Souveraineté numérique : reprendre la main en France et en Europe

COMPÉTENCES, CYBERSÉCURITÉ ET COUCHES BASSES DU CLOUD

ASSOCIATION NATIONALE RECHERCHE TECHNOLOGIE

FUTURIS

JANVIER / 2024

Rapport de synthèse du groupe de travail de l'ANRT FutuRIS 2023

Travail présidé par Gérard Roucairol, Président honoraire de l'Académie des Technologies
Pierre Bitard, ANRT, auteur
Clarisse Angelier, ANRT, directrice de publication

Ces travaux sont soutenus financièrement par les soucripteurs FutuRIS :

AI CARNOT, AIR LIQUIDE, AMPRIC - AIX-MARSEILLE UNIVERSITE, ANR, BERGER-LEVRAULT, BOUYGUES, BRGM, CEA, CNRS, France UNIVERSITES, EDF, ENGIE, META, GENERAL ELECTRIC, INSERM, INSTITUT MINES TELECOM, INRIA, INSTITUT PASTEUR, MINISTERE DE L'EDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS, MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE, NOKIA BELL LABS, REGION PAYS DE LA LOIRE, SCHNEIDER ELECTRIC, SNCF, SERVIER, TOTAL ENERGIES

Le contenu n'engage que la responsabilité de l'ANRT en tant qu'auteur et non celle des institutions qui lui apportent leur soutien.

Liste des experts ayant participé au groupe de travail

Elie Allini, EXPLEO
Sophie Bethoux, CEA
Antoine Camus, Minalogic
Bruno Charrat, CEA
Stephan Courcambeck, STMicroelectronics
Jacques Fournier, CEA
Thomas Germain, SpieBatignoles
Emmanuel Lebeuf, POCLAIN
Thierry Lelégard, SiPearl
Jamel Metmati, Thales
Rémy Nicolle, AirLiquide
Pierre Parrend, EPITA
Laura Sasportas, Google
Isabelle Tisserand, La Poste

S O M M A I R E

INTRODUCTION

La plateformisation numérique des entreprises repose sur l'usage de clouds communicants, qui en forment l'infrastructure. La qualité de cette infrastructure numérique s'incarne dans les compétences des entreprises, des administrations, dont les laboratoires publics et les établissements d'enseignement supérieur, en matière de sciences et de technologies de l'information et de la communication.

Les compétences foncières de l'informatique en nuage sont celles concernant les systèmes d'exploitation. La cybersécurité du cloud ressortit aussi au hardware, en particulier au microprocesseur qui exécute les instructions et traite les données des programmes.

Pour la France et l'Europe, le domaine majuscule de regain en souveraineté numérique consiste en la conquête de l'autonomie sur les systèmes d'exploitation et les microprocesseurs. Une cybersécurité souveraine doit être conquise pour que les entreprises industrielles Européennes aient véritablement l'opportunité de s'approprier les usages du cloud.

Il ne peut y avoir, pour les entreprises européennes, de réelle autonomie stratégique dans l'espace des données et services industriels sans maîtrise de la chaîne de cybersécurité du cloud. Il ne peut y avoir de maîtrise de la chaîne de cybersécurité du cloud industriel sans une appropriation des couches basses du cloud, système d'exploitation et microprocesseur compris[1]. En ce domaine, l'enjeu clé des toutes prochaines années consiste en la formation en nombre et en qualité suffisante des compétences cœur de l'informatique en nuage. Cela concerne la plateformisation numérique, la course de vitesse doit donc être engagée au plus vite.

Trois grandes entreprises américaines, Amazon, Microsoft et Google (AMG), détiennent l'essentiel de la clientèle industrielle du cloud en France et dans le monde. L'appétit pour les formations académiques sur ces domaines des 'couches basses' semble pourtant, à de nombreux égards, insuffisant pour relever le défi de la reconquête de souveraineté. Dans France 2030, la stratégie nationale d'accélération pour la cybersécurité entend contribuer à créer 37 000 emplois d'ici 2025 (soit un doublement des emplois). C'est bien une forte amplification de l'investissement dans les formations sur les couches basses qu'il convient d'envisager si la France, en Europe, veut reprendre la main sur le cloud industriel. Pour que s'imposent des solutions alternatives européennes de cloud sécurisé.

Ce rapport est structuré en cinq chapitres. Le premier chapitre rend compte de l'importance du cloud en tant qu'infrastructure de circulation des données industrielles en France et en Europe. Importance encore relative en France, tant en volume d'usage qu'en qualité d'usage ; ceci nous incite à considérer qu'adopter une trajectoire souveraine devient une urgente opportunité. Le deuxième chapitre précise le besoin d'une politique industrielle du cloud qui s'attache à soutenir et à encourager aussi bien l'offre, ce qui est généralement fait, que la demande. Ce choix complémentaire étant posé, il s'agit d'identifier, de caractériser et de dessiner un chemin possible vers un niveau de souveraineté désirable. Le rappel et l'analyse d'une référence historique clé, la fin des grands systèmes propriétaires, s'avèrera alors utile. C'est bien au niveau des couches profondes du cloud que s'affirme la souveraineté numérique, ainsi que l'analyse le chapitre 3, qui introduit la notion de chaîne de cybersécurité du cloud. Au cours du chapitre 4 se trouve explicité le rôle que doit jouer le microprocesseur au sein de la chaîne de cybersécurité et sa complémentarité avec un système d'exploitation open source souverain. Le dernier chapitre synthétise le diagnostic et en fournit les traductions concrètes en termes de pistes d'action.

1 Composantes des 'couches basses' qui font l'objet des développements qui suivent.

01

Le cloud, infrastructure de la circulation des données industrielles

Les données caractéristiques du fonctionnement et de la performance des systèmes de production industrielle, en passant par la conception et la logistique, revêtent une importance accrue. Elles sont de plus en plus systématiquement mobilisées aussi pour elles-mêmes par les entreprises comme sources de création de la valeur. Comme nos travaux précédents l'ont illustré[2], les données acquièrent de la valeur lorsque, provenant de sources différentes, elles sont combinées au profit d'un métier, d'une solution, d'une innovation. Alors informations elles deviennent connaissances à la faveur des traitements dont elles font l'objet. Seules les connaissances actionnables dans un but déterminé acquièrent de la valeur.

