MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE
*Liberté
Égalité
Fraternité*

**Direction générale
des Entreprises**

Paris, le 27/07/2026

JOURNEE CONNECT THE CODES - SYNTHESE

1 Synthèse

2 Présentation et objectifs de Connect the codes

. La Stratégie open source de l'Union souhaite faire de l'open source un levier de compétitivité et d'autonomie stratégique

En juin dernier, la Commission Européenne a dévoilé le European Technological Sovereignty Package, une stratégie globale visant à atteindre la souveraineté technologique, portée par des initiatives ciblant chaque étape de la chaîne de valeur, des puces électroniques aux infrastructures, en passant par les logiciels, le cloud et l'intelligence artificielle. Parmi ces initiatives, à savoir le *Chips Act 2.0*, le *Cloud & AI Development Act*, et la feuille de route stratégique pour la numérisation et l'IA dans le secteur de l'énergie, la Stratégie open source de l'Union vise à mobiliser l'open source comme une levier d'autonomie stratégique.

En effet, la Commission identifie dans l'open source un vecteur d'innovation et de compétitivité permettant de faire émerger des services numériques conçus et développés par des acteurs européens, alternatifs aux produits propriétaires bien souvent extra-européens. Les enjeux sont de taille, des projets comme PostgreSQL (base de données) ou LibreOffice (édition de documents) devenant aujourd'hui des produits capables de prendre en charge des cas d'usages complexes à grande échelle, avec des applications transverses à tous les domaines de l'industrie et des services. La stratégie de la Commission repose sur une articulation entre soutien au développement et à la maintenance de projets open source, et soutien à son adoption par les organisations publiques et privées, les deux pôles étant les conditions nécessaires à l'émergence de véritables produits capables de donner à leurs utilisateurs des garanties élevées de fiabilité, de maintenance, et de sécurité.

. La France partage les ambitions de la Commission sur l'open source

La France s'inscrit dans la vision développée par la Commission Européenne sur l'open source. Dans le contexte où les marchés numériques sont polarisés vers des acteurs extra-européens, posant des risques et des contraintes pour la maîtrise des données des organisations, l'open source, mode de développement mutualisé, est un moyen par lequel des produits compétitifs peuvent émerger. L'Europe dispose des compétences et des ressources pour contribuer et mener à bien des projets open source, mais un accompagnement structuré des acteurs est nécessaire afin de déboucher sur des résultats concrets : les utilisateurs, et en particuliers les grandes organisations, si elles souhaitent déjà se fournir en produits open source pour des raisons de gestion des risques, ont besoin de garanties très fortes sur la qualité du service (disponibilité, sécurité, support, etc.), ce qui demande un effort très important de développement.

Des initiatives publiques et privées mettent déjà en œuvre des moyens pour répondre à ces enjeux, qu'il s'agisse de l'EDIC Communs numériques, qui rassemble à l'heure actuelle l'Allemagne, l'Italie, la France, le Luxembourg et les Pays-Bas pour soutenir conjointement l'open source en Europe ; de la Sovereign Tech Agency en Allemagne, qui soutient des projets open source considérés comme stratégiques dans la chaîne de valeur numérique allemande ; d'EuroCommons, initiative à laquelle contribue notamment la Caisse des dépôts et consignations en France, qui a l'ambition de créer des groupes d'utilisateurs et de fournisseurs pour développer des produits open source à destination des premiers ; ou encore d'Eurostack, qui cherche à promouvoir l'adoption des offres numériques européennes, avec une orientation forte sur l'open source.

. Les objectifs de « Connect the codes » pour contribuer à la Stratégie open source de l'Union

Dans ce cadre, la journée « Connect the codes » souhaite rassembler les parties prenantes amenées à mettre en œuvre la stratégie open source, que ce soient des acteurs publics ou privés, dans le but de partager les pistes de politiques publiques devant être mises en œuvre pour atteindre les ambitions de la Stratégie open source de l'Union.

