

La souveraineté a un bus factor

Sept sites sur dix attendaient un Tchèque.

Ce que la semaine PHP2Shell dit de nos fondations numériques.

La souveraineté numérique se discute entre États et hyperscalers. Elle se décide à deux étages que personne ne regarde : des fondations financées par ces mêmes hyperscalers, et des individus qui ne doivent contractuellement rien à personne.

Bruno DE SAN NICOLAS

L'atelier de BDSN



Le mercredi 21 octobre, à 16 heures, sept sites web sur dix attendaient un Tchèque.

Pas une entreprise. Pas un État. Un homme, ingénieur DNS le jour, empaqueteur bénévole de PHP la nuit, qui a confié à la BBC se sentir « responsable de tous ces gens » et ne pas pouvoir les laisser tomber ¹. Vous venez de lire le contrat de service de l'internet mondial.

Vous voulez vous émanciper des hyperscalers ? Très bien. Moi aussi. Mais de qui dépend votre plan de secours ? D'un bénévole, d'une fondation que financent ces mêmes hyperscalers, et d'une licence qui dit « AS IS, WITHOUT WARRANTY ». La souveraineté a un bus factor. Personne ne l'a mesuré.

Le bus factor, pour ceux qui n'ont pas la chance de vivre entourés d'informaticiens, c'est le nombre de personnes qu'un autobus devrait renverser pour qu'un projet s'arrête. Quand il vaut un, on ne parle plus de risque. On parle de pari.



Illustration générée avec Gemini pour L'Atelier de BDSN.

I. Un Tchèque, un week-end, sept sites sur dix

Reprenons depuis le début. PHP est un langage de programmation vieux de trente ans. Vous ne le voyez jamais, mais il fait tourner WordPress, Drupal et, on l'a découvert cette semaine, les sites de nos préfectures ². Sept sites web sur dix dont on connaît le langage serveur sont écrits en PHP ³.

Cet été, des chercheurs assistés par des modèles d'intelligence artificielle ont trouvé deux failles dans le moteur même du langage. Présentes depuis 2012. Permettant de prendre le contrôle d'un serveur sans mot de passe. Une publication coordonnée fut organisée pour le 22 octobre, sous embargo : les correctifs circulent sous le manteau, chez les distributeurs, avant d'être rendus publics. Le 20 au soir, les identifiants des failles ont fuité, une vidéo de démonstration a été mise en ligne par erreur, et le lendemain matin un fournisseur d'images logicielles a publié ses correctifs six heures avant l'heure convenue, en invoquant des attaques déjà en cours ⁴. L'embargo était mort. La publication fut avancée d'un jour.

Résultat : la NSA et son homologue britannique ont recommandé de débrancher ce qui ne pouvait pas être corrigé immédiatement ⁵. Aux Pays-Bas, l'identité numérique DigiD et le site du Parlement ont été coupés par précaution. En France, le ministère de l'Intérieur a placé ses sites exposés en « maintenance préventive » à la demande de l'ANSSI ; les préfectures se sont tues à 14 heures ⁶. Cloudflare a compté des millions de tentatives d'attaque dans la journée ⁷.

Et dans tout cela, Ondřej Surý. Directeur de l'ingénierie DNS (l'annuaire de l'internet) dans une organisation à but non lucratif américaine, il tient depuis plus de vingt ans, sur son temps libre, les paquets PHP de Debian et d'Ubuntu, les deux distributions Linux les plus répandues sur les serveurs. Le travail d'un empaqueteur, pour le dire simplement : le projet PHP publie une recette ; lui en fait un plat prêt à servir, que n'importe quel administrateur installe en une commande. Sans lui, le correctif existe, mais il ne protège personne.

Prévenu sous embargo, il a vu la date avancer et a dit n'avoir « pas tant de temps que ça » pour préparer ses paquets ¹. Il a tout lâché. Il a livré le jour même, y compris pour des versions de PHP que le projet lui-même n'entretient plus ⁸. Son dépôt a plié sous la charge, certaines architectures ont pris du retard, et il a lâché, dans le fil de discussion de son projet, cette phrase qu'il faudrait encadrer : « Peut-être que je vous rends un mauvais service en rafistolant les vieilles versions, et que je devrais arrêter ? » ⁹. Il a reçu plus de 10 000 dollars de dons en quelques jours, « à peu près une année de contributions » au rythme habituel ¹. Sa page de parrainage, consultée ce dimanche, affiche 142 parrains et 6 % de l'objectif mensuel qu'il s'est fixé ⁹. Quand la journaliste lui a demandé si l'essentiel de la responsabilité reposait sur lui, il a répondu : « Oui, c'est à peu près vrai. » Ses collègues de l'entreprise Freexian pourraient reprendre, dit-il, mais ils n'ont pas encore son expérience accumulée ¹.

Vingt ans. Un homme. Sept sites sur dix. Et, pour sa relève, une page de dons.

Je précise tout de suite qu'il n'était pas seul : d'autres empaqueteurs, dans d'autres distributions, ont fait la même chose. C'est précisément le problème. Ils sont quelques dizaines, ils ont presque tous un autre travail, et aucun d'entre eux n'a signé quoi que ce soit.

II. Le web est libre, au sens de gratuit

Le mot « libre » prête à confusion. Un logiciel libre n'est pas un logiciel sans propriétaire : son code est public, chacun peut l'utiliser, le modifier, le redistribuer. Gratuit, le plus souvent. Garanti, jamais.

Or c'est sur ce socle que tout repose. Neuf serveurs web sur dix tournent sous Linux ou un cousin Unix ¹⁰. Sept sites sur dix sont en PHP, quatre sur dix sous WordPress ^{3, 11}. Près des deux tiers des sites tiennent leur cadenas, celui que vous voyez dans votre navigateur, d'une association à but non lucratif, Let's Encrypt ¹². Neuf serveurs sur dix accessibles à distance le sont par OpenSSH, un projet porté par les développeurs d'OpenBSD et financé par des dons ¹³. Le navigateur Chrome et son clone Edge, près des trois quarts du marché, sont bâtis sur Chromium, un projet libre ¹⁴. Et quand les auditeurs ouvrent le capot des logiciels commerciaux, ils trouvent de l'open source dans 98 % des bases de code, où il représente près des trois quarts des lignes ¹⁵.

