ROOT CAUSE Act : l'enquêteur logé chez ceux qu'il examine

Le 17 novembre 2026, un élu républicain et un élu démocrate ont déposé à la Chambre des représentants un texte qui créerait un bureau fédéral d'enquête sur les incidents numériques graves, même lorsque aucune attaque n'est en cause. La presse l'a présenté comme une réponse à la série de pannes de la mi-novembre. Il montre surtout ce qui a manqué cette semaine-là : une instance qui établit les causes sans désigner de coupable, ce que le psychologue James Reason appelait une culture juste. Le texte en reprend presque toutes les protections, sauf une : la séparation entre l'enquêteur et ceux qu'il devra examiner.

Par Alexandre Berge · 27 novembre 2026 · 15 min de lecture · Actualité

Une semaine de pannes, autant d'explications, puis un texte de loi

À la date du 23 novembre 2026, la séquence se résume ainsi. Le jeudi 12 novembre, une panne a frappé la messagerie et les outils de la suite Microsoft 365. Le représentant Andy Ogles l'a qualifiée, selon Nextgov, de « global Outlook outage » (panne mondiale d'Outlook). Le lendemain, la Federal Aviation Administration (FAA, l'autorité fédérale de l'aviation civile) a suspendu les départs dans tout le pays, ce qui a retardé plus de 10 000 vols selon le même titre. Dans les jours suivants, le réseau classifié de la National Security Agency (NSA) a ralenti le travail des analystes. Fortune rapporte que Bank of America, Wells Fargo et JPMorgan Chase ont connu des interruptions de service la même semaine. Selon Nextgov, les autorités n'ont attribué à une cyberattaque ni la panne de la FAA ni celle de Microsoft.

Le 17 novembre, Morgan Luttrell, représentant républicain du Texas, a déposé le texte H.R. 11046, avec Ritchie Torres, démocrate de New York, comme coauteur d'origine. Son intitulé (« Reviewing Origins, Outcomes, and Threats from Cyber and Artificial Intelligence to Understand Security Events Act ») forme l'acronyme ROOT CAUSE Act. Il créerait au sein de la Cybersecurity and Infrastructure Security Agency (CISA, l'agence fédérale chargée de la cybersécurité des infrastructures) un National Cyber and AI Investigations Board. Ce bureau établirait les causes profondes des incidents graves et recommanderait des mesures contre leur répétition. Le communiqué publié le 18 novembre par les républicains de la commission de la sécurité intérieure précise qu'il n'aurait « no regulatory or enforcement authority » (aucun pouvoir de réglementation ni de sanction), et que ses travaux n'imputeraient aucune responsabilité civile ou pénale. D'après Nextgov, le bureau pourrait examiner des

perturbations causées par des mises à jour défectueuses, des erreurs de configuration ou des défaillances d'intelligence artificielle, même sans indice d'attaque. Les systèmes de sécurité nationale, comme celui de la NSA, resteraient hors de son champ.

À la date d'arrêt des faits, la dernière action enregistrée est le renvoi du texte devant la commission de la sécurité intérieure de la Chambre, le jour même du dépôt. Ritchie Torres en reste le seul coauteur, et la fiche officielle de suivi ne mentionne aucun texte lié. Nextgov rappelle que les démocrates prendront le contrôle du Congrès en janvier, et que Bennie Thompson devrait alors présider la commission.

La couverture a raconté cette semaine à travers une question : l'intelligence artificielle est-elle responsable ? Fortune a titré sur le volume inédit de correctifs logiciels que provoque la découverte de failles par l'IA. Le magazine rappelle, d'après CNBC, que Bank of America a engagé 1 000 prestataires, en plus de 3 000 salariés, pour corriger les failles révélées par le modèle Mythos d'Anthropic.

Chaque panne a reçu une cause, aucune n'a reçu d'enquête

Mises côte à côte, les explications publiques de la semaine ne viennent pas du même endroit. La NSA a attribué la perturbation à une opération de maintenance, selon Nextgov. L'équipe du sénateur Mark Warner a relié, selon Fortune, des correctifs mal déployés à la panne de la NSA et aux pannes bancaires. JPMorgan Chase a évoqué devant le même titre « a temporary issue related to a software bug in on-premise hardware systems » (un problème temporaire lié à un bogue logiciel dans des matériels hébergés sur site), en écartant tout rôle des outils d'IA. Satya Nadella, directeur général de Microsoft, a indiqué au DealBook Summit du New York Times, selon Fortune, que l'entreprise avait appliqué au moins trois correctifs critiques le jour même. Pour sa propre panne, Microsoft avait annoncé l'annulation d'un changement récent de configuration réseau. La chronique publiée le 20 novembre a montré comment, à la FAA, l'explication officielle s'est fixée sur l'âge des équipements, puis sur le prestataire.

