HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Retour de l'audition d'Hexatrust dans le cadre de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de son effet d'entraînement.

1.De manière générale, considérez-vous que les entreprises françaises et européennes de cybersécurité bénéficient de bonnes conditions d'accès à la commande publique ?

La situation actuelle de la filière française de cybersécurité illustre un paradoxe saisissant qui mérite une analyse approfondie. Avec 10,45 milliards d'euros de chiffre d'affaires et 53 000 emplois en 2023, cette filière représente un poids économique significatif. Cependant, sa part dans les marchés publics numériques de grande ampleur reste minoritaire, révélant un déséquilibre structurel préoccupant.

L'analyse détaillée des attributions de marchés en 2023 est particulièrement révélatrice : huit grandes entreprises du numérique (Sopra Steria, Orange, SCC, ITNI, CGI, Capgemini, Computacenter, Thales) ont concentré environ 1,49 milliards d'euros de commandes informatiques de l'État. Plus inquiétant encore, aucune PME n'apparaît dans le classement des 30 premiers fournisseurs, témoignant d'un effet d'éviction systémique.

Cette situation est d'autant plus paradoxale que les entreprises françaises démontrent une excellence technologique reconnue internationalement. Comme l'a rappelé devant la commission d'enquête Jean-Noël de Galzain : "Nous avons aujourd'hui des acteurs du cloud qui sont performants et qui, avec les marchés vont se développer et peut être atteindront-ils la taille critique qui leur permettra d'être compétitifs face aux géants américains" .

Un problème structurel majeur réside dans la conception même des marchés publics qui privilégient des offres globales où la technologie est "invisibilisée" par le service. Cette approche crée une double problématique :

- Économique : Les grands intégrateurs serviciels sont souvent la clé d'entrée du marché. Or, ils contractualisent majoritairement auprès d'acteurs extra européens pour les briques logicielles du marché, ce qui invisibilise les consortiums de PME françaises innovantes.
- Technologique : car en l'absence de ces investissements, nos PME innovantes se retrouvent en difficultés pour continuer à proposer des solutions aux meilleurs niveaux et aux meilleurs prix

Cette situation est aggravée par le fait que les acheteurs publics pensent souvent acheter "souverain" en contractant avec des intégrateurs français, alors que la technologie sous-jacente est fréquemment d'origine extra-européenne.

2. Si tel n'est pas le cas, quels sont les principaux facteurs limitant l'accès de ces entreprises à la commande publique ?

Les obstacles à l'accès des entreprises françaises à la commande publique peuvent être analysés selon quatre dimensions principales :

Dimension structurelle :

- Les appels d'offre conçus comme des prestations globales forment une barrière à l'entrée pour les PME/ETI hautement spécialisées qui sont pertinentes sur un segment du marché
- Les exigences financières (CA minimum, garanties bancaires) sont souvent disproportionnées par rapport aux capacités des PME innovantes
- Les contraintes technologiques, notamment liées à l'écosystème Microsoft, créent des barrières à l'entrée qui devraient être surmontées :
    - « la trop souvente non-remise en compétition de la technologie, mais uniquement des prestataires de services, qui permettent aux acteurs extra-européens en place de conserver leurs monopoles de fait »
- L'inertie des systèmes en place favorise la reconduction des solutions existantes et souvent extra-européennes.

Dimension procédurale :

- La complexité administrative représente une charge particulièrement lourde pour les PME
- Les délais de réponse et de traitement, parfois de plusieurs mois, nécessitent une mobilisation de ressources importante
- La pondération excessive du critère prix (jusqu'à 70%) défavorise l'innovation et la qualité
- L'absence de "passeport fournisseur" unique multiplie les démarches administratives
- La non limitation de du nombre de lot attribués à un soumissionnaire laissant le champ libre aux acteur « hégémoniques »

Dimension culturelle :

- Le manque de formation des acheteurs publics sur les enjeux numériques, et sur les impacts économiques, stratégiques et géopolitiques du recours à des technologies, intégrateurs et infogéreurs extraterritoriaux par la commande publique et donc par les administrations, hôpitaux, collectivités ou OIV.
- Une aversion au risque qui favorise les acteurs établis
- Une méconnaissance des solutions françaises disponibles et le biais cognitif lié à l'effet de simple exposition.
- Une perception erronée du rapport qualité-prix des solutions souveraines

Dimension stratégique :

- L'absence de vision long terme sur la souveraineté numérique ou la gestion de nos dépendances
- Le manque de coordination entre politique industrielle et commande publique
- L'insuffisance des mécanismes de soutien aux PME innovantes
- La difficulté à valoriser les certifications et labels français

3. Avez-vous identifié des rigidités particulières dans les procédures applicables, de nature à faire obstacle à l'accès des entreprises françaises et européennes à la commande publique dans le domaine de la cybersécurité et du *cloud* ?