1 / LE CLOUD INDUSTRIEL

Le cloud, ou informatique en nuage, est un système technique de stockage, de traitement et de mutualisation des données numériques par lequel la gestion des ressources informatiques peut être externalisée. Le « fournisseur de services de cloud » offre, moyennant un abonnement, l'accès à des capacités hardware et/ou software à ses clients selon un mode mutualisé. Compte tenu d'une production croissante de données et d'une velléité nouvelle de les exploiter en masse, selon des rythmes qui ne sont pas toujours anticipables, les entreprises industrielles se tournent vers ces ressources externes.

Les entreprises manufacturières sont aujourd'hui dotées de leurs propres réseaux de serveurs fréquemment articulés avec des services de cloud (i.e. une offre commerciale externe). Elles font nécessairement appel à une infrastructure opérant plusieurs clouds, hétérogènes car ne répondant pas tous aux mêmes prérequis techniques, standards et performances. Non seulement un donneur d'ordre et un sous-traitant n'ont pas de raison d'utiliser le même fournisseur de cloud, mais il est maintenant fréquent qu'une même entreprise utilise plusieurs fournisseurs de services de cloud (on parle alors de multiclouds). Grâce à l'interconnexion de clouds, les entreprises deviennent capables de combiner des jeux de données d'origines différentes et de les analyser ou d'exploiter des services complémentaires chez ces différents fournisseurs. Chacune poursuit par là-même son intérêt, que rien n'oblige à être en compétition avec celui de ses partenaires.

Les entreprises évoluant vers le smart manufacturing[3], de plus en plus d'appareils et d'équipements industriels sont connectés (IoT), le volume de données obtenu au cours des différentes phases du cycle de vie du produit s'accroit. De nouvelles applications, de nouveaux services supposent l'analyse de volumes massifs de données.

En pratique, l'infrastructure de clouds est composite et en constante évolution. Elle n'en demeure pas moins « (…) le support d'une transformation systémique de l'espace économique et sociétal[4] » dans lequel une très grande variété d'activités économiques prennent la forme de services en ligne, i.e. XaaS (« tout en tant que service »). Nous disons qu'elle constitue le support de la plateformisation numérique des activités socioéconomiques.

2 / L'USAGE DU CLOUD DANS LES ENTREPRISES

A l'échelle internationale, les entreprises utilisent de plus en plus l'infrastructure de cloud[5]. Près d'un tiers (30 %) des entreprises ont déclaré que 41 à 60 % de leurs données sont stockées dans un cloud externe, et 22 % ont indiqué que plus de 60 % y sont stockées. Une bonne partie des entreprises utilisent plusieurs fournisseurs de services de cloud, on parle de « stratégie multicloud ».

2 Cf. *"La 5G dans les chaines de valeur des données – Un défi technologique et industriel devant nous"*, Les cahiers de FutuRIS, ANRT, mars 2021 ; *"Prix et valeur des données dans la plateformisation numérique - Repères pour les relations interentreprises"*, Les Cahiers de FutuRIS, ANRT, octobre 2019.

3 Cf. *"Vers le smart manufacturing. Proposition d'un plan national"*, Les cahiers de FutuRIS, ANRT, mai 2022.

4 Comme l'écrit Gérard Roucairol dans *"Développer l'infrastructure de la société numérique. Réseaux de clouds et circulation vertueuse des données"*, Académie des technologies, 2022, non publié.

5 Cf. 2022 Thales Data Threat Report, Global Edition. https://mb.cision.com/Public/20506/3530950/b55a39d9e52a4074.pdf

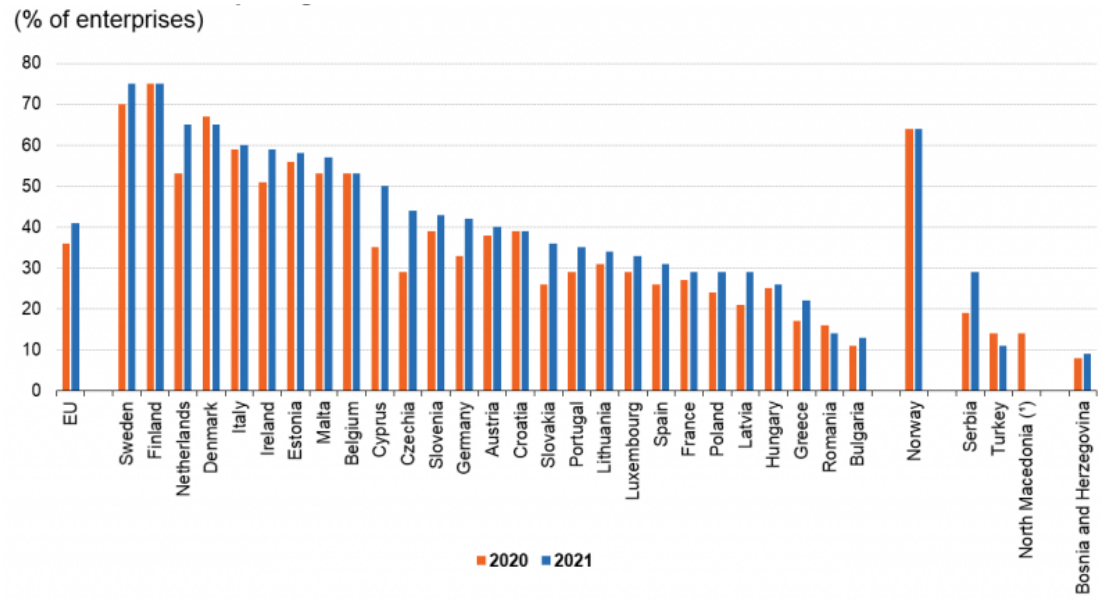
Ainsi, les entreprises utilisent fréquemment plusieurs fournisseurs pour l'infrastructure en tant que service (IaaS). En 2021-2022, 48 % des entreprises enquêtées ont déclaré utiliser AWS comme fournisseur IaaS, suivi de Microsoft Azure à 47 %. En 2020-2021, 53 % des entreprises ont déclaré avoir AWS comme leur fournisseur IaaS et 41 % Microsoft Azure, avec un chevauchement considérable entre Google Cloud, IBM Cloud, Oracle et Alibaba. L'utilisation du SaaS s'est diversifiée. 34 % utilisent au moins 50 applications SaaS et 17 % utilisent 100 applications SaaS ou plus.