Ces récits ne se contredisent pas tous. Aucun, pourtant, ne vient d'une instance qui aurait eu accès à l'ensemble des éléments, entendu toutes les parties et publié une analyse opposable aux autres. Chaque cause a été énoncée par l'organisation touchée, par un élu ou par un dirigeant d'entreprise, au moment et dans les termes qui lui revenaient. Ce constat ne prête d'intention à personne. Il décrit une structure : **en l'absence d'enquêteur, la cause d'une panne est celle que donne le premier qui s'exprime, depuis la place qu'il occupe**.

Reason a décrit la pente que suit alors l'explication. Blâmer des individus, observait-il en 2000, satisfait davantage que mettre en cause des institutions. Un routeur, un prestataire, un système vieillissant ou un outil d'IA trop zélé fournissent des causes nettes. Les décisions qui ont fixé le calendrier des correctifs, le budget de modernisation ou le contrôle des sous-traitants en fournissent de beaucoup moins confortables, et personne n'a reçu mandat pour aller les chercher.

> **La culture juste (James Reason, 1997)**
>
> Le psychologue britannique James Reason a développé la notion de *just culture* (culture juste) dans *Managing the Risks of Organizational Accidents* (Ashgate, 1997). Il la reprend en 2000 dans le *British Medical Journal* : une culture du signalement repose sur la confiance, et cette confiance suppose une compréhension collective de la ligne qui sépare les actes non blâmables des actes blâmables. La culture juste n'est donc pas l'absence de sanction. C'est une ligne tracée à l'avance, qui permet aux témoins de dire ce qu'ils savent sans que leur témoignage serve à les condamner. Elle s'appuie sur l'*approche système* du même auteur, pour qui les erreurs visibles découlent de *conditions latentes* installées en amont par des décisions de conception, de procédure et de direction.

La culture juste sépare ce qui s'apprend de ce qui se sanctionne

Reason oppose deux lectures de l'erreur. L'approche par la personne cherche qui a failli. L'approche système demande « not who blundered, but how and why the defences failed » (non pas qui a commis la bévue, mais comment et pourquoi les défenses ont cédé). Derrière les défaillances actives, comme un geste technique raté, il place des conditions latentes nées des décisions des concepteurs, des constructeurs, des rédacteurs de procédures et de la direction générale. Une enquête qui s'arrête au routeur ou au correctif ne voit que la première couche.

Le texte déposé traduit cette distinction en droit, presque terme à terme. Le bureau peut établir des constats sur « any act, omission, practice, or decision » (tout acte, omission, pratique ou décision) ayant contribué à l'incident. Il lui est interdit, en revanche, de déterminer les droits ou les responsabilités de quiconque et d'imputer une culpabilité civile ou pénale. Il juge l'efficacité des mesures prises à partir des informations raisonnablement disponibles au moment de l'incident, ce qui écarte le *biais rétrospectif* (la tendance à juger une décision passée avec ce qui n'a été su qu'après). L'article 2258(c) ajoute qu'aucune partie d'un rapport, final ou provisoire, ne peut faire l'objet d'une communication de pièces, être admise comme preuve ni servir dans une procédure civile, administrative ou devant un État fédéré. Les informations transmises volontairement échappent à la loi sur l'accès aux documents administratifs (le Freedom of Information Act), et l'identité de ceux qui les fournissent ne peut être révélée sans leur accord.

Ce dispositif correspond à la ligne tracée par Reason : nommer les décisions sans juger les personnes. Il permet d'atteindre les conditions latentes, parce que ceux qui les ont produites peuvent parler sans que leur témoignage devienne une pièce à charge. **Sans cette séparation, une enquête désigne au mieux un coupable, et explique rarement quoi que ce soit.** Encore faut-il que l'instance qui recueille ces témoignages survive à ceux qu'elle dérange.

Le précédent du CSRB montre ce que coûte une instance révocable

Washington a déjà essayé. Le décret présidentiel 14028 du 12 mai 2021 a prévu un Cyber Safety Review Board (CSRB), que le ministre de la Sécurité intérieure a installé en février 2022. Le bureau a publié un rapport sur la vulnérabilité Log4j le 11 juillet 2022, puis un rapport sur le groupe Lapsus$, rendu public le 10 août 2023. Son rapport sur l'intrusion du groupe Storm-0558 dans la messagerie en ligne de Microsoft, daté du 20 mars 2024 et publié le 2 avril, établissait que les attaquants avaient compromis les boîtes Exchange Online de 22 organisations et de plus de 500 personnes. Il concluait que l'intrusion avait réussi « because of a cascade of security failures at Microsoft » (en raison d'une cascade de défaillances de sécurité chez Microsoft).