Certains membres d'Hexatrust regrettent avoir plus de facilités à contractualiser dans le cadre de la commande publique étrangère que sur certains marchés nationaux.

Les procédures actuelles présentent des rigidités systémiques qui pénalisent particulièrement les entreprises françaises et européennes. Ces rigidités peuvent être analysées selon plusieurs dimensions :

Dimension méthodologique :

- Le sourcing amont avec préférence européenne reste insuffisamment pratiqué, limitant la découverte des solutions innovantes françaises
- Les partenariats d'innovation de type France 2030, pourtant conçus pour favoriser l'émergence de solutions nouvelles, sont sous-utilisés
- L'allotissement fonctionnel ou géographique, qui permettrait aux PME de se positionner sur des segments spécifiques, n'est pas systématique
- Les grilles de notation favorisent souvent les acteurs établis au détriment de l'innovation
- L'absence de prise en compte du coût global de possession (TCO) dans l'évaluation des offres

Dimension administrative :

- L'absence de "passeport fournisseur" unique oblige à une répétition fastidieuse des démarches administratives
- La sur-réglementation interne des acheteurs publics va souvent au-delà des exigences légales
- Les dispositifs existants comme l'"achat innovant" permettant des achats jusqu'à 300 000€ sans publicité ni mise en concurrence préalables sont sous-exploités
- L'utilisation excessive des centrales d'achat, même pour de petits montants, complexifie l'accès aux marchés

Dimension stratégique :

- Les critères RSE et d'insertion sociale sont parfois utilisés de manière discriminante
- La pondération excessive du critère prix initial favorise les grands acteurs pouvant pratiquer des prix artificiellement bas
- Le manque de valorisation des certifications et labels français/européens

4. Quels sont les risques, pour les personnes publiques, de recourir à des prestataires de services informatiques en *cloud* soumis à des législations extraterritoriales ? Comment les membres d'Hexatrust parviennent-ils à échapper à cette contrainte ?

Les risques liés aux législations extraterritoriales constituent une préoccupation majeure pour la souveraineté numérique française. L'article 702 du FISA, le Calea Act, le Patriot Act et le Cloud

Act créent une situation de conflit juridique particulièrement problématique, autorisant les autorités américaines à accéder aux données, même lorsqu'elles sont hébergées dans l'Union Européenne. Comme l'a précisé Jérôme Lecat lors de l'audition : "Le fait que les données soient hébergées en France, c'est complètement neutre dans le sujet. Ce qui compte c'est quelle est la nationalité de l'exploitant". Par ailleurs, le chiffrement des données ne constitue pas une protection suffisante si les clés sont détenues par le prestataire.

Pour l'Europe, cette situation crée des risques stratégiques, entre perte de contrôle possible sur les données sensibles de l'État, risque d'utilisation des données à des fins de renseignement économique, dépendance accrue vis-à-vis d'acteurs étrangers, et vulnérabilité face aux changements de politique étrangère, comme le montre le contexte actuel.

Et le recours à des acteurs extra-européens doit également être analysé sous l'angle économique : celle-ci fait fuir de la valeur ajoutée hors du territoire national, un processus amplifié par les stratégies d'optimisation fiscale agressive des grands acteurs étrangers. Avec pour conséquence un affaiblissement de l'écosystème numérique français, notamment via la perte de compétences et d'expertise locales.

5. Dans quelle mesure le recours à une entreprise française ou européenne en matière de cybersécurité garantit-il une protection renforcée à l'acheteur public s'agissant de la protection de données stratégiques ?

Le recours aux entreprises françaises en matière de cybersécurité offre un niveau de protection particulièrement robuste, fondé sur plusieurs aspects complémentaires. La conformité réglementaire constitue un premier niveau de sécurité, avec un alignement total sur le RGPD et les normes européennes, renforcé par les certifications nationales (ANSSI, HDS, SecNumCloud). Cette conformité s'accompagne d'une immunité naturelle aux législations extraterritoriales, garantissant une protection juridique complète des données.