« Connect the codes » se donne les objectifs suivants :

- discuter des enjeux posés par l'open source en tant que levier de compétitivité et d'autonomie stratégique
- présenter les principales initiatives publiques et privées qui tentent de répondre à ces enjeux (Stratégie open source de la Commission Européenne, EDIC Communs numériques, Sovereign Tech Agency, EuroCommons, Eurostack)

- explorer et présenter aux acteurs publics des pistes pour orienter les politiques de soutien à l'open source, afin de contribuer aux mieux aux ambitions de la Stratégie open source de l'Union.
- Mobiliser très largement l'écosystème numérique français et européen autour de l'open source

. Participants

La journée « Connect the codes » a rassemblé environ 200 participants représentant :

- les autorités publiques européennes
- les initiatives publiques ou privées portant sur l'open source
- les acteurs des filières numériques (cloud, cybersécurité, telco, IA…)
- les acteurs de l'open source (développeurs, fondations...)
- les utilisateurs publics et privés de service numériques open source

3 Synthèse des échanges et des ateliers

La journée état construite autour d'une matinée introductive abordant les principaux enjeux de l'open source, et les stratégies et programmes qui y apportent des réponses à l'échelle européenne. L'après-midi, les participants se sont répartis en 8 ateliers thématiques : coordination européenne, cloud, telco, cyber, IA, adoption de l'open source dans les grandes organisations, fondation open source du CSF LSNC, et séquence d'échange autour du Pacte Numérique signé entre la DINUM et les acteurs technologiques français.

. Séquence introductive

Dans l'ensemble, les prises de parole de la séquence introductive ont insisté sur le rôle de l'open source pour maîtriser ses dépendances, et donc améliorer sa souveraineté, sur celui de la commande publique comme moteur d'une politique efficace, et sur la question du financement des projets open-source, dont le manque de pérennité fragilise les chaînes de valeur.

Mme Anne Le Hénanff, Ministre chargée de l'IA et du numérique, a insisté sur le fait que l'open source était un outil pour pouvoir connaître et gérer ses dépendances numériques, car d'une part il améliore la confiance et la transparence des produits, et d'autre part il permet de se prémunir contre les risques de « kill switch », de réduire les coûts des systèmes d'information, d'allouer des ressources à l'innovation, et donne la possibilité aux utilisateurs d'adapter un produit selon leurs besoins. Elle a conclu par un appel à mener des actions à l'échelle européenne : une cartographie des projets open source stratégiques pour l'Europe, le renforcement de la présence européenne dans leur gouvernance, et l'augmentation des contributions techniques par des acteurs européens.

Mr Markus Richter, Secrétaire d'Etat au Ministère fédéral pour la transformation digitale et la modernisation du gouvernement (BMDS), a soutenu l'open source comme levier de confiance et d'innovation. Il a mis en avant les forces de l'Europe, mais aussi la fragilité des acteurs européens de l'open source. En guise d'exemple, il a évoqué le projet SPARK, projet allemand open source visant à accélérer les procédures administratives de planification et d'autorisation grâce à l'IA, et qui a permis des gains de temps de 85% par rapport à une procédure classique.

Mr Jérémie Vallet, directeur-adjoint de la DINUM, a insisté sur la nécessité d'avoir des briques capables de passer à l'échelle, et d'avoir une approche active sur les projets opens source, qu'il faut maîtriser techniquement, sécuriser, et auxquels il faut contribuer. Il a mentionné la fragilité des acteurs de l'open source en Europe, et plaider pour une approche interministérielle, afin de faire jouer les effets d'échelle. Enfin, il a clarifié le fait que l'État ne devait pas tout construire tout seul, mais collaborer avec les entreprises et startups pour les communs digitaux.

Mme Julia Mouzon, secrétaire générale du Comité stratégique de filière Logiciels et solutions numériques de confiance (CSF LSNC), et **Mr Nicolas Duffour, président du groupe « offres » du CSF LSNC**, ont mis en avant le rôle de l'open source comme outil de développement technologique, de créations de standards, et de résilience des chaînes de valeur, nécessaires pour favoriser le développement de la filière numérique française. Ils ont appelé à une politique ambitieuse basée sur des démonstrateurs industriels pour amorcer le passage à l'échelle, car seule la demande permettra de pérenniser la croissance de la filière.

Panel 1 : L'agenda stratégique européen sur l'open source

Mr Jean-Luc Dorel, directeur du programme open source à la Commission européenne, a mis en avant la récente publication de la Stratégie open source de l'Union, qui vise à soutenir offre et demande pour développer l'open source. Il a plaidé pour que l'on assume une interdépendance européenne (à l'exemple d'Airbus), et a insisté sur le rôle de la formation des futurs intégrateurs et techniciens pour faire adopter l'open source dans les structures. Il a ensuite mis en avant le programme Open Internet Stack, qui mobilise 40M€ pour soutenir 6 projets dont un système d'exploitation, des projets de sécurisation, une stack Python/IA.