Des économistes de Harvard ont tenté le calcul. Refaire tout le logiciel libre existant coûterait environ 4 milliards de dollars. Ce que les entreprises devraient dépenser s'il n'existait pas : 8 800 milliards. Sans lui, elles paieraient leur informatique trois fois et demie plus cher ¹⁶. La Commission européenne, plus modeste, estime sa contribution au PIB de l'Union entre 65 et 95 milliards d'euros par an ¹⁷.

Retenez le ratio : deux mille pour un. Le logiciel libre est l'actif le plus rentable de l'histoire économique. C'est aussi le seul dont personne n'a signé la garantie.

Et c'est la première chose que les débats sur le cloud souverain oublient. On discute de la salle des machines, de qui possède le bâtiment, de quelle loi s'applique aux disques. Mais le logiciel qui tourne dedans est le même à Paris, à Francfort et en Virginie. Libre, gratuit, et entretenu par des gens qui ne vous ont rien promis.

III. Qui paie ? Les mêmes

Deuxième illusion : « l'open source nous émancipe des géants américains ». Regardons qui paie.

La Linux Foundation, qui héberge le noyau Linux et près de quinze cents autres projets, prévoit 311 millions de dollars de revenus en 2025¹⁸. Ses membres Platinum, à 500 000 dollars par an avec siège au conseil, s'appellent Google, Microsoft, Meta, Huawei, Oracle, Samsung et, depuis le 7 octobre, AWS¹⁹. Plus de 90 % du code du noyau Linux est écrit par des salariés d'entreprises ; les bénévoles, qui en faisaient 15 % à la fin des années 2000, en faisaient 6 % dix ans plus tard²⁰. Linus Torvalds lui-même est salarié de la fondation²¹. Et sur ces 311 millions, le projet noyau Linux, celui qui fait tourner la planète, en reçoit 8,4. Trois pour cent¹⁸.

La fondation Apache ? Ses Platinum s'appellent Apple, AWS, Google, Meta, Microsoft, Huawei²². Le fonds Alpha-Omega, créé pour sécuriser les projets critiques ? Cinq millions de départ de Microsoft et Google, abondés depuis par AWS, puis en mars 2026 par les grands laboratoires d'IA²³. L'étude de faisabilité d'un fonds souverain européen pour le logiciel libre, remise en juillet 2025 ? Commandée par GitHub, filiale de Microsoft²⁴.

Soyons justes, car le texte perdrait toute crédibilité à crier au complot : cet argent est aussi ce qui fait tourner Linux. Le problème n'est pas que les géants paient. C'est qu'ils paient ce qu'ils veulent, quand ils veulent, où ils veulent. La PHP Foundation, qui porte sept sites sur dix, vit avec moins d'un million de dollars par an, a terminé 2025 en déficit, et son troisième financeur depuis sa création n'est ni Google ni Amazon : c'est l'agence publique allemande Sovereign Tech Agency²⁵. Alpha-Omega ne lui a rien versé en 2024 ni en 2025²³.

Les fondations sont aussi le lieu où les géants défendent leurs intérêts. Quand Redis et HashiCorp ont restreint leurs licences pour se protéger des hyperscalers, les scissions (les « forks ») ont surgi en quelques semaines sous la bannière de la Linux Foundation : Valkey, porté par AWS, Google et Oracle ; OpenTofu, avec dix-huit développeurs à temps plein promis sur cinq ans par ses soutiens²⁶. Victoire du libre, dit-on. Victoire, surtout, de ceux qui avaient les moyens de payer.

S'émanciper des hyperscalers par l'open source, c'est donc passer du contrat au don. On change de dépendance. On ne change pas de dépendant.

IV. Le facteur Nebraska

Il existe un dessin célèbre, publié en 2020 par xkcd : une tour d'infrastructure numérique, immense, toute l'économie moderne empilée dessus, tenant sur une petite pièce fine, tout en bas, légendée « un projet qu'une personne au hasard dans le Nebraska maintient sans remerciement depuis 2003 »²⁷. On en rit. Puis on mesure.



Le facteur Nebraska, revisité. Illustration générée avec Gemini pour L'Atelier de BDSN.

L'université Harvard et la Linux Foundation l'ont fait : 136 développeurs écrivent plus de 80 % du code des 50 bibliothèques les plus utilisées au monde ; près d'un projet sur quatre dépend d'une seule personne pour plus de 80 % de son code²⁸. Une étude académique devenue classique : deux projets populaires sur trois ont un bus factor de deux ou moins²⁹. Les mainteneurs eux-mêmes, interrogés en 2024 : 60 % ne sont pas payés, 60 % ont arrêté ou envisagé d'arrêter. Et la relève ne vient pas : la part des mainteneurs de moins de 26 ans est passée de 25 % à 10 % en trois ans³⁰.

La galerie des incidents n'est qu'une suite de visages. 2014, Heartbleed : la faille d'OpenSSL, la bibliothèque qui chiffre le web, expose un demi-million de sites de confiance. Le projet avait un seul développeur à temps plein et recevait 2 000 dollars de dons par an. Son président écrivit : « je vieillis, je suis las, et j'aimerais prendre ma retraite un jour »³¹. 2021, Log4Shell : une bibliothèque Java enfouie dans des dizaines de milliers de composants logiciels ; ses mainteneurs écrivent qu'ils travaillent « sans dormir » sur un travail « pour lequel nous ne sommes pas payés » ; un seul ministère américain y consacra 33 000 heures³². 2024, xz : un mainteneur seul écrit en 2022 que sa « capacité à s'en soucier » est limitée par des problèmes de santé mentale, qu'il s'agit d'un « projet de loisir non payé » ; un faux contributeur, patient, le soulage pendant deux ans, puis glisse une porte dérobée dans un composant présent sur à peu près tous les serveurs Linux. Elle est découverte par hasard, par un ingénieur intrigué par une demi-seconde de latence. L'agence américaine de cybersécurité conclut : « la prochaine fois, nous n'aurons peut-être pas cette chance »³³.

Je pourrais continuer : core-js, présent sur la moitié des mille premiers sites mondiaux, dont l'auteur touchait 400 dollars par mois pour 250 heures de travail³⁴ ; curl, embarqué vingt milliards de fois, dans votre voiture, votre télévision et votre téléphone, dont l'équipe de six personnes écrivait le 20 octobre dernier être « tendue, surchargée, au bord du gouffre »³⁵.

