



Les Rencontres CentraleSupélec

Quelle souveraineté demain ?

Vendredi 21 novembre 2025

ACTES DU COLLOQUE

**La souveraineté numérique :
une équation sans frontière ?**

Animatrice : Gabriela Belaid
Directrice Cybersécurité et Souveraineté



Gabriela Belaid (MS 10)

Co-Présidente
**CentraleSupélec Alumni
Au Féminin**

Intervenants :



Jean-Noël de Galzain

Fondateur et Président
d'Hexatrust et de WALLIX



Stéphane Clément

Président
de Tenexa



William Couchot (20)

Ecosystem Lead
S3NS

Table des matières

1. Introduction : une équation moderne inspirée des mathématiques.....	4
2. La souveraineté numérique : un concept pluriel et systémique	4
3. Cloud souverain et cloud de confiance : une différence fondamentale	6
4. Une dépendance inquiétante mais réversible.....	6
5. Le rôle de l'écosystème français	7
6. Régulation : frein ou opportunité ?	8
7. Conclusion : une responsabilité collective	8

1. Introduction : une équation moderne inspirée des mathématiques

Le numérique, par essence, ne connaît ni frontières, ni visas, ni douanes. À l'inverse, la souveraineté repose historiquement sur un territoire, des lois, des infrastructures, et une capacité politique à décider pour soi-même. Cette opposition structure un paradoxe fondamental, au cœur de la réflexion engagée lors de cette table ronde.

La souveraineté et le numérique peuvent être comparés à deux asymptotes : deux lignes qui se rapprochent à l'infini, mais qui ne se rencontrent jamais totalement. L'enjeu n'est donc pas une confusion des deux courbes, mais la réduction progressive de l'écart qui les sépare, dans un monde dominé par quelques géants technologiques extra-européens.

Dans un contexte de concurrence mondiale exacerbée, cette table ronde a interrogé les marges de manœuvre de la France et de l'Europe :

Que voulons-nous défendre ?

De quoi devons-nous réellement nous protéger ?

Et comment préserver notre autonomie stratégique dans un monde interconnecté ?

2. La souveraineté numérique : un concept pluriel et systémique

Stéphane Clément définit la souveraineté numérique comme la capacité à conserver la portabilité de son système d'information pour éviter l'enfermement technologique. Il insiste sur le devoir de souveraineté de l'État et la nécessité de faire des choix stratégiques sur les niveaux de protection des données.

Jean-Noël de Galzain perçoit la souveraineté comme la capacité à "avoir le choix". Le Larousse définit la souveraineté comme le caractère de ce qui est souverain, la souveraineté de ses décisions, et propose les synonymes autonomie et indépendance. Ces notions sont pleinement pertinentes lorsqu'on parle du numérique. Si le terme souveraineté n'est pas retenu dans certains débats, par ailleurs, c'est sans doute pour éviter ses connotations politiques, parfois jugées trop lourdes ou trop sensibles. Le numérique n'a pas de frontière et c'est pour cela qu'il met en tension le principe même de souveraineté. Or la souveraineté numérique consiste à garantir que l'internet reste un espace sûr et conforme à nos valeurs collectives, un espace où nos lois, nos choix et nos responsabilités peuvent pleinement s'appliquer.

Il prône un "renouveau numérique" pragmatique visant à reprendre le contrôle sur les données et le modèle économique pour financer la compétitivité. Il appelle les entreprises à augmenter leurs achats de technologies européennes pour créer un marché intérieur fort.

William Couchot aborde la souveraineté du point de vue du client, qui doit définir ce qui est souverain pour lui. Il explique que les solutions de "cloud de confiance" conformes au cadre de l'ANSSI, visent à protéger les données des lois extraterritoriales tout en accédant aux technologies d'hyperscalers comme avec S3NS par exemple. Il défend une approche pragmatique, reconnaissant que la collaboration avec des géants mondiaux permet d'acquérir un savoir-faire crucial en ingénierie à grande échelle.