Mr Laurent Rojey, directeur de l'EDIC Communs numériques, a présenté le rôle de l'EDIC pour fédérer des ressources et des projets éparpillés, afin de proposer des alternatives aux suites collaboratives propriétaires (O365), d'identifier les dépendances critiques et de s'assurer que les projets sont bien développés et maintenus dans la durée.

Mr Paul Sharrat, directeur de la recherche à la Sovereign Tech Agency, a mis en avant le fait que la plupart des projets open source sont sous-financés et manquent de contributeurs. Cela pose des risques importants pour les services numériques, notamment pour des projets qui sont massivement utilisés (à l'exemple de l'incident Log4Shell en 2021). Divers programmes ont été lancés par la Sovereign Tech Agency pour pallier à ce problème, dont un de 60M€ pour soutenir 110 projets, qui a abouti à la correction de 150

vulnérabilités. Si le nombre de projets est réduit, l'impact de ce programme est massif puisqu'ils sont très largement utilisés. Il a ensuite mis en avant la publication d'un article à venir le 12 novembre prochain sur l'investissement franco-allemand dans les startups faisant de l'open source.

Mr Patrick Laurens-Frings, représentant du programme EuroCommons, a présenté l'importance de l'indice de résilience numérique pour permettre aux organisations de mesurer leurs dépendances logicielles, et la stratégie du programme EuroCommons, lancé ce juillet, qui a pour but de combler l'écart entre les produits basés sur l'open source et les logiciels propriétaires en créant des coalitions d'acheteurs et de fournisseurs pour développer des produits.

Mme Cristina Caffarra, co-fondatrice de la fondation EuroStack, a insisté sur le problème de la mobilisation de la demande. Elle rappelle que l'open source, s'il contribue à la résilience des entreprises, ne sera adopté que si les utilisateurs y voient un investissement rentable, car eux-mêmes sont soumis à la concurrence sur leur marché. Le frein majeur reste le coût de migration, les marges étant assez faibles au sein des Directions des systèmes d'information. L'enjeu est donc de réduire le coût de migration en ayant des standards communs avec les solutions déjà déployées.

Panel 2 : Défis et opportunités pour la compétitivité et l'autonomie stratégique

Mme Sachiko Muto, présidente d'OpenForum Europe, a insisté sur l'utilisation de l'open source par certaines entreprises pour dominer un marché en réduisant leurs coûts, ce qui lève des questions de licences et de concurrence.

Mr Astor Nummelin-Carlberg, directeur de la souveraineté open source à SUSE, a souligné le fait que la stratégie open source de l'Union, si on peut considérer qu'elle est tardive à certains égards, reste la seconde publiée dans le monde, après la Chine il y a 7 ans. Il a aussi mentionné le fait que, d'après un rapport McKinsey, les coûts IT grignotent les profits, ce qui pousse à l'utilisation de projets OS.

Mr Homéric De Sarthe, vice-président de la commission IA de Numeum, a indiqué le retard d'environ 6 mois des modèles open source sur les solutions propriétaires. Il a insisté sur le fort besoin d'intégrateurs de solutions open source pour qu'elles deviennent viables, et donc de formations adéquates.

Mme Anna Zagorski, chercheuse à l'Agence allemande de l'environnement, a présenté le label Blue Angel, qui certifie l'efficacité énergétique, le fonctionnement sur un système vieux de 5 ans, ainsi que l'autonomie de l'utilisateur. Nextcloud, OpenCloud, KDE Ocular, ont par exemple déjà été labellisés.

Mme Amandine Le Pape, fondatrice de la fondation TheMatrix.org, et directrice d'Element, a insisté sur la nécessité pour les utilisateurs de contribuer durablement (financièrement, ou par des contributions), aux projets open source qu'ils utilisent directement ou indirectement, sous peine de fragiliser les projets par l'accumulation des charges importantes sur des équipes trop petites pour y faire face. L'open source n'est pas une ressource gratuite : il faut la financer. Elle a également pointé du doigt l'importance de conserver des structures de gouvernance ouvertes pour la pérennité des projets.

Mme Martine Gouriet, directrice de la transformation, des usages et du digital chez EDF, a souligné l'usage massif d'open source chez EDF, avec la maintenance et la contribution associée. L'open source réduit les coûts fixes d'infrastructure IT, donc améliore les marges et la compétitivité de l'entreprise. Elle a rappelé qu'aucun produit n'est totalement souverain, et qu'il est nécessaire de connaître ses dépendances et leur coût.