Et Torvalds, me direz-vous ? Linus Torvalds a 56 ans. Il tient le noyau Linux depuis 1991, en est l'autorité finale, et le noyau est le projet libre le mieux doté de la planète : 2 141 développeurs et 227 employeurs sur la seule version 6.19, sortie en février³⁶. Son plan de continuité a été écrit en janvier 2026. C'est un fichier texte. Il prévoit, si Linus venait à disparaître, soixante-douze heures de délibération entre mainteneurs pour désigner un successeur. Il ne contient aucun nom. Un des plus anciens mainteneurs l'a jugé « trop optimiste pour un plan de contingence »³⁷.

Torvalds n'est donc pas l'exemple de la fragilité. Il est l'exemple du déni : si le projet le plus riche, le plus peuplé, le plus scruté du logiciel libre n'a pas de relève nommée, imaginez les paquets PHP de Debian.

On ne s'émancipe pas d'un individu. On institutionnalise sa fonction, ou l'on prie. Certains l'ont fait : SQLite, la base de données la plus déployée au monde, est tenue par une poignée de développeurs, tous salariés d'une société qu'un consortium d'industriels finance à 150 000 dollars par an et par membre³⁸. OpenSSL, après Heartbleed, a fini par créer une société de services : vingt et une personnes, à Brno, qui vivent de contrats de support et financent plus de 70 % du budget de la fondation³⁹. Ce n'est pas la charité qui les a sauvés. C'est le contrat.

Appelons cela la dette d'altruisme : un passif que personne n'inscrit au bilan, et que l'on découvre le jour où le bénévole tombe malade, se lasse, ou se fait infiltrer.

V. L'urgence sans contrat

Car le contrat, précisément, n'existe pas. Ouvrez n'importe quelle licence libre. MIT : le logiciel est fourni « en l'état, sans garantie d'aucune sorte ». GPL : « il n'y a aucune garantie pour le programme ». Apache : idem⁴⁰. Un mainteneur l'a écrit sans détour en 2022 : « Si vous utilisez ceci, je ne vous dois rien. Rien du tout. »⁴¹. Ils ont raison. Ce sont les conditions que vous acceptez en téléchargeant.

Le législateur européen l'a compris et, à mon sens, bien compris. Le Cyber Resilience Act, qui s'applique par étapes depuis septembre, exempte explicitement les développeurs bénévoles ; il invente pour les fondations un statut d'intendant (« steward ») sans amende possible ; il fait peser les obligations sur ceux qui intègrent et vendent : diligence, nomenclature des composants, correction des failles⁴². Faire peser une obligation de résultat sur un bénévole, c'est le faire partir. En revanche, le texte crée une asymétrie curieuse : le fabricant doit désormais signaler à l'amont les failles qu'il trouve et lui transmettre ses correctifs. Autrement dit, une obligation d'écrire à quelqu'un qui ne vous doit rien, sans un euro en face⁴². NIS2 et DORA, de leur côté, exigent que banques et opérateurs critiques inventorient et évaluent leurs « fournisseurs » logiciels, y compris libres⁴³. Des fournisseurs qui n'ont rien fourni, qui n'ont rien signé, et qui ne répondront pas au téléphone.

La semaine PHP2Shell montre ce que cela donne quand l'amont manque de bras. La PHP Foundation : une salariée à temps plein, sa directrice, et quatorze contractants pour la plupart à temps partiel⁴⁴. En 2024, le premier audit de sécurité externe de l'histoire de PHP, financé par l'agence publique allemande et réalisé par une société française, avait repéré les premiers signes de la faille ; faute de budget, il s'était limité aux composants les plus critiques⁴⁵. Pas de chemin d'attaque démontré. Trois correctifs possibles,

chacun avec son inconvénient. Une équipe qui décide par consensus et qui, faute de bras et d'accord, laisse dormir le sujet pendant près de deux ans. La fondation l'écrit elle-même, le jour du correctif : « ce retard a été un échec structurel, dû à la fois au processus de décision de l'équipe de sécurité et à son manque de ressources »⁴⁵. Elle est passée au vote majoritaire et a recruté deux ingénieurs cet été. Avec quel argent ? Celui qu'elle n'a pas.

Pendant ce temps, l'autre plateau de la balance s'alourdit. Les failles de PHP ont été trouvées par trois équipes de chercheurs, dont l'une associée à un programme d'OpenAI, à l'aide de modèles d'OpenAI et de Google ; selon eux, un chercheur a fait en une semaine ce qui aurait pris des mois à une équipe⁴⁶. La fondation reçoit deux fois plus de propositions de modification qu'il y a un an, sans deux fois plus de relecteurs ; depuis juillet, quinze failles publiées et plus de cent signalements invalides à trier⁴⁵. Le mainteneur de curl a dû fermer son programme de primes, submergé de rapports générés par IA⁴⁷. Sam Altman déclarait jeudi soir : « je ne pense plus que nous pourrions corriger tous les bugs »⁴⁸. Surý, plus sobrement : « ce ne sera peut-être pas un incident isolé »¹.

Appliquons le test que j'ai proposé dans un précédent essai : qui parle, qui y gagne, dans quelle unité, qui peut vérifier. Qui parle ? Les laboratoires d'IA. Qui y gagne ? Ceux qui vendent la découverte. Dans quelle unité ? En failles trouvées, jamais en failles corrigées. Les chiffres existent, et ils sont cruels : un programme lancé au printemps par Anthropic avait divulgué 530 vulnérabilités en un mois ; 75 étaient corrigées fin mai, et des mainteneurs demandaient qu'on ralentisse. En octobre, un décompte de la Cloud Security Alliance donnait 97 corrections pour 1 596 signalements, six pour cent, et plusieurs canaux de signalement fermés faute de bras, dont celui de curl⁴⁹. Un chercheur américain a chiffré, dès août 2025, ce qu'il en coûterait de corriger plutôt que de trouver : 2,4 milliards de dollars, dans une « opération Patchlight » que personne n'a reprise⁴⁹. Un institut britannique l'a noté sans acrimonie : la capacité de découverte est désormais financée ; la capacité de remédiation reste bénévole, et l'influence des laboratoires d'IA sur les priorités de sécurité du logiciel libre mérite d'être regardée⁵⁰. J'ajoute un détail qui devrait faire tiquer les tenants de la souveraineté : quand la vague est arrivée, ce sont les règles de filtrage de Cloudflare, société californienne, déployées avant l'aube, qui ont encaissé les premières heures⁷. Le plan de secours de l'Europe, ce mercredi-là, était américain.