Les entreprises localisées en France font, en Europe, partie de celles dont le taux d'usage des services du cloud compte parmi les plus faibles. Avec un peu moins de 30% d'usage en 2021, les entreprises françaises sont parmi les moins utilisatrices de l'Union européenne, à un niveau compris entre celui de l'Espagne et celui la Pologne. La moyenne européenne s'établissant à 41%.

et n'utilisent aucun autre des services couverts. Les entreprises utilisant des services cloud intermédiaires achètent au moins l'un des services suivants : application logicielle de finance ou de comptabilité, ERP, ou CRM en tant que service cloud, mais aucun des services sophistiqués. Les entreprises utilisant des services cloud sophistiqués incluent celles qui utilisent au moins l'un des éléments suivants : applications logicielles de sécurité, hébergement de bases de données d'entreprise ou plate-forme informatique fournissant un environnement hébergé pour le développement, le test ou le déploiement d'applications.

Seule une entreprise française sur cinq environ fait partie des entreprises utilisant les services les plus sophistiqués du cloud (dont les logiciels de cybersécurité). Elles sont donc parmi les moins dépendantes au cloud de l'UE (à la 21e place du classement).

Figure 1 - Usage du cloud par les entreprises en Europe en 2020 et 2021



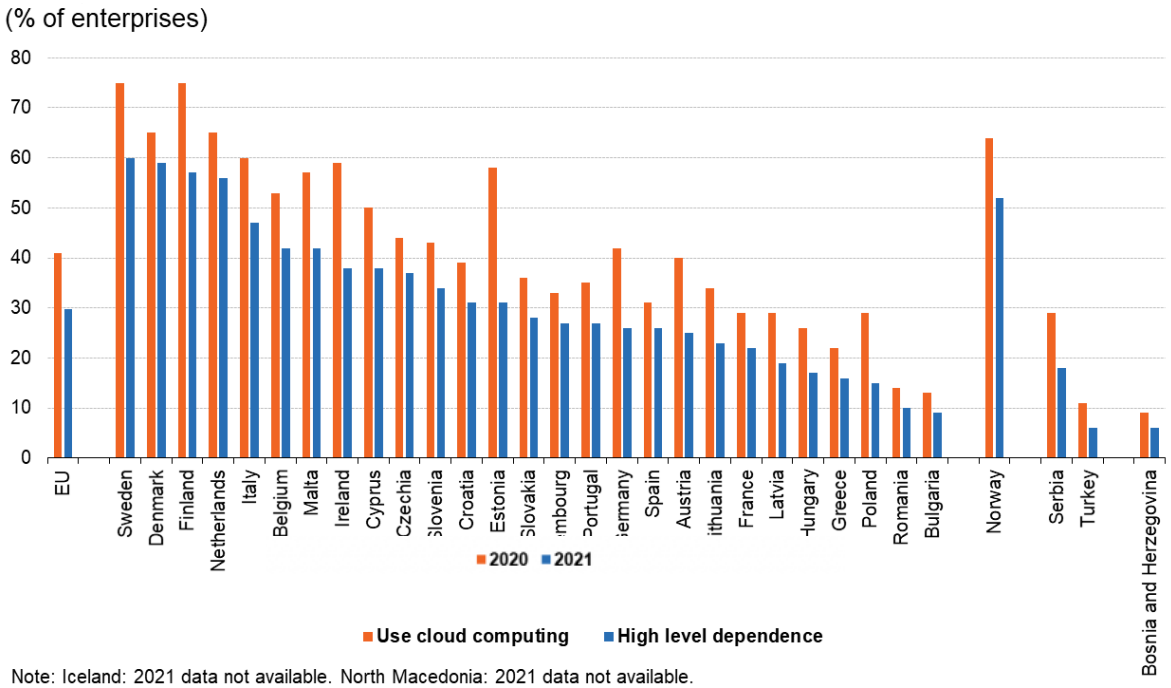
Source : https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

La même enquête d'Eurostat illustre les intensités d'usage du cloud par les entreprises, nommées « dépendances à l'égard des fournisseurs de services de cloud[6] ». Le degré de dépendance résulte du niveau de sophistication des services utilisés : plus l'entreprise utilise des services sophistiqués, plus grande est la dépendance. Les types de services ont été classés en trois niveaux : services de cloud de base, intermédiaires et sophistiqués.

Les entreprises utilisant des services cloud de base sont celles qui utilisent au moins l'un des services suivants : courrier électronique, logiciels de bureau, stockage de fichiers ou puissance de calcul pour exécuter les propres logiciels de l'entreprise,

6 L'enquête indique aussi qu'en moyenne en Europe l'usage du cloud varie selon la taille des entreprises, de 38% dans les petites à 72% dans les grandes en passant par 53% dans les moyennes.

Figure 2 - Usages du cloud et grande dépendance au cloud, 2021



Note: Iceland: 2021 data not available. North Macedonia: 2021 data not available.

Source : https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

Au-delà de cette enquête européenne, qui fournit de surcroît des points de comparaison, ni le niveau ni le degré de sophistication d'usage du cloud en France dans les entreprises industrielles ne sont suffisamment documentés. Très peu de travaux académiques contribuent au débat public et informent les décideurs publics. Ils ont même eu tendance à se raréfier au cours des cinq dernières années. Pourtant, plusieurs plans gouvernementaux cherchent à promouvoir et à renforcer l'écosystème français du cloud et ses composantes.

En outre, comme l'a illustré l'enquête d'Eurostat, la cybersécurité du cloud est considérée comme un « service très sophistiqué », impliquant un haut degré de dépendance.

Le tempo semble particulièrement adéquat pour prendre le bon virage en France vers des actions fortes qui favoriseraient l'adoption de solutions de services de cloud sécurisées et souveraines.

02

Vers une politique industrielle du cloud

Lorsque la politique industrielle entend s'avérer transformatrice et promeut un changement de paradigme (ex. passage de la mobilité thermique à la mobilité électrique), il convient de l'aborder « par les deux bouts » : par l'offre et par la demande[7]. C'est typiquement le cas en matière de politique industrielle du cloud.

1 / UNE POLITIQUE INDUSTRIELLE COMPLÈTE

Mobilisant une variété d'instruments, la politique publique soutient les entreprises d'un secteur, ici les fournisseurs de services de cloud, et les contributeurs en technologies ou en produits et services au secteur. Comment favoriser leur développement et leur croissance afin qu'ils prospèrent sur le territoire national (chiffre d'affaires, emploi) et au-delà ? Par une politique d'offre classique, « techno-push », qui consiste à soutenir l'écosystème du cloud. Ce dernier comprend des entreprises devant concurrencer les fournisseurs de services de cloud dominants et une myriade d'entreprises de tailles variées, startups comprises, susceptibles de fournir des briques technologiques, voire des services aux champions nationaux. Selon cette approche, la souveraineté économique nationale résulterait « naturellement » d'une action de l'Etat au profit de l'écosystème identifié.