Le 20 janvier 2025, jour de l'investiture, une note du ministre par intérim Benjamine Huffman a mis fin à toutes les nominations dans les comités consultatifs du ministère, CSRB compris, selon TechTarget et Dark Reading. Le bureau enquêtait alors sur l'intrusion du groupe Salt Typhoon dans les réseaux de télécommunications américains. Une instance créée par décision de l'exécutif a disparu par décision de l'exécutif.

Le ROOT CAUSE Act répond explicitement à cette fragilité. L'article 2261 interdit de supprimer, suspendre ou fusionner le bureau, comme de transférer ses fonctions, sans nouvelle loi. Aucun responsable ne peut modifier ni étouffer ses constats, et le bureau tient un registre des démarches extérieures visant à influencer une enquête. Le ministre doit notifier au Congrès toute révocation d'un membre dans les quinze jours, avec ses motifs.

Ces garanties sont réelles. Elles laissent pourtant intacte une dépendance de structure. Les neuf membres votants seraient nommés par le ministre de la Sécurité intérieure, dont trois membres à temps plein (le président compris) choisis parmi les agents du ministère, et le ministre conserverait le pouvoir de révocation. Le bureau siégerait au sein de la CISA, qui lui fournirait personnel et moyens jusqu'au vote des premiers crédits. Il devrait pourtant évaluer l'action de cette même agence avec la rigueur appliquée à toute autre entité, en écartant les agents personnellement impliqués. Le ministre ou le directeur de l'agence pourrait publier ses observations écrites à côté du rapport. **Le texte admet donc que l'agence d'accueil peut figurer parmi les causes, sans en tirer la conséquence institutionnelle.**

En 1974, le NTSB a quitté le ministère qu'il devait examiner

Le modèle invoqué a connu exactement cette tension. Le National Transportation Safety Board (NTSB, le bureau fédéral d'enquête sur les accidents de transport) a été créé en 1967 comme agence indépendante, mais logée au sein du nouveau ministère des Transports. Ce ministère exerce des responsabilités opérationnelles et réglementaires étendues, à commencer par la tutelle de la FAA. En 1974, le Congrès a refait du NTSB une entité extérieure au ministère. Il estimait, rappelle l'agence, qu'une autorité fédérale ne peut mener correctement des enquêtes que si elle est totalement séparée de toute autre agence. Le

motif est précisé : un accident peut révéler des défaillances du système dont le ministère a la charge.

L'architecture s'est complétée d'une protection procédurale. L'article 1154(b) du titre 49 du Code des États-Unis dispose qu'aucune partie d'un rapport du NTSB ne peut être admise comme preuve ni utilisée dans une action civile en dommages et intérêts. Au niveau international, l'Annexe 13 à la convention de Chicago fixe à l'enquête le seul objectif de prévenir les accidents, et la réunion spécialisée de l'Organisation de l'aviation civile internationale de 1974 a admis qu'elle n'a pas pour objet de répartir les fautes ou les responsabilités. Le NTSB déclare avoir émis plus de 15 700 recommandations à plus de 2 470 destinataires, et indique que l'action recommandée a été mise en œuvre pour 82 % des plus de 13 000 recommandations clôturées. Ces chiffres sont ceux de l'agence elle-même.

Le ROOT CAUSE Act reprend les deux protections, et élargit même la seconde aux procédures administratives. Il place pourtant son bureau là où le NTSB se trouvait avant 1974 : à l'intérieur de l'administration dont il pourrait avoir à examiner les décisions. Le texte ne l'ignore pas. Son article 2260(g) prévoit, trois ans après la première réunion puis tous les quatre ans, une évaluation qui devra examiner si le bureau doit devenir une agence indépendante. **La question de 1974 est posée, puis renvoyée à plus tard.**

Partout où le retour d'expérience relève de ceux qu'il examine

Le mécanisme se décrit sans aucun nom d'organisation : **lorsque l'instance qui établit les causes d'une défaillance dépend de ceux dont les décisions pourraient figurer parmi ces causes, l'imputation se reporte sur ce qui ne proteste pas, comme le matériel, l'ancienneté, le prestataire ou l'erreur de l'opérateur.** La protection des témoins ne suffit pas à l'empêcher. Elle délie la parole des opérateurs, mais pas celle de l'enquêteur à l'égard de son employeur.