VI. Quatre chantiers pour une souveraineté qui a un bus factor

Le diagnostic est posé depuis dix ans ; les rapports s'empilent. Ce qui manque, ce sont des mécanismes. En voici quatre, du plus classique au plus nouveau.

1. Financer la maintenance comme une infrastructure, pas comme une bonne œuvre.

L'Allemagne a ouvert la voie : sa Sovereign Tech Agency a commandé 41 millions d'euros de travaux de maintenance à 118 technologies en quatre ans, dont curl, OpenSSL, Log4j et PHP ; fin 2024, elle recevait déjà cinq fois plus de demandes qu'elle ne pouvait en financer, et son budget est revoté chaque année⁵¹. Sa règle vaut d'être copiée : des contrats de prestation, pas des subventions ; les associations françaises du libre, auditionnées en mai à l'Assemblée nationale, ne demandent rien d'autre⁵⁶. Et le retour d'expérience allemand enseigne une chose que les rapports oublient : une étude causale publiée en juin mesure, sur les projets financés, 144 % de modifications en plus chez les mainteneurs en place et aucun effet sur le nombre de contributeurs. L'argent accélère ceux qui sont là ; il ne fabrique pas de relève.

Log4j, financé deux ans, a vu son activité « décliner » dès la fin de la subvention⁵². Il faut donc financer des postes, pas des projets, et sur plusieurs années.

À l'échelle européenne, tout est écrit, rien n'est payé. L'étude de 2025 chiffre le minimum à 350 millions d'euros sur sept ans²⁴ : cinquante millions par an, contre 65 à 95 milliards de valeur annuelle. Un pour mille. Depuis le 3 juin, la Commission a même un nom pour cela, un « instrument de maintenance de l'open source », et un objectif d'environ deux milliards sur sept ans, public et privé confondus ; un objectif, pas un budget⁵³. L'outil existe : le consortium européen Digital Commons, installé à Paris depuis le 29 octobre 2025, dirigé depuis avril, pilote déjà un fonds avec l'agence allemande⁵⁴. En France, la commission d'enquête de l'Assemblée nationale sur nos dépendances numériques a tout écrit en juillet : une fondation « France Libre Open Source », un fonds « Logic » adossé à la Caisse des dépôts et à Bpifrance, qui pourrait « salarier des développeurs pour assurer la maintenance », l'open source obligatoire dans les marchés publics en 2030. Trois mois plus tard, aucune suite gouvernementale ; la Cour des comptes, le 22 octobre, recommandait encore de travailler davantage avec les entreprises qui maintiennent ces logiciels⁵⁵. La France a une doctrine, un catalogue, un pôle à la DINUM et des rapports parlementaires⁵⁶. Elle a tout, sauf le chéquier. Et l'acheteur public devrait faire ce que l'agence allemande lui demande depuis vendredi : inscrire la santé des dépendances critiques dans ses appels d'offres⁵⁷.

2. Contractualiser l'urgence. Si votre activité dépend d'un composant libre, achetez-lui un contrat, ou financez-en un. Cela existe, et cela se mesure. La fondation Python a embauché en 2023 un ingénieur sécurité à temps plein, payé par Alpha-Omega : ses avis de sécurité sont passés de 18 en 2024 à 175 au premier semestre 2026⁵⁸. L'agence allemande salarie désormais des mainteneurs en contrat de deux ans⁵⁸. Et la semaine PHP2Shell a départagé le contrat et le bénévolat à l'heure près : Debian a publié son avis à 15 h 45, un quart d'heure avant la sortie officielle ; Freexian, qui vend du support à long terme, a livré ses clients sur près de 120 plateformes le jour même ; les dérivés communautaires de Red Hat ont suivi quatre à dix heures plus tard, et le dépôt bénévole le plus utilisé de ce monde-là, le lendemain⁵⁹. Ce que fait OpenSSL depuis Brno vaut modèle : le support payant finance la fondation⁶⁰. Enfin, puisque l'embargo a craqué de partout cette semaine, la conduite d'embargo (qui reçoit les correctifs à l'avance, qui s'engage à ne rien publier) devrait figurer dans vos contrats de fourniture. Amazon, dont les pots de miel ont vu la première tentative d'exploitation quatre jours avant la publication, l'a résumé : un embargo ne protège les défenseurs que jusqu'à ce que quelqu'un d'autre trouve le même bug⁶¹.

3. La réserve du libre. C'est la proposition que je signe. Les armées ont des réserves : des gens formés en temps de paix, sous contrat, mobilisables en quelques heures. La cybersécurité en a aussi, en Estonie depuis 2011, au Royaume-Uni depuis 2013, en France depuis 2016, avec près de 400 réservistes opérationnels au commandement de la cyberdéfense et, depuis novembre 2025, un escadron de réserve cyber dans l'armée de l'Air et de l'Espace ; le Congrès américain a autorisé fin 2023 l'armée de terre à expérimenter une réserve civile de cybersécurité⁶². Rien de tel pour le logiciel qui fait tourner l'État. La doctrine, pourtant, existe : l'instruction du ministère des Armées de février 2019 privilégie le logiciel libre « à coût global, risques et efficacité opérationnelle comparables » et demande d'en « conserver la maîtrise en maintenant une réelle compétence technique »⁶³. La réserve du libre est l'exécution de cette phrase.

Imaginons-la : des empaqueteurs, des relecteurs, des mainteneurs identifiés à l'avance pour les composants critiques, formés aux procédures d'embargo, rémunérés pour une astreinte et mobilisés en crise. Qui la compose ? Des agents publics, et les ingénieurs de nos champions nationaux du cloud et du logiciel, mis à disposition par convention, comme on détache un réserviste. Qui l'anime ? Une agence,

nationale ou européenne. Le droit existe déjà : le mécénat de compétences permet à une entreprise de prêter un salarié jusqu'à trois ans à un organisme d'intérêt général, avec 60 % de réduction d'impôt ; la loi 3DS permet, à titre expérimental jusqu'à fin 2027, de mettre des agents publics à disposition d'associations ⁶⁴. L'Assemblée nationale a proposé en juillet qu'un agent de l'État puisse consacrer une journée par an aux communs numériques ⁵⁵. Une journée, c'est un geste. Une astreinte, c'est une capacité. Il ne manque que l'organisme qui recrute, forme et mobilise. Cette réserve ne concurrence pas les prestataires de support, elle les complète : le routinier au contrat, la crise à la réserve. Et que l'on ne s'y trompe pas : la réserve ne remplace pas les communautés, elle leur envoie des bras, sous leurs règles, dans leurs équipes. C'est ainsi que l'armée autrichienne, qui a migré seize mille postes sur LibreOffice parce qu'elle doit « pouvoir fonctionner même quand plus rien d'autre ne fonctionne », reverse ses développements au projet, et que la DINUM finance les briques amont de sa suite bureautique ⁶⁵. Je n'ai trouvé trace, en trois langues, d'aucune proposition de ce type. Le mercredi 21 octobre, cette réserve aurait livré les paquets PHP de Debian à 14 heures, et Ondřej Surý aurait pu dormir.