. Atelier 1 : Coordonner les efforts européens sur l'open source

Cet atelier était consacré à une discussion portant sur les enjeux de coordination des efforts européens sur l'open source de la part des acteurs institutionnels et privés, puis à une série de présentations sur des enjeux d'innovation et de politiques publiques.

Participants :

La première discussion a porté sur l'importance de mesurer en Europe l'état de l'open source, afin d'identifier les potentielles vulnérabilités et opportunités, et d'ainsi orienter les politiques de soutien européennes. Les principales difficultés sont le nombre de projets open source (3 millions de projets actifs) et l'obtention de certaines données, dont les données d'usage, pourtant essentielles. Elle a notamment permis d'identifier :

- des critères pour retenir un projet open source comme « fondationnel » : diffusion dans les chaînes de valeur numérique et industrielle, utilisation par des secteurs stratégiques
- des métriques à appliquer aux projets à analyser : analyses de sécurité, publication de CVE (révélatrices de potentielles failles), données d'utilisation des projets, *gap analysis* avec les solutions dominantes, identification récursive des dépendances des projets pour pouvoir agir au niveau de la librairie
- de la méthodologie à déployer : recours à des analyses de Software Heritage pour les données d'archives sur les projets open source, s'appuyer sur le CRA pour estimer les données d'usage des projets, simplifier la démarche pour les projets open source (guichets uniques…), conserver des capacités d'action sur des petits volumes d'aide suffisants pour régler des problèmes ponctuels dans de nombreux cas, réserver des lots de soutien à des tâches de R&D indispensables pour étudier la sécurité des projets

La discussion a également permis d'insister sur la nécessaire échelle européenne de telles actions, et sur l'importance de favoriser la diffusion des outils open source en en réduisant les coûts, par exemple via des outils d'aide à la migration.

Présentations :

L'atelier a permis ensuite à plusieurs participants de présenter des projets ou des pistes de réflexion sur l'open source :

- **l'ANSSI** a présenté les audits de sécurité conduits sur des projets open source. Elle a mis en avant le succès de cette démarche, qui a ciblé des projets très largement diffusés, et a appelé à un passage à l'échelle européenne pour pouvoir augmenter les capacités d'analyse, qui sont encore faibles (5 à 10 projets par an)
- **SUSE** a présenté ses idées pour soutenir la diffusion de l'open source, et en particulier le rôle de l'État sur la demande (*via* l'« open source first »), sur la mesure des vulnérabilités de la chaîne de valeur, et sur le soutien à l'adoption
- **Dalibo** a présenté le projet TheCrypticElephant, soutenu par la fondation NLNet, projet d'encryption du système de gestion de bases de données PostgreSQL, condition nécessaire a la compatibilité DORA du projet, et à son adoption à large échelle
- **CleverCloud** a présenté son projet Biscuit, brique de gestion des identités et des accès open source, qui se veut comme une alternative à EntraID de Microsoft, et qui est déjà utilisée à grande échelle par Outscale
- **NeoNephos** a présenté sa fondation, qui a pour objectif de rassembler des projets open source portant sur la pile logicielle data et cloud pour des capacités de calcul décentralisées fédérées

. Atelier 2 : L'open source pour les services cloud

Cet atelier a abordé deux sujet : l'identification des composants open source critiques utilisés par les fournisseurs de cloud européens, et leurs avantages et inconvénients principaux ; et la présentation des initiatives open source portées par les fournisseurs de cloud et discuter des enjeux associés : passage à l'échelle, viabilité, coopération sur ces solutions.

L'atelier a permis d'aboutir au conclusions suivantes :

- le socle stratégique est sous contrôle américain : les fournisseurs européens s'appuient sur une pile open source gouvernée à plus de 80% par des fondations américaines (CNCF, Linux Foundation en tête), avec des feuilles de route alignées sur les intérêts de leurs contributeurs *hyperscalers* et une adhérence de segments entiers à des écosystèmes comme Red Hat et IBM ;
- des difficultés structurelles sont partagées : intégration complexe de briques hétérogènes développées en interne par chaque fournisseur, gestion du cycle de vie, de l'obsolescence et des vulnérabilités rendue coûteuse, faible culture de contribution open source, et risque de bascule de licence ou de sortie de l'open source (précédent Terraform) ;
- une dynamique européenne réelle mais fragmentée : de nombreuses briques développées en interne ont un fort potentiel (OS, orchestration, IAM, gateway, GitOps…), mais il existe peu de synergies, et pas de passage à l'échelle, notamment à cause de la difficulté à trouver des fondations pour soutenir tôt les projets, et de mettre en place une gouvernance adaptée ;