Il peut être pertinent et puissant pour l'Etat de compléter sa politique industrielle par des mesures en faveur de la demande. En l'occurrence, la politique publique s'attachera à contribuer à l'adoption d'un nouveau système technique dont les vertus sont jugées désirables pour l'amélioration de la performance industrielle nationale. Tout en s'assurant de fournir aux industriels offreurs de biens et services visés - ici les fournisseurs de services de cloud nationaux - une opportunité de montée en puissance et de montée en gamme. Le choix des instruments de cette politique de la demande, dont on voit que la complémentarité avec la politique de l'offre est clé, se révèle délicat. La phase de design de la politique nécessite l'acquisition d'une compréhension fine du besoin des utilisateurs/consommateurs – i.e. des usages – et donc aussi des capacités et performances du système technique à l'état de l'art, tel qu'il peut être produit par les industriels nationaux. Les pouvoirs publics s'attachent alors à développer une politique d'infrastructure, au sens fort. Elle peut être envisagée comme un investissement majeur dans des conditions-cadres favorables à l'industrialisation. La souveraineté économique nationale procédera ici d'une rencontre judicieuse entre les ambitions politiques et les capacités et besoins industriels. Cette forme de souveraineté n'a rien de mécanique, et ne découle donc pas simplement d'une décision étatique. Si bien que se pose alors la question pour l'Etat et les entreprises du juste degré de souveraineté atteignable.

Pour un pays comme la France au sein de l'Union européenne, la voie d'atteinte du niveau de souveraineté souhaitable en matière de cloud est étroite et reposera nécessairement sur la combinaison judicieuse d'actions de politique industrielle orientées offre et demande.

2 / VERS UN NIVEAU DE SOUVERAINETÉ DÉSIRABLE

Les entreprises collectent, stockent et manipulent d'immenses quantités de données. Si l'on adopte la perspective de l'entreprise, la souveraineté en matière de données[8] consiste à être capable de déterminer les conditions précises selon lesquelles, si elles le souhaitent, d'autres entreprises peuvent utiliser certaines de ses données : quand, comment, voire à quel prix.

L'atteinte d'un haut niveau de transparence au sein d'une chaîne d'approvisionnement permet des gains répartis entre les acteurs qu'elle contient ; le partage des données rend possible la participation d'entreprises nouvelles susceptibles de fournir un service

7 Criscuolo, Chiara., N. Gonne, K. Kitazawa, G. Lalanne, K., 2022, *An industrial policy framework for OECD countries: old debates, new perspectives,* OECD science, technology and industry papers Policy papers, n°127.

8 Référence à l'approche de l'International Data Space Association: *"Sharing data while keeping data ownership. The potential of ids for the data economy"*, Livre blanc, IDSA, Octobre 2018.

spécialisé sur un maillon de la chaîne. Dans l'industrie automobile, sont souvent citées des sociétés fournissant des services d'impression 3D. Sécurité et confidentialité y sont préservées grâce à la mise en place des outils qui permettent la circulation de modèles de pièces (virtuels) par exemple. Selon cette acception des termes 'souveraineté des données', les entreprises qui détiennent les données peuvent protéger celles des utilisateurs. Souveraineté est alors synonyme de garantie d'un usage des données conforme à des règles protectrices strictement définies. A l'échelle des entreprises françaises et européennes, l'atteinte du niveau de souveraineté désirable correspond à leur maîtrise technique[9] de leur environnement de données.

La valeur des données résulte de leur circulation. L'Union européenne constitue, dans le monde, une remarquable exception en ce domaine : elle a inscrit ce principe comme source de développement économique dans une série de lois (RGPD, DMA, DSA et DGA) et d'initiatives coordonnées[10]. Le régime juridique de l'Union procède de ces institutions – i.e. les lois et règlements dans lesquels s'incarnent ces principes et valeurs – qui revêtent un double caractère de protection et d'encouragement à l'initiative économique. Car ce sont bien les règles collectivement adoptées et mises en œuvre qui expriment les principes sur lesquels se fondent la souveraineté. Le cadre légal et règlementaire européen créée des conditions propices à la circulation des données industrielles.

En matière d'usage du numérique (confidentialité, *privacy*, interopérabilité, etc.), le modèle étatsunien affiche un régime morcelé : les Etats fédérés relèvent de règles différentes, et surtout, les entreprises dominantes du secteur, les AMG (Amazon, Microsoft, Google) revendiquent et mettent en œuvre des règles propres. Cette archipellisation de l'espace numérique américain s'articule à la propension à déployer leur droit à l'échelle internationale. Par les risques, voire les menaces, qu'elle fait peser sur l'usage des données qui circulent *via* des acteurs américains, l'extraterritorialité du droit américain en matière numérique compense sa faible cohérence intrinsèque. Tout se passe comme si la bataille des normes et des technologies était remportée sur un autre terrain, celui du droit. Le réseau constitué par les utilisateurs des AMG, les entreprises dominantes du secteur, représente les trois quarts du marché mondial du cloud et constitue de fait l'arme de la souveraineté américaine.

Dans ce contexte, quelle voie stratégique privilégier pour la France afin qu'elle accède au niveau de souveraineté en matière de numérique industriel auquel elle peut légitimement aspirer ?

3 / UN CHEMIN VERS LE NIVEAU DE SOUVERAINETÉ VISÉ

L'histoire des technologies peut aider à l'identification d'une stratégie d'accès au niveau de souveraineté visé. Un parallèle historique peut être suggéré avec la fin de la domination des mainframes d'IBM et l'émergence et la généralisation d'Unix entre le milieu des années 1970 et le début des années 1990. La manière dont s'est déroulée la transformation doit guider les stratégies nationale et européenne pour tirer tout le bénéfice qu'il y a lieu d'attendre d'une souveraineté reconquise.

Ainsi, les ordinateurs centraux IBM, « grands systèmes » le plus souvent nommés simplement « Mainframes IBM », ont largement dominé le secteur informatique des années 50 jusqu'au milieu des années 70. Le célèbre System/360 a été le premier ordinateur à inclure du hardware dédié à l'utilisation de systèmes d'exploitation, mais aussi des programmes et des instructions en mode superviseur et des applications, ainsi que des fonctions de protection de la mémoire intégrées. Ce système intégré comportait donc une machine équipée du programme qui pilote l'utilisation des ressources et des logiciels applicatifs. Ce faisant, l'utilisateur subit un effet de lock-in (ou enfermement propriétaire). Des parties distinctes mais complémentaires du système sont encapsulées de manière indissociables et spécifique dans le produit, formant un tout. L'utilisateur était donc techniquement empêché d'acheter ailleurs que chez IBM des composants ou applications que requerrait l'usage de l'ordinateur central. L'interopérabilité technique n'était d'ailleurs pas assurée et les conditions contractuelles et de garantie le précisaient clairement.