4. Mesurer et s'exercer. On ne gère pas ce qu'on ne mesure pas. Le bus factor se calcule ; la communauté CHAOSS l'a même rebaptisé « facteur d'absence des contributeurs » ⁶⁶. Exigez-le de vos fournisseurs, avec la nomenclature de leurs composants. Les outils de balayage comptent aujourd'hui 2,24 millions de serveurs PHP exposés sur l'internet, dont 59 % sur des branches sans correctif ; la France en compte plus de 25 000 ⁶⁷. Et faites ce que j'appelais ailleurs un exercice d'évacuation numérique : où tourne PHP chez vous, qui a le droit de le corriger, en combien d'heures. Beaucoup d'organisations ne savaient pas répondre mercredi ⁶⁸. Aux Pays-Bas, DigiD est revenu après six heures ; le centre national de cybersécurité, qui avait coupé son propre site, a publié le lendemain un arbre de décision et conclu deux jours plus tard que l'exploitation était « compliquée » ⁶⁷. On a coupé non parce qu'on était attaqué, mais parce qu'on ne pouvait pas garantir d'avoir tout corrigé à temps. On coupe parce qu'on ne sait pas.

Coda

« Je ne peux pas les laisser tomber. » Voilà, aujourd'hui, l'accord de niveau de service de l'internet mondial. Accepteriez-vous cela pour votre électricité ? Pour votre eau ?

Linus Torvalds sera remplacé un jour. La question n'est pas par qui. C'est par quoi : une institution, ou un autre inconnu du Nebraska.

La souveraineté a un bus factor. Le nôtre tient dans un fichier de 2 102 noms et dans la page de dons d'un Tchèque. Il est temps de le mesurer. Puis de le relever.

Notes

1. Shiona McCallum, « How one man became the unsung hero of the internet during a cyber-security scramble », BBC News, 25 octobre 2026. <https://www.bbc.com/news/articles/cw30ejqlj43o>
2. ActuIA, « PHP flaws: France's ANSSI orders sites offline after AI-assisted discovery », 22 octobre 2026 (alerte CERTFR-2026-ALE-014, ministère de l'Intérieur, préfectures). <https://www.actuia.com/en/news/php-flaws-frances-anssi-orders-sites-offline-after-ai-assisted-discovery/> ; CERT-FR, CERTFR-2026-ALE-014. <https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-014/>
3. W3Techs, « Usage statistics of server-side programming languages for websites », relevé du 24 octobre 2026 : PHP 69,3 % des sites dont le langage est connu. https://w3techs.com/technologies/overview/programming_language
4. The PHP Foundation, « Today's PHP Security Release, and How We're Strengthening PHP Security », 21 octobre 2026 (chronologie : fuite des identifiants CVE, vidéo publiée par erreur, images publiées six heures avant la sortie). <https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/> ; justification de Chainguard (attaques en cours) : Socket.dev, 22 octobre 2026. <https://socket.dev/blog/php-embargo-dispute> ; politique de Chainguard. <https://www.chainguard.dev/legal/coordinated-vulnerability-handling-policy>
5. NSA : The Guardian, 23 octobre 2026, via JournalArta. <https://journalarta.com/en/2026/10/24/black-october-cybersecurity-experts-ai-hacking/> ; NCSC (Royaume-Uni), « Critical security issue affecting PHP ». <https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php>
6. Pays-Bas : Rijksoverheid, 21 octobre 2026. <https://www.rijksoverheid.nl/actueel/nieuws/2026/10/21/aantal-websites-rijksverheid-preventief-offline-na-kwetsbaarheden-php> ; The Hacker News, 21 octobre 2026. <https://thehackernews.com/2026/10/php-issues-emergency-patches-for-two.html> ; France : note 2.
7. Cloudflare, « PHP vulnerabilities: WAF protection », 21 octobre 2026 (règles actives à 03:02 UTC). <https://blog.cloudflare.com/php-vulnerabilities-waf-protection> ; volumes rapportés par Matthew Prince : Reuters, 23 octobre 2026. <https://wkzo.com/2026/10/23/php-foundation-under-funded-with-one-full-time-staff-member-director-says/>
8. HeroDevs, « PHP2Shell: The Volunteer Who Patched PHP 5.6 Through 8.5 », octobre 2026. <https://www.herodevs.com/blog-posts/the-php2shell-story-the-manwho-keeps-php-running>
9. Fil de discussion du dépôt deb.sury.org, ticket #145, 21-22 octobre 2026 (« Perhaps I am doing you a disservice by patching the old crap and I should stop doing this? »). <https://codeberg.org/oerdnj/deb.sury.org/issues/145> ; page GitHub Sponsors d'Ondřej Surý, relevé du 25 octobre 2026 (142 parrains, 6 % d'un objectif de 15 000 \$/mois). <https://github.com/sponsors/oerdnj>
10. W3Techs, systèmes d'exploitation, 24 octobre 2026 : Unix 92,2 %. https://w3techs.com/technologies/overview/operating_system
11. W3Techs, systèmes de gestion de contenu, 24 octobre 2026 : WordPress 39,6 % de tous les sites. https://w3techs.com/technologies/overview/content_management
12. W3Techs, autorités de certification, 25 octobre 2026 : Let's Encrypt 64,4 % des sites. https://w3techs.com/technologies/overview/ssl_certificate
13. Liste openssl-unix-dev, 14 février 2026 (relevé Shodan : 90,2 % des serveurs SSH exposés sous OpenSSH). <https://lists.mindrot.org/pipermail/openssl-unix-dev/2026-February/042362.html>
14. StatCounter, parts de marché des navigateurs, septembre 2026. <https://gs.statcounter.com/browser-market-share> ; Microsoft, annonce du passage d'Edge à Chromium, 7 décembre 2018. <https://blogs.windows.com/msedgedev/2018/12/07/recapping-open-source-announcements/>
15. Black Duck, « Open Source Security and Risk Analysis 2026 », 25 février 2026 (98 % des 947 bases auditées). <https://www.blackduck.com/blog/open-source-security-risk-analysis.html> ; Synopsys, OSSRA 2024, 27 février 2024 (77 % du code). <https://news.synopsys.com/2024-02-27-New-Synopsys-Report-Finds-74-of-Codebases-Contained-High-Risk-Open-Source-Vulnerabilities,-Surging-54-Since-Last-Year>
16. M. Hoffmann, F. Nagle, Y. Zhou, « The Value of Open Source Software », Harvard Business School, SSRN, 16 janvier 2024. <https://papers.ssrn.com/abstract=4693148>
17. Estimation de la Commission européenne (65 à 95 Md€/an), reprise dans OpenForum Europe, « EU-STF Policy Primer », octobre 2025. <https://openforumeurope.org/wp-content/uploads/2025/10/EU-STF-Policy-Primer.pdf>
18. Linux Foundation, rapport annuel 2025, 18 décembre 2025 (revenus prévisionnels 311,3 M\$; projet noyau Linux 8,41 M\$ sur 284,8 M\$ de dépenses). https://www.linuxfoundation.org/hubfs/Publications/2025%20Linux%20Foundation%20Annual%20Report_122225a_lr.pdf
19. Linux Foundation, grille d'adhésion (Platinum 500 000 \$/an). https://www.linuxfoundation.org/hubfs/lf_mem_benefits_0010625.pdf ; AWS membre Platinum, 7 octobre 2026. <https://www.linuxfoundation.org/press/aws-becomes-a-platinum-member-of-the-linux-foundation-deepening-commitment-to-ope>