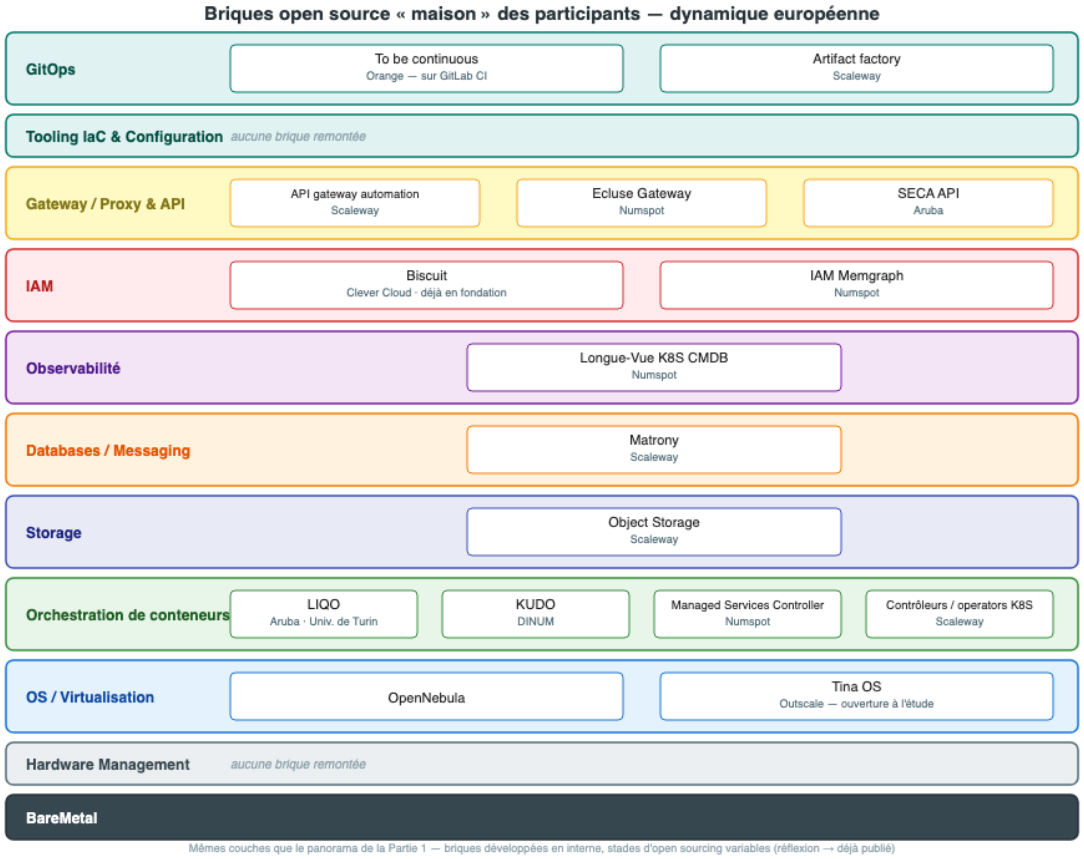
Ainsi, les problèmes soulevés conduisent à réfléchir à des pistes possibles de solutions : améliorer l'approche collective du développement des briques open source entre fournisseurs, en prenant appui sur les fondations existantes, améliorer la contribution des fournisseurs européens aux briques critiques, par exemple via les programmes de financement existants, diffuser la culture open source dans les entreprises

Les participants ont développé le tableau suivant de recensement des projets open source critiques :

Couche	Solution	Définition	Gouvernance / fondation	Nationalité
Hardware Management	OpenBMC	Firmware open source de gestion des serveurs (BMC, IPMI/Redfish)	Linux Foundation (LF Projects)	États-Unis
OS / Virtualisation	Linux OS	Socle système universel (noyau et distributions Linux)	Linux Foundation	États-Unis
	KVM	Hyperviseur intégré au noyau Linux	Projet noyau Linux (Linux Foundation)	États-Unis
	QEMU	Émulateur et virtualiseur de machines (souvent associé à KVM)	Projet communautaire indépendant (qemu.org)	International
	Talos OS	Linux minimal, immutable et API-driven dédié à Kubernetes	Sidero Labs (société)	États-Unis
	OpenStack	Plateforme IaaS complète (compute, réseau, stockage)	Open Infrastructure Foundation (OIF)	États-Unis
	Vates OS (XCP-ng)	Hyperviseur Xen open source (fork de XenServer)	Vates SAS (société + communauté)	France
Orchestration de conteneurs	Kubernetes	Orchestrateur de conteneurs de référence	CNCF (Linux Foundation)	États-Unis
	Rancher	Gestion multi-clusters et distribution Kubernetes	SUSE (société)	Allemagne
	K3S	Kubernetes léger pour l'edge et les environnements contraints	CNCF (sandbox)	États-Unis
Contrôleurs d'infrastructure	Crossplane	Plan de contrôle d'infrastructure piloté par Kubernetes (IaC)	CNCF (incubation)	États-Unis