Il en va de même concernant l'infogérance ou le management des services d'infrastructures informatiques déployées directement sur site, effectué par une entreprise française. Les données restent en France, et plus précisément chez le donneur d'ordre et les services managés et l'accès qu'ils supposent aux données du donneur d'ordre sont performés par un acteur français sous législation territoriale.

La proximité opérationnelle représente un atout majeur, comme en témoigne Jean-Noël de Galzain : "Croyez-moi, quand on a un client qui nous appelle, je peux vous dire n'importe quel entrepreneur autour de la table, vous pouvez nous appeler à n'importe quelle heure du jour et de la nuit, le week-end, nous sommes toujours là pour répondre ». Cette réactivité s'accompagne d'une compréhension approfondie des enjeux réglementaires locaux et d'une capacité d'adaptation aux spécificités des organisations publiques françaises.

6. Les entreprises françaises précurseurs en matière de cybersécurité disposent-elles aujourd'hui de garanties technologiques et sécuritaires équivalentes aux leaders

mondiaux ? Les acheteurs publics ont-ils tendance à favoriser de grands éditeurs de logiciels internationaux dans leur politique d'achat ?

L'excellence technologique des entreprises françaises de cybersécurité et de cloud est, aujourd'hui, une réalité incontestable. Les éditeurs français ont développé des solutions à l'état de l'art dans des domaines critiques tels que le chiffrement, la détection et réponse aux menaces (EDR), les centres opérationnels de sécurité (SOC), les infrastructures de reprise ou continuité d'activité, les plateformes collaboratives, et les infrastructures cloud. L'investissement massif en R&D, atteignant parfois 25% du budget, témoigne de cet engagement vers l'excellence.

Pourtant, les tendances d'achat révèlent un paradoxe préoccupant. La "prime à la notoriété" et la recherche de continuité dans les suites logicielles créent une dépendance technique favorisant systématiquement les acteurs établis. Les acheteurs français, parfois par manque de connaissance des solutions françaises disponibles, privilégient ce qui leur semble être le « risque zéro », en faisant appel à des solutions dominantes

Aujourd'hui, un phénomène particulièrement inquiétant concerne les suites bureautiques : l'achat de licences peut inclure des fonctionnalités d'IA hébergées sur des clouds étrangers, permettant l'utilisation des données publiques pour l'entraînement de modèles d'IA étrangers, créant ainsi une nouvelle forme de dépendance technologique alors que des acteurs français et européens existent et permettent de localiser la donnée et l'usage sans crainte de fuites ou utilisations extraterritoriales pouvant porter préjudice à la compétitivité du tissu économique français et européen

7. Les marchés publics ayant trait au cloud et à la cybersécurité sont-ils souvent assortis de clauses et de critères sociaux et environnementaux ? Le cas échéant, dans quelle mesure leur présence est-elle un frein ou un levier dans l'accès des entreprises françaises et européennes ? Ces clauses et critères restreignent-ils l'accès des start-ups à la commande publique ou, au contraire, le favorisent-elles ?

La situation concernant les critères sociaux et environnementaux est complexe et en évolution. L'article 35 de la loi Climat-Résilience impose qu'à compter du 22 août 2026, tout marché public comporte au moins un critère environnemental. Ces exigences, lorsqu'elles représentent ≥ 10 % de la note, valorisent les offres locales (datacentres bas-carbone, emplois régionaux) et constituent un levier plutôt qu'un frein. Parallèlement, l'article 33 de la loi SREN va imposer aux fournisseurs de services cloud de publier des informations sur l'empreinte environnementale de leurs services, notamment en matière d'empreinte carbone, de consommation d'eau et de consommation d'énergie...

En théorie, ces critères devraient favoriser les entreprises françaises, notamment grâce à leurs datacenters alimentés en énergie décarbonée. Cependant, la réalité est plus nuancée :

- Le volet social, particulièrement l'emploi local qualifié et la formation, n'est pas suffisamment valorisé par les méthodes de notations actuelles.
- La complexité administrative liée à ces critères peut paradoxalement avantager les grandes structures internationales : les PME innovantes françaises peuvent se trouver

désavantagées face aux moyens marketing considérables des grands groupes pour documenter ces aspects souvent invérifiables (par manque de normes internationales et d'inspection ou revalidation desdites normes)

8. Avez-vous identifié une volonté particulière des acheteurs publics, et notamment de l'État, de soutenir l'accès d'entreprises française à la commande publique dans le domaine du numérique, de la cybersécurité et du *cloud* ?