20. J. Corbet, Linux Foundation, 26 avril 2018 (bénévoles de 15 % à 6 % du code depuis le noyau 2.6.20).
<https://linuxfoundation.org/blog/jonathan-corbet-on-linux-kernel-contributions-community-and-core-needs> ; LWN, statistiques du noyau 6.19, 9 février 2026. <https://lwn.net/Articles/1057302/>
21. Linux Foundation, page « Leadership » (Linus Torvalds, Fellow). <https://www.linuxfoundation.org/about/leadership>
22. Apache Software Foundation, page des sponsors, octobre 2026. <https://www.apache.org/foundation/thanks.html>
23. OpenSSF, lancement d'Alpha-Omega, 1er février 2022. <https://openssf.org/press-release/2022/02/01/openssf-announces-the-alpha-omega-project-to-improve-software-supply-chain-security-for-10000-oss-projects/> ; Alpha-Omega, rapport annuel 2025 (donateurs AWS, Citi, Google, Microsoft ; aucune subvention à la PHP Foundation).
https://alpha-omega.dev/wp-content/uploads/sites/22/2026/07/Alpha-Omega-Annual-Report-2025_073126a.pdf ; Linux Foundation, 17 mars 2026 (12,5 M\$ d'Anthropic, AWS, GitHub, Google, Google DeepMind, Microsoft, OpenAI). <https://www.linuxfoundation.org/press/linux-foundation-announces-12.5-million-in-grant-funding-from-leading-organizations-to-advance-open-source-security>
24. GitHub, « We need a European Sovereign Tech Fund », juillet 2025 (étude OpenForum Europe / Fraunhofer ISI / Institut universitaire européen, 350 M€ minimum).
<https://github.blog/open-source/maintainers/we-need-a-european-sovereign-tech-fund/>
25. Open Collective, PHP Foundation, relevé du 25 octobre 2026 (budget annuel estimé 974 118 \$; cumulés par financeur).
<https://opencollective.com/phpfoundation> ; The PHP Foundation, rapport de transparence 2025, 27 mai 2026 (dons 730 534 \$, dépenses 784 376 \$). <https://thephp.foundation/blog/2026/05/27/impact-and-transparency-report-2025/> ; Sovereign Tech Agency, financement de PHP. <https://www.sovereign.tech/tech/php-2025>
26. Linux Foundation, lancement de Valkey, 28 mars 2024 (AWS, Google Cloud, Oracle, Ericsson, Snap).
<https://www.linuxfoundation.org/press/linux-foundation-launches-open-source-valkey-community> ; Linux Foundation, annonce d'OpenTofu, 20 septembre 2023 (dix-huit développeurs à temps plein sur cinq ans).
<https://www.linuxfoundation.org/press/announcing-opentofu> ; HashiCorp, 10 août 2023.
<https://www.hashicorp.com/blog/hashicorp-adopts-business-source-license>
27. xkcd 2347, « Dependency », 17 août 2020. <https://xkcd.com/2347/>
28. Linux Foundation / Harvard LISH, « Census II of Free and Open Source Software », mars 2022.
https://www.linuxfoundation.org/hubfs/Research%20Reports/lfr_harvard_censusII_mar2022_042824b.pdf
29. G. Avelino, L. Passos, A. Hora, M. T. Valente, « A Novel Approach for Estimating Truck Factors », ICPC 2016 (65 % de 133 projets populaires). <https://arxiv.org/abs/1604.06766>
30. Tidelift, « State of the Open Source Maintainer », 17 septembre 2024. <https://www.silicon.co.uk/press-release/tidelift-study-reveals-paid-open-source-maintainers-do-significantly-more-critical-security-and-maintenance-work-than-unpaid-maintainers> ; part des moins de 26 ans (25 % en 2021, 10 % en 2024) : The Register, 18 septembre 2024, citant le même rapport.
31. Netcraft, 8 avril 2014. <https://netcraft.com/blog/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug/> ; S. Marquess, « Of Money, Responsibility, and Pride », 12 avril 2014.
<http://veridicalsystems.com/blog/of-money-responsibility-and-pride/>
32. Google, 17 décembre 2021 (35 863 artefacts touchés).
<https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html> ; LWN, 15 décembre 2021 (V. Yazıcı).
<https://lwn.net/Articles/878802/> ; Cyber Safety Review Board, juillet 2022 (33 000 heures pour un ministère fédéral), via SiliconANGLE, 14 juillet 2022.
<https://siliconangle.com/2022/07/14/dhs-review-board-declares-log4j-endemic-vulnerability/>
33. L. Collin, liste xz-devel, 8 juin 2022. <https://www.mail-archive.com/xz-devel@tukaani.org/msg00567.html> ; R. Cox, chronologie xz, 1er avril 2024. <https://research.swtch.com/xz-timeline> ; A. Freund, oss-security, 29 mars 2024.
<https://www.openwall.com/lists/oss-security/2024/03/29/4> ; CISA, « Lessons from XZ Utils », avril 2024.
<https://cisa.gov/news-events/news/lessons-xz-utils-achieving-more-sustainable-open-source-ecosystem>
34. D. Pushkarev, « So, what's next? », 14 février 2023.
<https://github.com/zloirock/core-js/blob/master/docs/2023-02-14-so-whats-next.md>
35. curl, « Users » (plus de vingt milliards d'installations). <https://everything.curl.dev/project/users> ; D. Stenberg, « The 2026 curl team », 12 octobre 2026. <https://daniel.haxx.se/blog/2026/10/12/the-2026-curl-team/> ; D. Stenberg, 20 octobre 2026.
<https://daniel.haxx.se/blog/2026/10/20/do-minor-curl-vulnerabilities-in-the-open/>
36. LWN, statistiques du noyau 6.19 (note 20) ; Linux Foundation, « Leadership » (note 21).
37. Documentation du noyau Linux, « conclave.rst », janvier 2026.
<https://www.kernel.org/doc/html/latest/process/conclave.html> ; M. Carvalho Chehab, LKML, 24 janvier 2026.
<https://lkml.iu.edu/2601.3/00054.html> ; The Register, 27 janvier 2026.
https://www.theregister.com/2026/01/27/linux_continuity_plan/

