration « is very costly » (coûte très cher), parce que la matérialité doit être réévaluée en permanence avec l'aide d'avocats et d'équipes externes. La lettre ajoute que la déclaration précoce peut être prématurée, renseigner les attaquants et gêner la coopération avec les services d'enquête. CTIA n'est pas isolée. Le 22 mai 2025, cinq organisations bancaires et financières, dont l'American Bankers Association et la SIFMA, avaient déjà déposé une pétition demandant l'abrogation de la rubrique 1.05.

Ces arguments sont sérieux. Le Government Accountability Office (GAO, l'organe de contrôle du Congrès) a recensé le 22 juillet 2026 cent dix-sept réglementations fédérales de cybersécurité émanant de trente-sept agences, dont quatre-vingts (environ 70 %) contiennent une obligation de déclaration de même nature qu'une autre. Mais le paradoxe demeure. Dans le périmètre consulté, les 8-K de 2026 sont la seule trace publique et datée de l'ordre de causalité entre réseau et prévisions. Le rapport annuel de Boston Scientific ne le contenait pas sous forme mesurée. Supprimer l'obligation reviendrait à laisser le marché découvrir ce couplage au moment des résultats trimestriels, sans le récit causal qui permet de le comprendre. Un document de travail non évalué par les pairs (Maxwell Block, décembre 2025) recense 54 rapports de ce type déposés par 36 sociétés au 12 novembre 2025, suivis en moyenne d'une baisse de cours de 3,07 % sur cinq séances. Dans la liste des projets de règles de la SEC consultée le 18 octobre 2026, aucune proposition ne vise encore la règle de 2023, alors que l'abrogation des règles de publication climatique a été proposée le 29 mai 2026.

Le régime européen sert ici de miroir, à condition d'être décrit avec exactitude. La directive (UE) 2022/2555, dite NIS2, impose aux entités essentielles et importantes une alerte précoce dans les 24 heures, une notification d'incident dans les 72 heures et un rapport final au plus tard un mois après, adressés à l'équipe nationale de réponse aux incidents ou à l'autorité compétente. L'information du public n'y intervient qu'à l'initiative de cette équipe ou de cette autorité, après consultation de l'entité. Le règlement (UE) 2022/2554, dit DORA, organise de même pour le secteur financier une déclaration à l'autorité compétente. Le règlement (UE) n° 596/2014 sur les abus de marché impose bien à tout émetteur de rendre publiques, dès que possible, les informations privilégiées qui le concernent directement. Une société cotée française dont un incident compromet les prévisions doit donc informer le marché. Mais cette obligation de principe ne prescrit ni rubrique dédiée, ni description de la nature, de l'étendue et du calendrier de l'incident. Une direction française dispose ainsi d'obligations de notification nombreuses, majoritairement confidentielles, et d'une obligation de publicité générale, sans équivalent public de la précision causale qu'impose la rubrique 1.05 (la transposition française de NIS2 a fait l'objet d'une chronique le 3 octobre 2026).

> **Grille de lecture**
>
> 1. Quel document présenté au conseil exprime, en jours ou en part du chiffre d'affaires trimestriel, l'effet d'une indisponibilité de l'annuaire ou du réseau principal, et de quand date sa dernière version ?
> 2. Combien de sites de production, d'entrepôts et de fonctions de facturation dépendent du même domaine d'authentification ?
> 3. Le plan de réponse aux incidents prévoit-il une frontière de confinement plus petite que l'organisation entière, et a-t-elle été exercée ?
> 4. Parmi la prise de commande, la libération des lots, l'expédition et la facturation, quelles opérations disposent d'un mode dégradé documenté et exercé au cours des douze derniers mois ?

Partout où l'intégration a effacé les frontières de panne, la même chaîne attend son incident

Le mécanisme ne tient ni au secteur des dispositifs médicaux ni au droit américain. Il se formule sans nom d'organisation : plus l'intégration des systèmes de gestion, de production et de logistique progresse pour gagner en efficience, plus le système d'information devient un intrant commun de toutes les étapes qui produisent le chiffre d'affaires, et plus son indisponibilité se transmet directement au compte de résultat, sans que cette transmission figure dans les documents de gouvernance avant l'incident.