	KubeVirt	Exécution de machines virtuelles dans Kubernetes	CNCF (incubation)	États-Unis
	Cluster API (CAPI)	Provisionnement déclaratif de clusters Kubernetes	CNCF (SIG Cluster Lifecycle)	États-Unis
Databases / Messaging	PostgreSQL	SGBD relationnel-objet de référence	Communauté internationale (PGDG), sans fondation formelle	International
	MariaDB	SGBD relationnel, fork communautaire de MySQL	MariaDB Foundation	Finlande
	Kafka	Plateforme distribuée de streaming d'événements	Apache Software Foundation	États-Unis
Observabilité	OpenTelemetry	Standard unifié de télémétrie (traces, métriques, logs)	CNCF	États-Unis
	Prometheus	Collecte, requêtage et alerte de métriques (séries temporelles)	CNCF (graduated)	États-Unis
	Stack Grafana (Loki, Mimir, Tempo)	Logs, stockage métriques long terme et traces	Grafana Labs (société)	États-Unis / Suède
IAM	Keycloak	IAM / SSO (OIDC, SAML), historiquement Red Hat	CNCF (incubation)	États-Unis
Gateway / API	OpenAPI	Spécification de description d'APIs REST (spécification, pas un produit)	OpenAPI Initiative (Linux Foundation)	États-Unis
	KONG	Passerelle API et management (open core)	Kong Inc. (société)	États-Unis
	Gravitee	Passerelle API et management full-stack (open core)	Gravitee.io (société)	France
	WSO2	Suite API management / identity (open core)	WSO2 Inc. (société)	Sri Lanka / États-Unis
	Envoy	Proxy L7 / edge, socle des service meshes	CNCF (graduated)	États-Unis
Tooling IaC	Terraform	Provisionnement d'infrastructure en code (licence BUSL, non OSI)	HashiCorp / IBM (société)	États-Unis
	OpenTofu	Fork open source (MPL) de Terraform	Linux Foundation	États-Unis
	Ansible	Automatisation de configuration et gestion de parc	Red Hat / IBM (société)	États-Unis

Les participants ont ensuite mis en regard les produits open source critiques et ceux développés par des fournisseurs européens :