38. SQLite, « Copyright » (Hwaci emploie tous les développeurs). <https://www.sqlite.org/copyright.html> ; « SQLite Consortium » (150 000 \$/an par membre). <https://www.sqlite.org/consortium.html>
39. OpenSSL Corporation, rapport annuel 2025, 10 février 2026 (21 salariés, Brno, plus de 70 % du budget de la Fondation). <https://openssl-corporation.org/about/Annual-Report-2025.pdf>
40. Licence MIT. <https://opensource.org/license/mit> ; GPLv3, \$15. <https://opensource.org/license/gpl-3-0> ; Apache 2.0, \$7. <https://www.apache.org/licenses/LICENSE-2.0>
41. T. Depierre, « I am not a supplier », 31 décembre 2022. <https://www.softwaremaxims.com/blog/not-a-supplier>
42. Règlement (UE) 2024/2847 (Cyber Resilience Act), considérants 15, 18 et 19, art. 3(14), 13(5), 13(6), 24, 64(10). <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> ; Commission européenne, communication C(2026) 5252, 27 juillet 2026 (guidance, exemple 34). <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation>
43. Directive (UE) 2022/2555 (NIS2), art. 21(2)(d). <https://data.consilium.europa.eu/doc/document/PE-32-2022-INIT/en/pdf> ; règlement délégué (UE) 2024/1774 (DORA), art. 10(2)(d)(i). <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32024R1774>
44. Reuters, 23 octobre 2026 (E. Barron : « one full-time staff member (that's me) and 14 mostly part-time contractors »). Voir note 7.
45. The PHP Foundation, 21 octobre 2026 (note 4) ; The PHP Foundation, « PHP Core Security Audit Results », 10 avril 2025 (« Due to budget constraints, the recent security audit focused on the most critical components »). <https://thephp.foundation/blog/2025/04/10/php-core-security-audit-results/>
46. Calif, « php2shell: A tale of two PHP remote vulnerabilities ». <https://calif.io/php2shell/> ; Wiz Research, « PHP2Shell ». <https://www.wiz.io/blog/php2shell-php-rce> ; The Hacker News, 21 octobre 2026. <https://thehackernews.com/2026/10/php-issues-emergency-patches-for-two.html> ; Latent Space (programme « Patch the Planet »). <https://www.latent.space/p/ainews-openais-patch-the-planet-program>
47. D. Stenberg, « Death by a thousand slops », 14 juillet 2025. <https://daniel.haxx.se/blog/2025/07/14/death-by-a-thousand-slops/> ; fermeture du programme de primes : The New Stack, 22 janvier 2026.
48. The Guardian, 23 octobre 2026, via JournalArta (note 5).
49. Anthropic, « Project Glasswing: initial update », mai 2026 (530 vulnérabilités divulguées, 75 corrigées au 22 mai). <https://www.anthropic.com/news/glasswing-initial-update> ; Cloud Security Alliance, décompte du 7 octobre 2026 (97 corrections sur 1 596), source secondaire ; M. Brundage, « Operation Patchlight », Institute for Progress, 11 août 2025 (1,4 Md\$ « Fix », 1 Md\$ « Empower »). <https://ifp.org/operation-patchlight/>
50. Bloomsbury Intelligence and Security Institute, « PHP2Shell: Critical PHP Vulnerabilities and the Fragility of the Web's Foundations », 23 octobre 2026. <https://bisi.org.uk/reports/php2shell-critical-php-vulnerabilities-and-the-fragility-of-the-webs-foundations>
51. Sovereign Tech Agency, « Tech » (41,1 M€, 118 technologies). <https://www.sovereign.tech/tech> ; communiqué de novembre 2024 (500 candidatures pour 114 M€). <https://sovereign.tech/press/release-sovereign-tech-agency> ; « Celebrating five years », 13 octobre 2026. <https://www.sovereign.tech/news/celebrating-five-years> ; revote annuel : OSOR, 19 juin 2025. <https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/funding-open-source-case-study-sovereign-tech-fund>
52. L. Domenech Burin, étude causale sur les financements STA (contrôle synthétique, 12 dépôts financés, 62 témoins), arXiv 2607.05413, juin 2026. <https://arxiv.org/abs/2607.05413> ; Apache Software Foundation, minutes du conseil, Logging Services, 19 février 2025 (« Log4j activity has declined following the conclusion of funding from the Sovereign Tech Agency »). https://whimsy-vm9.apache.org/board/minutes/Logging_Services.html
53. Commission européenne, « Strategy for EU Open Digital Ecosystems », 3 juin 2026 (« Open Source Maintenance Instrument », objectif d'environ 2 Md€ sur sept ans). https://commission.europa.eu/news-and-media/news/commission-boosts-open-and-interoperable-digital-ecosystems-public-administrations-2026-06-03_es ; FSFE, 3 juin 2026. <https://fsfe.org/news/2026/news-20260603-01.html>
54. Décision d'exécution (UE) 2025/2170 du 29 octobre 2025 (EDIC Digital Commons). https://eur-lex.europa.eu/eli/dec_impl/2025/2170/oj/eng/pdf ; NGI Commons, 1er avril 2026 (directeur, pilote EU-STF). <https://commons.ngi.eu/2026/04/01/digital-commons-edic-takes-shape-with-more-countries-director-and-first-projects/>
55. Assemblée nationale, commission d'enquête sur les dépendances et vulnérabilités dans le secteur du numérique, rapport n° 3054, 8 juillet 2026 (recommandation 15, propositions 2, 3 et 10). https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/117b3054-t1_rapport-enquete.pdf ; Cour des comptes, rapport sur les outils bureautiques et collaboratifs de l'État, 22 octobre 2026, via Acteurs publics. <https://acteurspublics.fr/articles/la-cour-invite-encore-la-dsi-de-letat-a-collaborer-davantage-avec-les-ministeres-pour-sa-suite-numerique> ; Conseil national de l'IA et du numérique, rapport « Souveraineté numérique », mai 2026. https://www.conseil-ia-numerique.fr/files/uploads/2026/Souverainet%C3%A9%20numerique_De%20l'urgence%20d'organiser%20la%20cooperation%20public-p