Les échanges ont permis de dépasser une vision simplifiée de la souveraineté réduite à la seule localisation physique des données. La souveraineté numérique est apparue comme un concept complexe, recouvrant plusieurs dimensions complémentaires.

Elle concerne tout d'abord (1) la **souveraineté de la donnée** : sa localisation, son traitement, son hébergement, mais aussi l'ensemble de son cycle de vie, les conditions d'accès, et les environnements juridiques auxquels elle peut être soumise (2) la **souveraineté opérationnelle** : qui a accès à l'infrastructure de bout en bout, en particulier côté fournisseur et (3) la **souveraineté technologique** : la résilience, réversibilité et réponse aux scénarios catastrophe. Il a notamment été rappelé qu'une donnée hébergée en France peut néanmoins être accessible par un État étranger si l'un des prestataires des opérations est soumis à une législation extraterritoriale.

Stéphane Clément : *Il faut distinguer les niveaux de sensibilité des données : toutes n'ont pas besoin du même niveau de protection. Il faut faire des choix stratégiques. Certaines données nécessitent une protection maximale ("pur souverain"), d'autres un "cloud de confiance" (sans extraterritorialité), et d'autres peuvent utiliser des technologies non souveraines.*

William Couchot *La souveraineté de la donnée inclut tout son cycle de vie (transit, traitement, accès), pas seulement son lieu de stockage.*

Elle concerne ensuite la **souveraineté des infrastructures et des compétences** : la localisation des data centers, des équipes de supervision, de maintenance ou de support, ainsi que la maîtrise technique par des experts européens.

Enfin, la **souveraineté de la gouvernance et de l'actionnariat** est un facteur déterminant. La présence d'un seul actionnaire soumis à une législation étrangère peut suffire à remettre en question l'indépendance du système. La souveraineté ne peut donc être pensée uniquement en termes techniques : elle est aussi juridique, financière, économique et politique.

La souveraineté numérique n'est pas un contrôle absolu, mais la capacité de conserver le choix, d'éviter l'enfermement technologique et de maîtriser son destin économique et réglementaire.

3. Cloud souverain et cloud de confiance : une différence fondamentale

"Cloud de confiance" vs "Cloud souverain": Il existe une distinction entre le "cloud souverain" (idéal difficile à atteindre) et le "cloud de confiance", une approche pragmatique (définie en France par l'ANSSI via SecNumCloud 3.2) qui vise à se prémunir des lois extraterritoriales tout en utilisant des technologies avancées

Une distinction essentielle a été clarifiée au cours des échanges entre le concept de « cloud souverain » et celui de « cloud de confiance », deux expressions souvent confondues.

Le **cloud souverain** suppose une maîtrise complète de l'ensemble de la chaîne : infrastructures, logiciels, données, gouvernance, exploitation et décisions stratégiques. Il repose sur une autonomie totale, sans dépendance juridique ou technologique à une puissance étrangère.

Le **cloud de confiance**, en revanche, repose sur un modèle défini par l'ANSSI visant à garantir une protection contre l'application de toute loi extraterritoriale non EU. Cette approche peut être hybride dans lequel un acteur de confiance (souvent français ou européen) vient encadrer, sécuriser, opérer une technologie,

Ce modèle, aujourd'hui largement déployé en France, apparaît comme une réponse immédiate aux enjeux actuels, dans l'attente de la construction d'alternatives européennes pleinement autonomes.

4. Une dépendance inquiétante mais réversible

Un chiffre clé a fortement marqué les échanges : aujourd'hui, **83 % des dépenses numériques européennes bénéficient à des acteurs extra-européens**, principalement américains et asiatiques. Seuls **17 %** restent actuellement dans le tissu économique européen.

Cependant, cette trajectoire n'est pas irréversible. Un objectif volontaire mais atteignable a été évoqué : porter cette part européenne à **30 % en dix ans**. Cela représenterait près de **600**

milliards d'euros réinjectés dans l'économie européenne, permettant de stimuler l'innovation, l'emploi, la recherche et la compétitivité.