Cette situation de lock-in fait écho à celle, actuelle, du cloud selon les AMG. Les offres de services des Amazon Web Services, Microsoft Azure et Google Cloud, intègrent de facto verticalement toutes les couches, qui sont proposées comme intégrées. Avec chaque marque, il est possible d'effectuer la totalité des services accessibles en cloud : calcul, stockage, réseau, gestion de base de données, analyse de données, services applicatifs, déploiement, gestion de système, etc. Comme pour le System/360 d'IBM, une fois acheté, l'accès à une machine (virtuelle) comprend une couche d'applicatifs de différents niveaux. On peut donc dire que l'informatique en cloud est « repropriétarisée », i.e. victime d'un nouvel « enfermement propriétaire ».

Du fait de leur caractère fermé, les mainframes propriétaires ont souffert à la longue de leur insuffisante capacité d'innovation. Les systèmes d'exploitation se sont retrouvés sur des machines qui n'étaient pas assez puissantes.

L'irruption du système d'exploitation standard développé en UNIX a changé la donne. Ainsi, UNIX a apporté l'interopérabilité et la transparence des protocoles de communications, ce qu'on a appelé les « systèmes ouverts ». Si Unix a commencé par être une plate-forme pour les programmeurs dévelop-

9 Et juridique et en termes d'organisation.

10 Cf. EC, 2020, "Shaping Europe's digital future", Communication, Février.

pant des logiciels, le système s'est étendu progressivement lorsque le système d'exploitation (BSD et « system V (5) »[11]) commençait à se répandre dans les cercles universitaires et que les utilisateurs ajoutaient leurs propres outils au système et les partageaient avec des collègues. Tout un écosystème libre s'est alors développé après la première vente de licence UNIX par les Bell Labs, en 1975, au département d'informatique de l'Université de l'Illinois. De nombreuses startups l'ont adopté et adapté jusqu'à devenir largement majoritaire dans les années 90, voir notamment la version libre européenne Linux. UNIX a contribué à une dépropriétarisation des systèmes d'exploitation, des OEM d'ordinateurs, des éditeurs de logiciels, etc. Androïd et MacOS sont tous deux développés sur une base UNIX.

Une même logique devrait présider au développement d'un nouveau système d'exploitation cloud concurrent européen de celui des AMG. A l'instar de l'exemple d'UNIX, une clé pourrait se trouver dans l'IaaS, l'infrastructure en tant que service. La fin de la dépendance totale aux clouds des AMG pourrait passer par le déploiement d'un « Linux de l'IaaS », un système d'exploitation standard pour le cloud développé en open source. La maîtrise européenne d'un tel système d'exploitation et des composants liés représente la meilleure chance du regain d'autonomie stratégique et d'innovations désirés.

11 Cf. Dans les années 1980 et au début des années 1990, UNIX System V et Berkeley Software Distribution (BSD) étaient les deux versions majeures d'UNIX, https://en.wikipedia.org/wiki/UNIX_System_V.

03

Les couches profondes du cloud, espace de définition de la souveraineté numérique

L'offre de cybersécurité du cloud émane principalement aujourd'hui des 'services-providers', les fournisseurs de service de cloud AMG (Amazon Web Services, Microsoft Azure et Google Cloud). Ces derniers sont aussi de plus en plus systématiquement concepteurs et propriétaires des technologies sous-jacentes[12]. Cette interdépendance technique forte crée un brouillage qui renforce le lock-in et constitue une menace accrue pour la souveraineté.

1 / LA CHAÎNE DE CYBERSÉCURITÉ DU CLOUD

La chaîne de cybersécurité représente le maillon faible de la souveraineté pour deux raisons : la première, technique, la seconde, économique. Techniquement, l'attention se focalise sur le processus (le chemin emprunté par la « charge virale » de l'attaque) alors que la solution peut se trouver au cœur du système (le microprocesseur).

La seconde raison tient au fait que le marché du cloud est un oligopole renforcé par des effets de lock-in. Ainsi, certains fournisseurs de services de cloud vont jusqu'à concevoir leurs propres microprocesseurs[13]. La performance des services rendus par le cloud, qu'il s'agisse d'Iaas, de PaaS ou de SaaS, ou d'une combinaison de ceux-ci, est alors présentée comme optimisée du fait de l'imbrication hardware/software propre à l'AMG vendeur[14].

Cette nouvelle donne où la cybersécurité est encapsulée dans les systèmes d'exploitation et dans les offres des services providers relève de la stratégie des acteurs dominants. L'oligopole en place en tire parti, les entreprises émergentes, proposant des solutions en rupture sur l'un ou l'autre segment des nombreux marchés impliqués la combattent. De multiples barrières à l'entrée naissent de cette situation sur autant de niches et de segments de marché que peut en contenir la chaîne de services de cloud, sécurité comprise.

Les étudiants, en France et en Europe, savent qu'a priori l'obtention d'une certification des AMG en cybersécurité a des chances de leur garantir un emploi. Si la formation fondamentale sur les couches basses compte, l'accès à l'emploi dans l'une de ces sociétés nécessite 'seulement' la bonne certification. Une pénurie de ressources humaines spécialisées en cybersécurité sévit tandis que les besoins augmentent.

Outre le système d'exploitation, le processeur constitue un maillon essentiel de la chaîne de cybersécurité (voir infra) et ne doit pas être une source de risque de brèche. Une entreprise européenne a conçu et développe un processeur qui entend apporter un supplément de sécurité au-delà de ce que permettent les processeurs classiques du cloud, SiPearl. Autour d'elle, et de quelques autres, doit être mis en place un écosystème européen qui forme aux métiers du design et de la production de microprocesseurs. L'une des principales entreprises mondiales du secteur est ASML, aux Pays-Bas, qui fabrique des machines à graver les circuits intégrés sur des galettes de silicium, matière première des producteurs de microprocesseurs.