Le mécanisme se reproduit dans toute organisation où trois conditions se cumulent. La première est un retour d'expérience rédigé par l'équipe qui a opéré le changement, ou par une fonction rattachée à la direction qui a arbitré le budget, le calendrier ou le choix du fournisseur. La deuxième est la possibilité d'utiliser ce document hors de l'apprentissage, dans un litige avec un prestataire ou une procédure disciplinaire, ce qui conduit chacun à calibrer son témoignage. La troisième est l'absence de tout tiers mandaté pour confronter le récit de l'organisation cliente à celui de son fournisseur.

Les signes se voient de l'extérieur du service concerné. Les analyses d'incident concluent à l'« erreur humaine » ou à la défaillance du prestataire. Leurs recommandations portent sur la technique, jamais sur les arbitrages qui l'ont précédée. L'examen s'arrête une fois les pénalités contractuelles réglées. Un même incident reçoit deux causes selon qu'il est raconté par la direction des systèmes d'information ou par le fournisseur. Dans ces organisations, ce n'est pas la rigueur technique qui manque au retour d'expérience. C'est une position depuis

laquelle les conditions latentes peuvent être dites.

> **Grille de lecture**
>
> 1. Qui rédige l'analyse d'un incident majeur, et à qui cette personne rend-elle compte ?
> 2. Le document d'analyse peut-il être versé à un dossier disciplinaire ou à un litige avec un fournisseur ?
> 3. Sur les trois derniers incidents majeurs, combien de recommandations portaient sur une décision de direction (budget, calendrier, choix de prestataire) plutôt que sur un composant technique ?
> 4. Lorsque le client et le prestataire donnent deux causes différentes au même incident, quelle instance tranche, et sa conclusion est-elle écrite ?

Conclusion

La semaine du 12 novembre 2026 a produit autant d'explications que d'acteurs. Le ROOT CAUSE Act est la reconnaissance, par deux élus de bords opposés, qu'aucune de ces explications n'avait d'auteur légitime. Il emprunte au NTSB la séparation entre causes et responsabilités, cœur de la *culture juste* décrite par James Reason, ainsi que l'interdiction d'utiliser les rapports en justice. Il ne lui emprunte pas ce qui a rendu cette séparation crédible : l'extériorité de l'enquêteur par rapport à ceux qu'il examine.

S'il n'est pas adopté avant la fin de la législature en cours, le texte devra être redéposé devant un Congrès à majorité démocrate. L'hypothèse de cette chronique est vérifiable de l'extérieur. Si la dépendance structurelle est bien le point faible du dispositif, une version redéposée avant le 30 septembre 2027 retirera la nomination des membres à la seule main du ministre de la Sécurité intérieure, ou sortira le bureau de la CISA, sans attendre l'évaluation prévue à trois ans. Second indicateur, à l'horizon du 13 novembre 2027 : si aucune des pannes de novembre 2026 n'a donné lieu à une analyse causale publiée par une instance distincte de l'organisation touchée, le manque que le texte voulait combler aura été démontré par les faits.

Note méthodologique

Cette chronique repose sur le texte de la proposition de loi, la fiche officielle de suivi du Congrès (Congress.gov et Government Publishing Office), le communiqué de la commission de la sécurité intérieure de la Chambre, les rapports du CSRB et les pages officielles du ministère de la Sécurité intérieure, du NTSB, du Code des États-Unis et de l'Organisation de l'aviation civile internationale, ainsi que sur la presse spécialisée et économique (Nextgov, Fortune, CyberScoop, TechTarget, Dark Reading). La fiche du Congrès date le dépôt du 17 novembre 2026, alors que le communiqué et Nextgov le présentent le 18 : la date officielle est retenue. Les causes des pannes de novembre 2026 sont attribuées à ceux qui les ont énoncées, aucune n'ayant fait l'objet d'une enquête publique à la date d'arrêt des faits, le 23

novembre 2026. Le choix de la *culture juste* de James Reason, de préférence aux *accidents normaux* de Charles Perrow déjà mobilisés sur elegartech.fr, ainsi que celui du NTSB comme parallèle historique, relèvent de l'auteur. 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