Il se reproduit dès que quatre conditions se cumulent. La première est l'appui de toute la chaîne, de la commande à l'encaissement, sur un socle commun d'identité et de réseau, ce qui transforme une défaillance locale en indisponibilité générale. La deuxième est la disparition des amortisseurs (stocks de sécurité, procédures papier, autonomie des sites), sacrifiés à l'efficience. La troisième est une contrainte calendaire, trimestre, exercice ou campagne, qui convertit quelques jours d'arrêt en écart de prévision. La quatrième est une cartographie des risques exprimée en échelles qualitatives de probabilité et de gravité plutôt qu'en unités de compte de résultat.

Les signes sont observables dans une organisation quelconque. Le risque cyber y figure comme une ligne parmi d'autres de la cartographie, avec une cotation et un propriétaire, mais sans durée ni montant. Les objectifs de reprise sont fixés application par application et non par flux de revenus, si bien que nul ne sait combien de temps la facturation survit à la perte de l'annuaire. Les exercices de continuité testent la restauration technique, rarement la capacité à expédier et facturer en mode dégradé. Le plan de confinement ne connaît qu'un geste, l'extinction générale. Que le flux concerné soit l'encaissement des cotisations d'une mutuelle, la facturation des séjours d'un établissement de santé ou l'expédition d'une ETI industrielle, la durée tolérable d'indisponibilité relève de la direction financière autant que de

la DSI (direction des systèmes d'information), et l'angle mort naît de ce qu'aucune des deux ne la possède.

Ce que diront le 28 octobre et le prochain rapport annuel

Le cas Boston Scientific ouvre une hypothèse vérifiable de l'extérieur. Lors de sa conférence du 28 octobre 2026, la société chiffrera l'effet de l'incident sur les ventes du troisième trimestre, ce que montrera le communiqué de résultats déposé auprès de la SEC. Son rapport annuel pour l'exercice 2026, attendu au premier trimestre 2027 comme le précédent, retirera de la rubrique 1C l'affirmation selon laquelle aucun risque cyber ne l'a affectée matériellement, et décrira l'incident dans ses facteurs de risque, sans exprimer pour autant la dépendance de la fabrication et de la distribution en jours ou en part de chiffre d'affaires. Enfin, au 31 octobre 2027, la rubrique 1.05 du formulaire 8-K sera toujours en vigueur, ce que permettra de constater la liste des règles de la SEC.

Si ces indicateurs se vérifient, le constat sera net. Le BPA tenait au réseau, la cyberattaque l'a révélé, et seule la déclaration d'incident l'aura dit publiquement, avec l'ordre des causes. Une gouvernance qui attend ce révélateur pour mesurer la décomposabilité de son système d'information découvre la taille de sa montre au moment où elle tombe en morceaux.

Note méthodologique

Sources principales : formulaires 8-K, 8-K/A, 10-K et 10-Q de Boston Scientific, West Pharmaceutical Services et Stryker déposés sur EDGAR, lettre de CTIA et pétition 4-856 au dossier de la SEC, règle SEC 33-11216, textes européens sur EUR-Lex, rapport annuel 2017 d'A.P. Møller-Mærsk. Les dates retenues pour les 8-K sont les dates de signature, distinctes des dates d'événement déclarées. L'absence de mesure de dépendance est constatée dans les rubriques 1A et 1C du 10-K 2025 de Boston Scientific, et l'absence de projet de règle visant la rubrique 1.05 dans la liste des travaux réglementaires de la SEC de juin 2025 au 9 octobre 2026, consultées le 18 octobre 2026. Le couplage serré de Perrow et le couplage lâche de Weick ayant déjà servi de cadre central à des chroniques de ce site, l'auteur a retenu la quasi-décomposabilité de Simon (1962). Le calcul de 55 millions de dollars de ventes par jour est une moyenne arithmétique établie par l'auteur à partir du 10-K. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Documents des organisations