56. code.gouv.fr (Pôle Open Source et Communs Numériques). <https://code.gouv.fr/fr/> ; Next, 7 mai 2026 (auditions April, Framasoft, Mastodon : « ce ne sont pas des dons »).
<https://next.ink/237134/souverainete-les-acteurs-du-libre-plaident-pour-une-meilleure-organisation-des-financements>
57. Sovereign Tech Agency, « PHP2Shell shows why critical open source needs investment at scale », 23 octobre 2026.
<https://www.sovereign.tech/news/php2shell-shows-why-critical-open-source-needs-investment-at-scale>
58. Python Software Foundation, « Developers in Residence ». <https://www.python.org/psf/developersinresidence/> ; avis de sécurité CPython (18 en 2024, 41 en 2025, 175 au premier semestre 2026) : relevé publié par H. van Kemenade, 13 juillet 2026, source secondaire ; Sovereign Tech Agency, Fellowship 2026 (contrats de deux ans).
<https://www.sovereign.tech/news/2026-fellowship-applications-open>
59. Debian, suivi de sécurité CVE-2026-109618 (DSA-6574-1). <https://security-tracker.debian.org/tracker/CVE-2026-109618> ; Freexian, « PHP2Shell updates », 22 octobre 2026. <https://www.freexian.com/blog/php2shell-updates/> ; délais par distribution : Digital Applied, relevé du 21-22 octobre 2026, source secondaire.
<https://www.digitalapplied.com/blog/php2shell-fixes-by-distro-control-panel-php-version> ; dépôt Remi, billet du 22 octobre 2026. <https://blog.remirepo.net/>
60. OpenSSL Corporation, rapport annuel 2025 (note 39).
61. Amazon Threat Intelligence, « PHP2Shell exploitation prior to public disclosure in MadPot », octobre 2026. <https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot/>
62. Estonie : CCDCOE, « Cyber Defence Unit of the Estonian Defence League », 2013.
https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf ; Royaume-Uni : Joint Cyber Reserve annoncée le 29 septembre 2013 (source secondaire) ; France : État-major des armées, guide explicatif de la réserve de cyberdéfense, novembre 2016.
https://archives.defense.gouv.fr/content/download/491674/7859279/file/20161115_EMACYBER_Guide_explicatif.pdf ; ministère des Armées, COMCYBER, 21 novembre 2025 (près de 400 réservistes opérationnels, cible 500 en 2030). <https://www.defense.gouv.fr/comcyber/actualites/european-cyber-week-reservistes-operationnels-cyberdefense-au-coeur-du-combat-cyber> ; États-Unis : 10 U.S.C. chapitre 747 (pilote de réserve civile de cybersécurité, loi du 22 décembre 2023).
<https://www.law.cornell.edu/uscode/text/10/subtitle-B/part-II/chapter-747> ; Allemagne : Bundestag, Drucksache 19/23415 (Cyber-Reserve). <https://dserver.bundestag.de/btd/19/234/1923415.pdf>
63. Ministère des Armées, instruction générale sur la politique logicielle, 8 février 2019.
<https://archives.defense.gouv.fr/content/download/576629/9865076/file/politique%20logiciel.pdf>
64. Mécénat de compétences (art. 238 bis du CGI) : service-public.fr.
<https://entreprendre.service-public.gouv.fr/vosdroits/F22263> ; mise à disposition d'agents publics (loi 3DS, art. 209, décret du 27 décembre 2022, expérimentation jusqu'au 27 décembre 2027) : fonction-publique.gouv.fr. <https://www.fonction-publique.gouv.fr/etre-agent-public/mon-parcours-professionnel/le-mecanat-de-competences-dans-la-fonction-publique>
65. The Document Foundation, « Why and how the Austrian military moved to LibreOffice », 7 et 14 août 2026.
<https://blog.documentfoundation.org/blog/2026/08/14/why-and-how-the-austrian-military-moved-to-libreoffice-part-2/> ; DINUM, FOSDEM 2026, « Building digital workplace solutions on top of foundational libraries », 31 janvier 2026. https://archive.fosdem.org/2026/schedule/event/DC97FQ-building_digital_workplace_solutions_on_top_of_foundational_libraries_blocknote/
66. CHAOSS, « Bus Factor » (renommée « Contributor Absence Factor »). <https://chaoss.community/kb/metric-bus-factor/>
67. CybelAngel, « Critical PHP RCE vulnerabilities », octobre 2026 (2,24 millions d'hôtes, 59 % sur branches sans correctif, France 25 439 hôtes). <https://cybelangel.com/blog/critical-php-rce-vulnerabilities-cve-2026-109618-and-cve-2026-109619/> ; NCSC-NL, 23 octobre 2026 (« Misbruik is ingewikkeld »).
<https://www.ncsc.nl/alerts/update-php-kwetsbaarheden-nog-steeds-reden-om-direct-te-patchen> ; Rijksoverheid (note 6).
68. J. Care, KuppingerCole, « PHP2Shell Wasn't a Supply Chain Attack. That's the Problem », 23 octobre 2026.
<https://www.kuppingercole.com/blog/care/php2shell-wasnt-a-supply-chain-attack-thats-the-problem>