L'architecture du cloud procède de développements modulaires à partir de microservices[15]. On doit s'interroger sur la capacité des formations en cybersécurité en France à adresser cette problématique. Rappelons que les entreprises localisées en France font, en Europe, partie de celles avec le taux d'usage des services du cloud les plus faibles

12 Ce faisant, ils concurrencent directement les technology-providers du cloud tels Intel ou AMD.

13 En juillet 2022, Google Cloud a annoncé qu'elle avait commencé à adopter des puces informatiques basées sur la technologie d'ARM. Là où Amazon (et Alibaba) conçoivent leurs propres puces basées sur ARM et les font fabriquer par des usines de puces, l'offre de Google tirera partie des puces Altra d'Ampere Computing. Entreprise américaine fabless qui conçoit des microprocesseurs de serveurs cloud natifs. Avec l'annonce du chip « Microsoft Azure Cobalt 100 » équipé de cœurs ARM, mi-novembre 2023, Microsoft fait maintenant partie des opérateurs cloud qui développent leurs propres microprocesseurs pour leurs besoins internes.

14 Cette tendance se retrouve chez des OEM en dehors du secteur informatique. Le constructeur automobile Tesla vend des véhicules électriques proposant de l'assistance à la conduite. Cette dernière nécessite une grande puissance de calculs pour pouvoir entraîner les modèles et gérer la masse de données nécessaire. Le constructeur a annoncé avoir créé sa propre puce, en août 2021. La « Tesla Dojo D1 » a été conçue spécifiquement pour l'entraînement de modèles d'intelligence artificielle de conduite semi-autonome, elle dispose d'une puissance de traitement de 360 TFLOPS.

15 Selon Microsoft, l'architecture de microservices désigne un style d'architecture utilisé dans le développement d'applications. Les applications cloud natives modernes sont généralement construites sous forme de microservices à l'aide de conteneurs. Cf. https://cloud.google.com/learn/what-is-microservices-architecture?hl=fr

(parmi les 7 derniers pays européens, au niveau de l'Espagne et de la Lettonie).

2 / LA CYBERSÉCURITÉ, FONDEMENT DE LA SOUVERAINETÉ

La montée en puissance de l'usage du cloud s'est accompagnée d'un nombre croissant d'attaques informatiques, certaines spectaculaires. Se sont développées de nouvelles menaces d'un haut degré de dangerosité pour les organisations et infrastructures d'importance stratégique voire vitale. La place prise par les services de cloud dans tous les secteurs de la vie économique nationale fait de la cybersécurité la clé de voute de la souveraineté. En attestent les travaux, actions et initiatives de l'ANSSI, mais aussi des acteurs de la recherche et de l'enseignement supérieur. Avec ces derniers, se joue la capacité du système français à disposer des compétences en qualité et en nombre susceptible de soutenir l'effort en matière de cybersécurité.

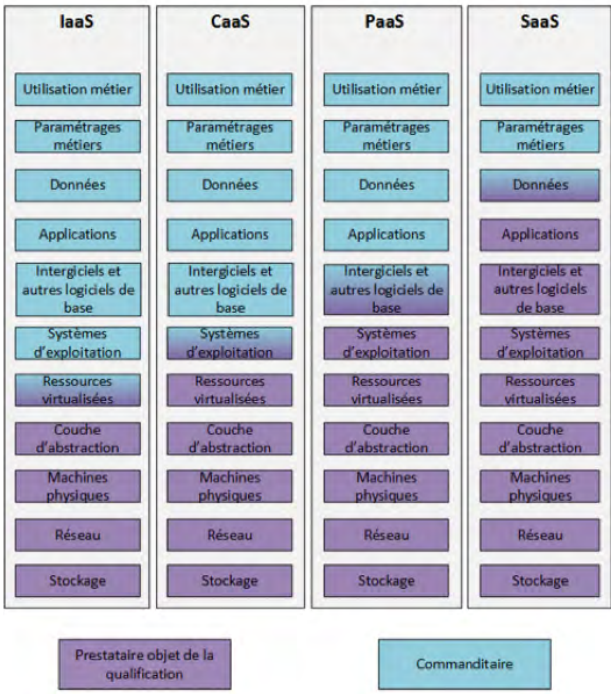
2.1 / L'ANSSI ET LE RÉFÉRENTIEL SECNUMCLOUD

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a pour mission « d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale ». Son envergure d'autorité nationale de cybersécurité ne cesse de croître depuis sa création, par décret, en juillet 2009[16]. Elle fonde sa doctrine sur les principes fondamentaux de la sécurité de l'information suivants : confidentialité, intégrité et disponibilité. C'est à partir de ces principes que les composantes techniques de la cybersécurité des infrastructures ont été renforcées pour répondre aux problématiques nouvelles liées au cloud.

Élaboré en 2016 par l'ANSSI, le référentiel SecNumCloud[17] permet la qualification de prestataires de services de cloud. Il entend promouvoir, enrichir et améliorer l'offre de prestataires de confiance à destination des entités publiques et privées souhaitant externaliser l'hébergement de leurs données, applications ou systèmes d'information. La qualification atteste de la qualité et de la robustesse de la prestation, de la compétence du prestataire ainsi que de la confiance pouvant lui être accordée. Respecter les exigences du référentiel SecNumCloud garantit le stockage et le traitement de données sensibles (i.e. pour le commandtitaire).

Quatre types de services fournis par les fournisseurs de services de cloud sont concernés : le SaaS (applications hébergées sur une plateforme cloud), le PaaS (plateformes d'hébergement d'applications), le CaaS (mise à disposition d'outils permettant le déploiement et l'orchestration de conteneurs) et l'IaaS. L'ANSSI définit l'IaaS comme un service de « mise à disposition de ressources informatiques abstraites (puissance CPU, mémoire, stockage etc.). Le modèle IaaS permet au commanditaire de disposer de ressources externalisées, potentiellement virtualisées. Le commanditaire conserve le contrôle sur le système d'exploitation (OS), le stockage, les applications déployées ainsi que sur certains composants réseau (pare-feu, par exemple) ».

Figure 3 – Modèle de répartition des responsabilités selon le type de service (typologie de l'ANSSI)



Le SecNumCloud fournit une nomenclature des domaines/activités de cybersécurité à surveiller : politiques de sécurité de l'information et gestion du risque ; organisation de la sécurité de l'information ; sécurité des ressources humaines ; gestion des actifs ; contrôle d'accès et gestion des identités ; cryptologie ; sécurité physique et environnementale ; sécurité liée à l'exploitation ; sécurité des communications ; acquisition, développement et maintenance des systèmes d'information ; relations avec les tiers ; gestion des incidents liés à la sécurité de l'information ; continuité d'activité ; conformité.