- Boston Scientific Corporation, Form 8-K, Item 1.05 « Material Cybersecurity Incidents », signé le 8 septembre 2026, https://www.sec.gov/Archives/edgar/data/0000885725/000088572526000059/bsx-20260907.htm
- Boston Scientific Corporation, Form 10-K for the fiscal year ended December 31, 2025, signé le 17 février 2026, https://www.sec.gov/Archives/edgar/data/885725/000088572526000010/bsx-20251231.htm
- West Pharmaceutical Services, Inc., Form 8-K, Item 1.05, signé le 11 mai 2026, https://www.sec.gov/Archives/edgar/data/0000105770/000010577026000068/wst-20260507.htm
- West Pharmaceutical Services, Inc., Form 8-K/A (Amendment No. 1), signé le 20 mai 2026, https://www.sec.gov/Archives/edgar/data/0000105770/000010577026000077/wst-20260507.htm
- West Pharmaceutical Services, Inc., Form 10-Q for the quarterly period ended June 30, 2026, signé le 23 juillet 2026, https://www.sec.gov/Archives/edgar/data/0000105770/000010577026000099/wst-20260630.htm
- Stryker Corporation, Form 8-K/A (Amendment No. 1), signé le 9 avril 2026, https://www.sec.gov/Archives/edgar/data/310764/000119312526149607/d112875d8ka.htm
- Stryker Corporation, Form 10-Q for the quarterly period ended March 31, 2026, signé le 11 mai 2026, https://www.sec.gov/Archives/edgar/data/0000310764/000031076426000031/syk-20260331.htm
- CTIA (The Wireless Association), « Comment on Reforming Regulation S-K (File No. CLL-15), Cybersecurity Disclosures », 2 octobre 2026, https://www.sec.gov/comments/CLL-15/cll15-1082159-3759646.pdf
- American Bankers Association, Bank Policy Institute, Securities Industry and Financial Markets Association, Independent Community Bankers of America, Institute of International Bankers, « Joint Petition for Rulemaking to Amend the SEC Cybersecurity Risk Management, Strategy Governance & Incident Disclosure rule to rescind Form 8-K, Item 1.05 and Form 6-K requirements » (pétition 4-856), 22 mai 2025, https://www.sec.gov/files/rules/petitions/2025/petn4-856.pdf

Textes officiels et décisions d'autorités

- Securities and Exchange Commission, « Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure », Release No. 33-11216, 26 juillet 2023, https://www.sec.gov/files/rules/final/2023/33-11216.pdf
- Securities and Exchange Commission, guide de conformité « Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure », mis à jour le 10 septembre 2024, consulté le 18 octobre 2026, https://www.sec.gov/resources-small-businesses/

small-business-compliance-guides/cybersecurity-risk-management-strategy-governance-incident-disclosure

- Paul S. Atkins, « Statement on Reforming Regulation S-K », SEC, 13 janvier 2026, https://www.sec.gov/newsroom/speeches-statements/atkins-statement-reforming-regulation-s-k-011326
- Securities and Exchange Commission, « Rulemaking Activity », consulté le 18 octobre 2026, https://www.sec.gov/rules-regulations/rulemaking-activity
- Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 (NIS2), article 23, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022L2555
- Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 (DORA), article 19, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022R2554
- Règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché, article 17, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32014R0596

Études et statistiques

- U.S. Government Accountability Office, « Cybersecurity Regulations: Multiple Sectors Are Subject to Potentially Duplicative Reporting Requirements », GAO-26-108606, 22 juillet 2026, https://www.gao.gov/products/gao-26-108606
- Maxwell Block, « Market Reactions to Material Cybersecurity Incident Disclosures », arXiv:2512.06144 (document de travail), 5 décembre 2025, https://arxiv.org/abs/2512.06144

Cadre théorique

- Herbert A. Simon, « The Architecture of Complexity », *Proceedings of the American Philosophical Society*, vol. 106, n° 6, 12 décembre 1962, p. 467-482, https://pdodds.w3.uvm.edu/research/papers/others/1962/simon1962a.pdf

Parallèle historique

- A.P. Møller-Mærsk A/S, Annual Report 2017, 9 février 2018, https://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf

Chroniques publiées sur elegartech.fr

- « Hélios, l'efficience comptable sans plan de secours », 11 juin 2026, https://elegartech.fr/articles/helios-l-efficience-comptable-sans-plan-de-secours
- « Tchap, l'accident normal de la souveraineté », 2 juillet 2026, https://elegartech.fr/articles/tchap-l-accident-normal-de-la-souverainete

- « NIS2 : la France condamnée à l'astreinte pendant que le référentiel cyber s'impose aux collectivités », 3 octobre 2026, https://elegartech.fr/articles/nis2-la-france-condamnee-a-l-astreinte-pendant-que-le-referentiel-cyber-s-impose-aux-collectivites