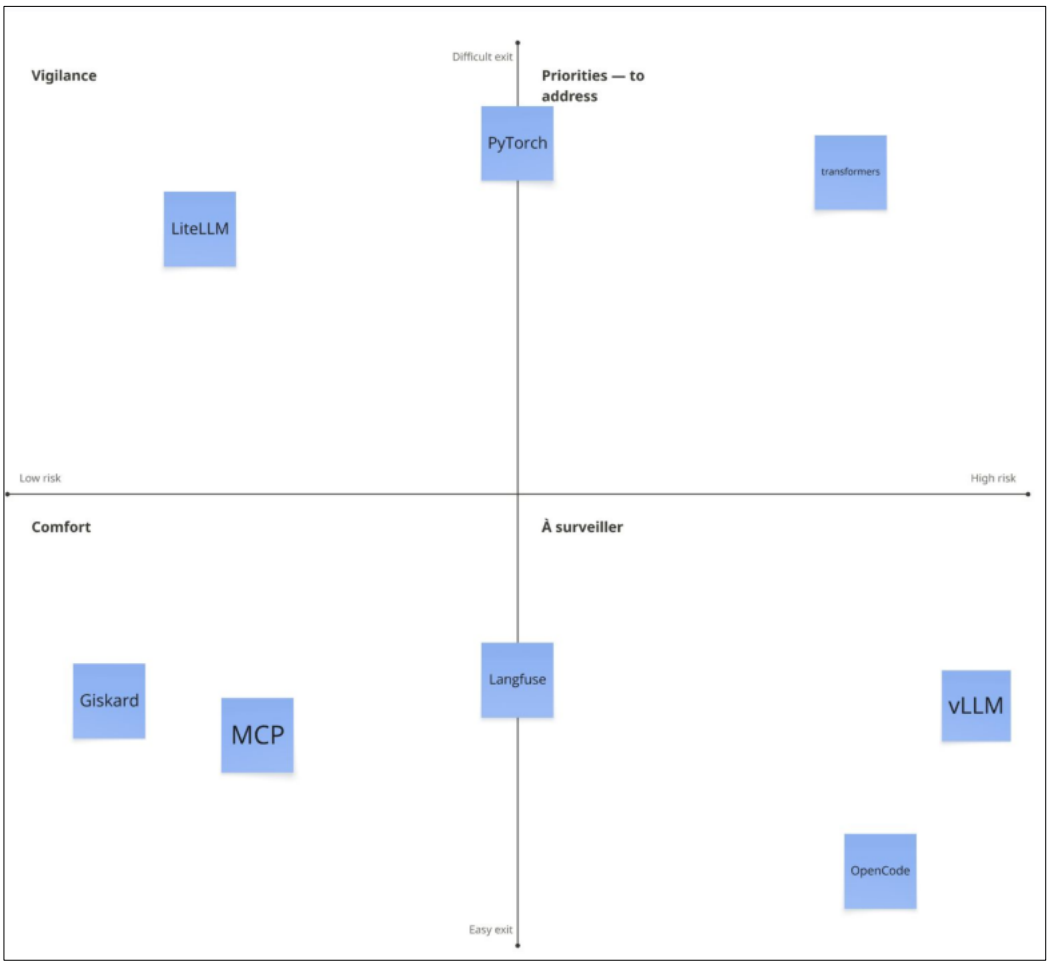


. Atelier 3 : L'open source pour les réseaux du futur

. Atelier 4 : Les composants open source pour l'IA agentique

Cet atelier s'est concentré sur la cartographie des composants open source nécessaires au déploiement de l'IA agentique, et sur l'évaluation de la dépendance européenne sur ces derniers.

Les projets open source identifiés sont **PyTorch, LiteLLM, Giskard, MCP, Langfuse, VLLM, OpenCode et les *transformers.*** Les participants les ont ensuite classés selon le verrouillage, défini par la disponibilité d'alternatives, et le risque associé, défini par l'importance du projet, la complexité technique, et le contrôle de la gouvernance. La matrice ci-dessous fait apparaître l'absence de dépendances majeures sur ces briques, hormis les *transformers*, tout en nuançant la situation en fonction des projets, et en proposant une grille de lecture pour prioriser l'action publique :



En conclusion, les participants appellent à poursuivre le travail initié sur l'identification des briques open source de la chaîne de valeur de l'IA agentique et des risques associés, en l'élargissant aux domaines de l'entraînement et du *serving*, et en mettant en place une surveillance des licences.

. Atelier 5 : Cybersécurité – Gestion des risques

Cet atelier s'est concentré sur l'analyse de la réactivité lors de la découverte de vulnérabilités sur un projet open source. Il a pris l'exemple de la réception par une équipe de sécurité d'une organisation d'une faille de sécurité exploitée activement, sur un composant open source présent dans plusieurs applications qu'elle utilise, et pour laquelle la CVE déposée est incomplète.

Les participants ont convergé vers l'identification des principales difficultés existant aujourd'hui pour résoudre le problème :

- le nombre important d'alertes reçues par les mainteneurs de projets open source, empêchant leur analyse
- l'envoi d'alertes de nature diverse à des organismes divers
- la difficulté d'identifier les composants concernés par une vulnérabilité au sein des produits industriels et numériques utilisés par l'entreprise
- les difficultés pour alerter le fabricant concernant la vulnérabilité, et le fait que ce dernier ne connaisse pas toujours le mainteneur responsable
- l'évolution des modèles économiques et opérationnels
- la distribution des impacts sur l'ensemble de la chaîne d'approvisionnement

Les participants on discuté de la manière d'atteindre les objectifs du CRA. Ils ont d'une part appuyé la nécessité de créer et maintenir un ensemble de « Bill of Material » (Software BoM, Crypto BoM, AI BoM, HW BoM), la difficulté étant la capacité à cartographier l'ensemble de ces éléments, et d'en tracer les changements, et d'autre part la capacité à tracer la provenance des composants Open Source (y compris la viabilité des dépôts, de la communauté et sa capacité au maintien en condition de sécurité).