Textes officiels et documents d'autorités

U.S. House of Representatives, Committee on Homeland Security, texte de la proposition « Reviewing Origins, Outcomes, and Threats from Cyber and Artificial Intelligence to Understand Security Events Act » (ROOT CAUSE Act), version datée du 13 novembre 2026, consultée le 23 novembre 2026. https://homeland.house.gov/wp-content/uploads/2026/11/ROOT-Cause-Act_Ready-for-Intro_11.16.2026.pdf

U.S. Government Publishing Office, Bill Status H.R. 11046 (119e Congrès), fichier mis à jour le 18 novembre 2026, consulté le 23 novembre 2026. https://www.govinfo.gov/bulkdata/BILLSTATUS/119/hr/BILLSTATUS-119hr11046.xml

U.S. House of Representatives, Committee on Homeland Security, « Homeland Republicans Lead Legislation to Strengthen, Modernize DHS's Cybersecurity Mission as AI Reshapes the Threat Landscape », 18 novembre 2026. https://homeland.house.gov/2026/11/18/homeland-republicans-lead-legislation-to-strengthen-modernize-dhss-cybersecurity-mission-as-ai-reshapes-the-threat-landscape/

Cyber Safety Review Board, « Review of the December 2021 Log4j Event », 11 juillet 2022. https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf

U.S. Department of Homeland Security, « Cyber Safety Review Board Releases Report on Activities of Global Extortion-Focused Hacker Group Lapsus$ », 10 août 2023. https://dhs.gov/news/2023/08/10/cyber-safety-review-board-releases-report-activities-global-extortion-focused

Cyber Safety Review Board, « Review of the Summer 2023 Microsoft Exchange Online Intrusion », 20 mars 2024. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf

U.S. Government Publishing Office, United States Code, 2024 Edition, Title 49, § 1154 « Discovery and use of cockpit and surface vehicle recordings and transcripts », consulté le 23 novembre 2026. https://www.govinfo.gov/content/pkg/USCODE-2024-title49/html/USCODE-2024-title49-subtitleII-chap11-subchapIV-sec1154.htm

National Transportation Safety Board, « History of The National Transportation Safety Board », page mise à jour le 21 octobre 2026, consultée le 23 novembre 2026. https://www.ntsb.gov/about/history/Pages/default.aspx

Organisation de l'aviation civile internationale, « The Postal History of ICAO », page Annex 13 « Aircraft Accident and Incident Investigation », consultée le 23 novembre 2026. https://www.icao.int/sites/default/files/postalhistory/annex_13_aircraft_accident_and_incident_investigation.htm

Presse de référence

David DiMolfetta, Nextgov/FCW, « Bipartisan bill would create cyber and AI review board amid series of tech outages », 18 novembre 2026. https://www.nextgov.com/policy/2026/11/bipartisan-bill-would-create-cyber-and-ai-review-board-amid-series-tech-outages/417299/

Emily Forlini, Fortune, « Behind the recent wave of IT outages: AI is driving an unprecedented number of software patches », 18 novembre 2026, mis à jour le 20 novembre 2026. https://fortune.com/2026/11/18/ai-played-a-major-role-in-the-nsa-banking-outages-but-not-in-the-way-you-may-think/

Elias Groll, CyberScoop, « Cyber review board blames cascading Microsoft failures for Chinese hack », 2 avril 2024. https://cyberscoop.com/microsoft-csrb-china-hacking/

Alexander Culafi, TechTarget, « Former CSRB members largely silent on dismissal », 27 janvier 2025. https://www.techtarget.com/cybersecurity/news/366618514/Former-CSRB-members-largely-silent-on-dismissal

Becky Bracken, Dark Reading, « Trump Fires Cyber Safety Board Investigating Salt Typhoon Hackers », mis à jour le 22 janvier 2025. https://www.darkreading.com/threat-intelligence/trump-fires-cyber-safety-board-salt-typhoon-hackers

Cadre théorique

James Reason, « Human error: models and management », *BMJ*, vol. 320, n° 7237, 18 mars 2000, p. 768-770. https://pmc.ncbi.nlm.nih.gov/articles/PMC1117770/

Chroniques publiées sur elegartech.fr

« Panne FAA : l'âge, le prestataire, jamais le changement », 20 novembre 2026. https://elegartech.fr/articles/panne-faa-l-age-le-prestataire-jamais-le-changement

« Panne Microsoft 365 : quand la crise perd son canal », 16 novembre 2026. https://elegartech.fr/articles/panne-microsoft-365-quand-la-crise-perd-son-canal

« Tchap, l'accident normal de la souveraineté », 2 juillet 2026. https://elegartech.fr/articles/tchap-l-accident-normal-de-la-souveranete