A l'échelle européenne, et avec la participation de l'ANSSI, est développée l'European Union Cloud Services Scheme (EUCS). Une version préliminaire du dispositif European Cybersecurity Certification Scheme for Cloud Services, qui définit la certification cybersécurité des services de clouds, a été publiée en décembre 2020. Le texte a fait l'objet d'une consultation publique, il continue à être soumis à discussions, la version finale n'est pas disponible. Au-delà de ces difficultés de tempo, on soulignera

16 Ses effectifs ont augmenté de 120 à sa création en 2009 à près de 600 en 2021, avec un objectif de 750 personnes.

17 « SecNumCloud » est le référentiel d'exigences pour les prestataires de services d'informatique en nuage. https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf

les éléments suivants. Rien n'interdit aux majors du Cloud américains et d'ailleurs de viser une certification EUCS. Bien souvent, ils font partie des tout premiers à obtenir de telles certifications. S'ils sont américains, comme nous l'avons souligné plus haut, bien qu'ils hébergent les données en Europe, avec du personnel européen, dans des filiales de droit européen, ils seraient tenus de répondre à une requête des autorités américaines dans le cadre du Cloud Act. Les hyperscalers disposent des meilleures compétences juridiques leur permettant de répondre parfaitement à l'ensemble des critères technico-juridiques de la certification. Laquelle s'intéresse à la forme et non au fond.

L'importance accordée à la cybersécurité en France ne se réduit pas au poids d'une agence nationale. Plusieurs initiatives politiques récentes dans le cadre de France 2030 par exemple ont été lancées pour améliorer, par les compétences, la capacité nationale de défense et de contre des menaces cyber. Initiatives auxquelles des écoles d'ingénieurs, des universités et des établissements publics de recherche prennent activement part.

2.2 / L'ENGAGEMENT DU CEA

Les acteurs américains et israéliens dominent le secteur industriel de la cybersécurité. Afin de garantir leur sécurité et leur souveraineté dans le numérique, la France et l'Europe ont lancé depuis 2016 de nombreuses initiatives. Elles poursuivent plusieurs objectifs : l'émergence d'une filière au meilleur niveau mondial, l'atteinte de ruptures et de la souveraineté dans certaines technologies clés, la création un bouclier cyber. Elles visent, en accord avec leurs valeurs de démocratie et de droits de l'Homme, à augmenter la sécurité de la société numérique.

Depuis le début des années 2000, le CEA a constitué des équipes de recherche d'excellence en cybersécurité, contribuant au développement d'une filière industrielle française souveraine. La position du CEA découle de la construction d'une expertise opérationnelle en cyberdéfense et en recherche technologique en cybersécurité. Aujourd'hui, près de 160 ingénieurs et chercheurs développent de nouveaux outils d'analyse de la sécurité des matériels et des logiciels et des technologies pour sécuriser les systèmes d'information (SI) contre les risques et menaces présents et futurs. Le CEA mène plusieurs programmes de recherche avancée au plus proche des besoins des industriels nationaux en matière de technologies de souveraineté. La cybersécurité des systèmes d'exploitation en fait éminemment partie. Ses activités de recherche sont structurées selon deux axes : l'analyse des vulnérabilités et la protection des systèmes avec des travaux de recherche portés par ses deux instituts phares sur ces sujets, le CEA-Leti à Grenoble et le CEA-List à Saclay.

Le CEA-Leti conduit des activités de recherche sur la sécurité du matériel. Ses laboratoires de sécurisation des composants et des systèmes électroniques traitent l'enjeu de sécurité des couches basses en proposant des briques et de nouvelles architectures de composants intrinsèquement sécurisés aux attaques. Le CEA-Leti héberge par ailleurs un des trois Centres d'évaluation de la sécurité des technologies de l'information (Cesti) « hardware » du schéma Français de certification, dirigé par l'ANSSI. Ces Cesti évaluent notamment la sécurité de composants hardware, comme des puces et des boîtiers sécurisés de type HSM (Hardware Security Materiel), indispensables dans les infrastructures numériques sécurisées.

Le CEA-List conduit des activités de recherche sur la sécurité des logiciels et des données. Il développe ainsi des outils d'analyse de vulnérabilité des systèmes logiciels, comme Frama-C et Binsec et de nouvelles technologies de sécurité, comme le chiffrement homomorphe, la détection d'intrusion ou de nouveaux systèmes d'exploitation embarqués (Xanthos).

Le CEA est co-pilote scientifique de l'ensemble des programmes de recherche (PEPR) des stratégies d'accélération du numérique (Quantique, Cybersécurité, IA, Cloud, 5G, Electronique) et des PEPR exploratoires NUMPEX et SPIN, ce qui lui donne une vision consolidée des enjeux de cybersécurité dans l'approche système couplant matériel, logiciel et données mentionnée ci-dessus. Dans la stratégie nationale pour la cybersécurité, il est impliqué aux côtés de l'Université Grenoble Alpes et de l'Institut Mines Télécom dans leurs actions de formation financées par l'initiative Compétences et Métiers d'Avenir.

Il copilote également avec le CNRS et Inria le programme de recherche (PEPR) Cybersécurité, doté de 65M€ sur 6 ans et assure de plus la responsabilité programme. Dans ce PEPR, trois projets sur la sécurité des systèmes sont en cours depuis 2022 :

- Le projet SUPERVIZ (Supervision et orchestration de la sécurité) cible la détection, la réponse et la remédiation aux attaques informatiques, sujets regroupés sous l'appellation de « supervision de sécurité », qui cherche à renforcer les mécanismes de protection préventifs et à pallier leurs insuffisances.
- Le projet SECUREVAL, coordonné par le CEA, vise à concevoir de nouveaux outils bénéficiant des nouvelles technologies numériques pour vérifier l'absence de vulnérabilités matérielles comme logicielles, et réaliser les preuves de conformité requises.
- Le projet ARSENE, coordonné par le CEA, vise à accélérer de manière coordonnée et structurée la recherche et le développement de solutions de sécurité souveraines et industrialisables. La mise en œuvre de démonstrateurs ASIC et FPGA intégrant les briques étudiées et développées permettra dans une dernière étape de tester et valoriser ces travaux de recherche.

2.3 / ENSEIGNEMENTS ET FORMATIONS DANS LES UNIVERSITÉS ET ÉCOLES

Plusieurs écoles et universités prodiguent en France des cours de niveau L ou M consacrés aux aspects fondamentaux des systèmes d'exploitation et de leurs interactions avec le hardware dans la perspective d'une formation diplômante en cybersécurité. Au-delà des cas listés ici, ces aspects fondamentaux n'apparaissent en tout état de cause pas comme majeurs au sein des enseignements. En tout cas, pas à la hauteur des enjeux de souveraineté nationale.