La volonté de soutenir les entreprises françaises existe mais souffre d'un décalage important entre les intentions et la réalité. D'un côté, des initiatives comme la Stratégie nationale cybersécurité (France 2030), la doctrine "Cloud de confiance" et la création de labels témoignent d'une volonté politique. De l'autre, la pratique d'achat et la commande publique ne traduisent pas cette ambition.

Comme le souligne la filière depuis plusieurs années, le besoin n'est pas tant dans les subventions que dans les commandes effectives. Cette situation rejoint l'observation de Jean-Noël de Galzain : "Plus que le financement, c'est la commande qui représente le levier dont ont besoin les entreprises pour franchir le plafond de verre".

9. Disposez-vous d'exemples significatifs de marchés publics en matière d'hébergement de données remportés par des entreprises françaises et, au contraire, de marchés publics que de telles entreprises auraient dû, à vos yeux, remporter et qui ont été attribuées à des entreprises étrangères ?

Les succès significatifs des entreprises françaises dans les grands marchés publics restent malheureusement rares. En revanche, les occasions manquées sont nombreuses et préoccupantes :

- Le marché bureautique de l'Éducation nationale (2025) attribué à Microsoft malgré l'existence d'alternatives européennes
- La lenteur de la migration du Health Data Hub vers un opérateur cloud certifié SecNumCloud
- Le déploiement de pare-feux et sondes français dans plusieurs régions et hôpitaux sur Azure
- Le questionnement d'un OIV comme EDF sur l'hébergement de données sensibles sur un cloud extraterritorial

Dans le même temps, et comme l'a rappelé Hexatrust lors de son audition, aucun acteur de l'écosystème cyber ou cloud français peut s'enorgueillir d'avoir signé un tel contrat dans les dix dernières années, ce qui pose également un problème d'un point de vue réputationnel, et dans l'objectif de changer le narratif autour de la qualité des entreprises du numérique français.

10. Dans quelle mesure les entreprises de cybersécurité et de *cloud* étrangères accèdent-elles à la commande publique française ? À l'inverse, dans quelle mesure les entreprises françaises accèdent-elles à la commande publique étrangère ?

La situation révèle une asymétrie flagrante. Alors que le marché français reste largement ouvert, les États-Unis, par exemple, protègent leur marché via le Small Business Act qui réserve jusqu'à 40% des marchés fédéraux aux PME américaines. Cette asymétrie est d'autant plus significative que de nombreux leaders américains de la Tech ont bénéficié du soutien de la commande publique (DARPA, armées, renseignements, agences fédérales).

Ce modèle de soutien public se retrouve aujourd'hui dans de nombreux pays (Arabie Saoudite, Corée, Japon) et même, dans une certaine mesure, chez nos voisins européens comme l'Allemagne. Sans l'activation de ces leviers, la France aura des difficultés à faire émerger ses champions.

11. Quelles évolutions de la réglementation ou des pratiques des acheteurs publics recommanderiez-vous pour favoriser l'accès des entreprises françaises et européennes de cybersécurité à la commande publique ?

Les recommandations pour améliorer l'accès des entreprises françaises à la commande publique s'articulent autour de plusieurs axes :

Évolutions réglementaires :

- Adoption de mesures inspirées du Small Business Act, réservant une part de la commande publique aux acteurs PME/ETI françaises et européens.
- Créer une catégorie de marchés « sensibles cyber ». Par exemple, pour les achats liés à des SI critiques, imposer des conditions de souveraineté numérique (acteurs français ou européens certifiés) pour les OIV, voire les EE ou EI, pour s'assurer que l'accompagnement de NIS 2 se fait dans un esprit de réduction de nos dépendances.
    - Une approche « par catégorie » qui pourrait par ailleurs être appliqué dès aujourd'hui à l'IA et la localisation des données en France.
- Intégrer les notions de dépendance géopolitique et technologiques dans le **Guide pratique pour des achats numériques responsables** de la DINUM et dans les rapports annuels de l'Etat.

Simplification administrative pour les PME :

- Simplification documentaire (Passeport numérique) et allotissement systématique en vertu de l'**Article L2113-10** du CCP.
- Prise en compte obligatoire du coût complet (TCO) et de la réversibilité ;
- Favoriser le dialogue compétitif, qui part ses différentes étapes (expression des besoins, première soutenance, phase de questions) permet de mieux mettre en valeur les solutions et la capacité d'adaptation des acteurs français.