Cette bascule ne dépend pas uniquement des États. Elle repose également sur les **choix quotidiens des entreprises, des DSI, des acheteurs publics, des dirigeants, des ingénieurs et des citoyens**. La souveraineté apparaît ainsi comme un acte concret, répété, engagé — et non comme un simple discours politique.

Un appel est lancé pour que les entreprises européennes augmentent leurs achats de technologies locales afin de créer un marché intérieur robuste.

Jean-Noël de Galzain « Comme les États-Unis avec le *Buy American Act*, nous devons assumer un *Buy European Act* : faire évoluer la réglementation, créer une commande publique exemplaire et acheter européen. *Si le courage politique ne vient pas alors le changement devra venir des entrepreneurs eux-mêmes, qui construisent une alternative aux géants en développant des solutions numériques européenne. Le problème de fond est le manque d'éducation numérique des dirigeants, qui ont été engagés dans le cloud sans en mesurer les conséquences.*

Fragmentation du marché européen : Bien que premier marché mondial, l'Europe est fragmentée, ce qui empêche l'émergence de concurrents face aux géants américains et chinois. La stratégie française "Cloud au centre" est vue comme une transition nécessaire mais insuffisante.

5. Le rôle de l'écosystème français

L'exemple d'Hexatrust a illustré concrètement la capacité de structuration d'un écosystème souverain français. Fondée initialement par onze entreprises, puis élargie à plus de 150 acteurs, l'association constitue aujourd'hui un pilier de la cybersécurité et de la souveraineté numérique française.

Cette dynamique repose sur une conviction forte : **aucun acteur seul ne peut rivaliser durablement avec les géants mondiaux**. La coopération, la mutualisation des compétences et la construction de chaînes de valeur locales sont des leviers essentiels.

La souveraineté ne peut exister sans confiance mutuelle entre les producteurs de solutions numériques et les utilisateurs. Elle nécessite une relation renouvelée entre les acteurs publics et privés, fondée sur la transparence et l'engagement commun.

6. Régulation : frein ou opportunité ?

Contrairement à certaines idées reçues, la régulation européenne a été présentée non comme un obstacle, mais comme un **levier stratégique**. Des cadres tels que le RGPD, NIS2, SecNumCloud dans sa version 3.2. ou encore les discussions autour de l'EUCS contribuent à poser un socle commun de protection et d'exigence.

le référentiel SecNumCloud 3.2 de l'ANSSI est le seul qui fonctionne aujourd'hui pour se protéger des lois extraterritoriales

En structurant un cadre éthique et sécuritaire élevé, l'Europe peut construire un **modèle alternatif**, fondé sur la confiance, la protection des droits fondamentaux et la résilience des infrastructures. Une innovation qui ne respecte pas ces principes est vouée à perdre sa légitimité, voire son utilité.

L'innovation encadrée apparaît ainsi non comme un renoncement, mais comme une opportunité de différenciation dans un monde numérique saturé.

7. Conclusion : une responsabilité collective

Il ressort de cette table ronde une conviction forte : **la souveraineté numérique ne se décrète pas, elle se construit**. Elle ne sera probablement jamais parfaite, ni totale, mais elle peut être renforcée, consolidée et défendue.

Elle nécessite des décisions courageuses, une vision à long terme, des investissements soutenus, mais surtout une mobilisation collective. Elle implique les États, les entreprises, les ingénieurs, les chercheurs, les étudiants et les citoyens.

Ainsi, même si la souveraineté et le numérique resteront toujours, en partie, comme deux asymptotes qui ne se rejoignent jamais complètement, l'enjeu n'est pas de les confondre, mais de **réduire chaque jour un peu plus la distance qui les sépare**.

Pour reprendre les mots de clôture de la modératrice :

« La souveraineté numérique ne se décrète pas. Elle se construit. »