A propos du nombre croissant de vulnérabilités et du temps de réaction imposé par le CRA (24h maximum pour les « vulnérabilités activement exploitées contenues dans le produit » - KEV), ainsi que le nombre d'éditeurs devant communiquer, la question est posée sur la capacité réelle de traitement de ces notifications. A titre d'exemple, si un composant open source très largement utilisé est qualifié de KEV, le CERT récipiendaire devra traiter un nombre égal au nombre de produits potentiellement affectés, et ce pour un composant similaire. La même question se pose pour le nombre de « découvreurs » créant potentiellement des CVE différentes pour une vulnérabilité similaire. Ils ont discuté du fait qu'en raison de la difficulté, pour les éditeurs, de traiter en moins de 24h les KEV, les faux positifs sont possibles et admissibles (dès qu'il est détecté que « tel produit » contient une KEV, l'éditeur notifie le CERT sans attendre la confirmation que cette KEV est réellement exploitable dans ledit produit).

Sur les **questions d'environnement économique des briques open source, et de leurs impacts sur la sécurité des produits**, les participants ont noté que, les communautés n'étant pas rémunérées, la pression pesant de plus en plus sur leur capacité de réaction aux vulnérabilités rend le modèle vulnérable. Il faut donc s'assurer que les contributeurs des communautés open source restent mobilisables, et motivés, dans un contexte où l'open source devient aussi de moins en moins attractif. Ils ont proposé de d'établir un modèle de rétribution équitable entre les éditeurs rémunérés s'appuyant sur des logiciels open source, et les communauté. Ils ont également évoqué la possibilité, dans le cadre précis du CRA, d'établir une matrice RACI impliquant tous les acteurs (Communauté open source, open source « Steward », éditeur, utilisateur), avec pour objectif de définir plus clairement les « droits et devoirs » de chaque acteur (le CRA établit déjà les règles pour les open source stewards en particulier). Enfin, ils ont discuté du changement possible du modèle économique actuel des communautés open source, qui détermine en cascade les stratégies des éditeurs.

Les participants ont ensuite appelé à poursuivre les échanges entre les éditeurs, la DGE et l'ANSSI pour continuer à approfondir les sujets.

. Atelier 6 : Adoption par l'industrie et les grands comptes

. Atelier 7 : Fondation OpenInterop

Cet atelier visait à lancer les travaux de la fondation OpenInterop, fondation open source crée par le CSF Logiciels et solutions numériques de confiance, avec l'objectif de créer des composants d'interopérabilité pour soutenir l'adoption de solutions numériques françaises.

Les discussions ont permis de définir :

- les critères nécessaires à un acheteur pour vérifier l'interopérabilité effective des composants ;
- les livrables que la fondation devrait fournir pour permettre l'interopérabilité des logiciels ;
- les briques open source existantes à réutiliser dans ce cadre ;
- les scénarios de référence à prendre en compte dans la spécification des besoins (type et volume de données, caractéristiques de la source et de la destination…), et les données à surveiller lors de l'exécution de ce scénario.

Les travaux engagés sur chaque axe permettront de soutenir la poursuite des travaux au sein de la fondation.

. Atelir 8 : Pacte Numérique et IA

Cet atelier visait à présenter le Pacte Numérique, le pacte « Numérique et IA » crée pour une durée initiale de trois ans, renouvelable, un cadre opérationnel piloté par la DINUM permettant une adaptation continue aux enjeux technologiques et industriels. Ce cadre vise à :

- Identifier les besoins prioritaires de l'État en matière de numérique et d'IA.
- Faire émerger des solutions françaises et européennes, en s'appuyant sur les compétences et les partenaires du Comité Stratégique de Filière Logiciels et Solutions Numériques de Confiance, d'Hexatrust, avec le soutien de Numeum et en associant les acteurs privés de l'Équipe de France du numérique.
- Contribuer à renforcer les capacités industrielles nécessaires à la souveraineté numérique, et créer une véritable Base Industrielle et Technologique du Numérique sur le modèle de la Base Industrielle et Technologique de Défense (BITD).

Les travaux s'articuleront autour de plusieurs axes prioritaires, incluant : la définition des besoins capacitaires de l'État ; l'identification des technologies clés et des standards ; la cartographie des compétences industrielles françaises ; la résilience et la sécurité des infrastructures critiques et l'acculturation des acteurs publics aux enjeux de défense numérique.

L'atelier a permis aux participants (la DINUM et les membres du CSF LSNC et de NUMEUM) d'initier des échanges visant à préciser le cadre et les modalités d'exécution du Pacte Numérique et IA.