Nouveaux critères d'évaluation :

- Attribuer une part de la note à l'impact du soumissionnaire sur le développement économique territorial (emplois, formation, etc)

- Attribuer une part de la note à la qualité des mesures de cybersécurité (certifications, audits, SOC, etc.) les solutions certifiées et labellisées selon l'article **L2152-7** du CCP
- Intégrer les certifications ANSSI comme critères d'éligibilité aux marchés innovants.
- Privilégier les solutions éthiques et respectent la fiscalité
- Privilégier les solutions qui produisent en Europe
- Privilégier les solutions qui sont immunisées aux lois extraterritoriales
- Intégrer l'évaluation de la dépendance géopolitique et technologique dans le système de notation
- Privilégier un critère de proximité dans les délais d'intervention (localisation des données, supports en France, délai d'intervention, etc.)
- Exclure les opérateurs à risque qui ont fait l'objet d'une sanction pour non-respect d'obligations légales en matière de sécurité des SI (protections des données, extra-territorialité, etc), sur le fondement de l'article **L2141-7** du CCP.

L'article **R2152-7** du Code de la commande publique prévoit déjà la possibilité d'ajouter des critères qui nous permettraient de prendre en compte une dimension de souveraineté ou d'autonomie stratégique dans la commande publique, notamment au travers des **conditions de production et de commercialisation**, le **service après-vente**, la **sécurité des approvisionnements**, les **caractéristiques opérationnels**. D'autres **critères non listés peuvent être également pris en compte s'ils sont justifiés par l'objet du marché ou par son exécution**. La dépendance de la France aux solutions numériques américaines et l'abus de position dominante qui en découle doivent nous faire analyser les critères différemment.

Évolutions stratégiques :

- Continuité entre subventions d'innovation et commandes publiques
- Renforcement du sourcing
- Intégrer la cybersécurité dans les critères RSE
- Création d'un Médiateur des Marchés Publics pour favoriser les pratiques achats et la médiation en cas de besoin
- Formation des acheteurs aux enjeux du numérique et à l'impact économiques, stratégiques et géopolitiques du recours à des technologies, intégrateurs et infogéreurs extraterritoriaux
- Vigilance quant au recours à une procédure négociée sans publicité ni mise en concurrence préalables en raison de la présence de droits d'exclusivité pour mettre une barrière à l'entrée aux solutions « challengers ». (CJUE 9 janvier 2025, aff.C-578/23)

Selon l'étude Asterès commandé par le CIGREF, les entreprises US représentent 83% du marché du cloud-logiciel européen soit 54 milliards pour la France par an. « *La facture numérique de l'Europe est d'un montant comparable à sa facture énergétique* ».
Les tarifs cloud augmentent d'environ 10 % par an, grevant la balance des paiements européenne tout en améliorant celle des États-Unis de quelque 421 milliards d'euros sur dix ans !

Si 15% étaient réorientés vers des acteurs nationaux à échéance 5 ans, il s'agirait faire revenir 8 milliards d'euros vers les entreprises locales avec les conséquences induites que ce flux

provoquerait sur l'emploi, la taxation et le développement d'une politique industrielle structurante pour constituer de nouveaux industriels européens.

De la même manière, au regard de l'enjeux économique relatif à l'avènement de l'Intelligence Artificielle estimé à plus de 1200 milliards sur les trois prochaines années au niveau européen, il parait primordiale de router les achats publiques vers des entreprises françaises et européennes proposant des solutions sur cloud privés dédiés ou mutualisé, externalisé ou On-Premise (sur site client) muent par des LLM libre ou français/européen afin d'allier pertinence de l'investissement dans le tissu économique européen et préservation de l'indépendance technologique.

12. Quel regard portez-vous sur les articles 30 et 31 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique et leur mise en œuvre jusqu'à présent ? À votre connaissance, ces dispositions ont-elles conduit des personnes publiques à changer de prestataire pour des services informatiques de *cloud* ?

Ces articles représentent une avancée potentiellement significative :

- L'article 30 confie à l'ARCEP des pouvoirs de contrôle et de sanctions (amendes jusqu'à 3% du CA mondial) pour garantir la portabilité, l'interopérabilité et le plafonnement des frais de sortie dans le cloud.
- L'article 31 impose à l'État d'utiliser un cloud protégé de tout accès par une autorité non-UE pour les données d'une "sensibilité particulière", avec une première vague de migrations en cours dans les domaines de la santé et de la fiscalité.

Cependant, l'absence de décrets d'application rend complexe l'évaluation de leur mise en œuvre effective, illustrant la difficulté de la puissance publique à se saisir pleinement des outils réglementaires existants pour favoriser le développement de solutions souveraines.