L'École pour l'informatique et les techniques avancées (EPITA) dispense des formations en cybersécurité et, depuis 2019, est devenue partenaire de la Défense Nationale française dans ce domaine. Plus récemment, son Bachelor Cybersécurité a obtenu le Grade de Licence et sera opéré à partir de la rentrée 2024 avec l'Ecole Polytechnique pour préparer une partie des promotions aux métiers du Ministère des Armées. L'école héberge au sein de son laboratoire de recherche une équipe spécialisée dans la cybersécurité et les systèmes d'exploitation. Le système d'exploitation représente le cœur de son expertise, du noyau à l'interface du logiciel et du hardware, en passant par la mutualisation et le middleware. au-delà des cours sur ces thématiques, les étudiants spécialisés en sécurité participent à un « atelier de sécurité », qui prend la forme d'un cours intensif sur les vulnérabilités de base et les techniques d'exploitation, avec des exercices pour pratiquer l'exploitation ou la participation aux exercices grandeur nature du ComCyber DEFNET.

L'Ensimag (École nationale supérieure d'informatique et de mathématiques appliquées de Grenoble) a pour spécificité d'associer les compétences en mathématiques appliquées et informatique. Des cours y sont dispensés en matière de sécurité, en première, deuxième (Analyse de code pour la sûreté et la sécurité) et troisième année (Sécurité des systèmes d'information, Sécurité et sûreté matérielle, Construction d'infrastructures sécurisées et Sécurité informatique et confidentialité).

L'IMT Nord Europe dispense un master spécialisé en ingénierie de la cybersécurité. Formation qui bénéficie du label SecNumedu de l'ANSSI. Sur les 45 crédits ECTS, 2 portent sur les « systèmes d'exploitation /Unix » et « cloud computing et sécurité du cloud ».

On observe une certaine dynamique des acteurs publics en matière de cybersécurité. Et si la cybersécurité s'avère un sujet relativement ancien, ainsi qu'en atteste le Livre blanc défense de 2008[18], les choses évoluent rapidement. Se manifestent des attaques d'une puissance démultipliée, mobilisant des nouvelles technologies de pointe, très chères mais très rentables. On peut noter le développement de l'OSINT (open source intelligence) et son emploi dans les fonctions de sécurité nationale, d'application de la loi et de veille économique. En face, les AMG dépensent des sommes croissantes pour tenter de garantir la sécurité de leurs systèmes et celle de leurs clients, jusqu'à 3 milliards d'euros en 2021. Cette même année Google Cloud a fait l'acquisition de Mandiant pour 5,4 milliards de dollars. Mandiant, qui a longtemps fait partie des prestataires privilégiés du gouvernement américain, fournit des renseignements sur les menaces. Google, qui dispose déjà de Chronicle et de Security Command Center, va par cette acquisition égaler Microsoft en matière de services de cloud. La concurrence par la cybersécurité fait rage entre les 3 principaux Amazon WS, Microsoft Azure et Google Cloud.

3 / LA CYBERSÉCURITÉ DU CLOUD

Chaque catégorie de services du cloud renvoie à un contexte de sécurité spécifique, et à des problématiques de sécurité différentes. Dans les datacenters, l'environnement physique (situation, organisation, alimentation flux, etc.) représente un point d'attention majeur. La sécurité de l'IaaS renvoie principalement à une problématique de hardware. Dans le cas de la PaaS, le sujet sécurité majuscule concerne la maîtrise de l'environnement d'exécution et de la chaine logistique du logiciel. Pour le SaaS, il s'agit des services et de sécurité logicielle.

3.1 / SELON LES SERVICES DE CLOUD, DES PROBLÉMATIQUES DE CYBERSÉCURITÉ DIVERSES

L'enjeu de souveraineté numérique peut d'abord s'envisager comme un enjeu de localisation des ressources informatiques (et des données) : localisation des serveurs et services cloud et/ou des datacenters. En France, se développent plusieurs offres de clouds « souverains de confiance » : BLEU réunit Orange, Cap Gemini et Microsoft ; S3NS, Google Cloud et Thales ; NUMSPOT, Docapost, Dassault Systèmes, Bouygues et la CDC.

18 Cf. Livre blanc « Défense et sécurité nationale », Ed. Odile Jacob, Juin 2008, https://www.diplomatie.gouv.fr/IMG/pdf/0000.pdf

Figure 4 – Offre sur le site internet de S3NS (Google Cloud et Thales), mai 2023

Pour ce qui concerne la « maîtrise de l'environnement physique », la souveraineté concerne les conditions de cybersécurité de la configuration, de l'architecture des bâtiments et des équipements des datacenters. L'accident survenu dans l'un des datacenters d'un fournisseur de service de cloud reconnu a favorisé la prise de conscience de l'importance de la vulnérabilité physique[19].

On peut distinguer deux approches de la souveraineté numérique, ainsi qu'en ont attesté les discussions pendant la phase de préfiguration de GAIA-X et lors de son lancement. La souveraineté peut être approchée principalement comme une question de localisation, au sens géographique, des équipements et données. Elle peut alternativement être considérée comme une question d'adhésion, de respect à des règles, qui elles-mêmes traduisent des valeurs. Compte tenu de l'extraterritorialité du régime juridique américain, la localisation importe peu en réalité : à partir du moment où une entreprise américaine, ou une entreprise employant un salarié américain, ou ayant une activité économique sur le territoire américain, est impliquée dans l'usage des données, l'Etat américain peut, sous conditions, obtenir l'accès (cf. Clarifying Lawful Overseas Use of Data Act ou C.L.O.U.D. Act, 2018). L'approche de la souveraineté numérique par la localisation s'avère mise en échec. Réciproquement, il convient de considérer que les normes de cybersécurité et de circulation des données emportent l'implantation.

La qualité de service d'un datacenter dépend de ses caractéristiques physiques en premier lieu, puis de son système énergétique, de la robustesse de ses protections matérielles informationnelles et humaines, de sa surface, de sa configuration spatiale, de son hardware, de la chaîne d'exécution et de développement logiciel, et de son Plan de Continuité en cas de crise.

Pour la maîtrise de l'environnement d'exécution et de la chaine logistique du logiciel, à l'interface entre l'Iaas et le PaaS, se trouvent l'usage et l'intérêt du conteneur. Il s'agit d'une enveloppe virtuelle qui permet de distribuer une application avec tous les éléments dont elle a besoin pour fonctionner : fichiers source, environnement d'exécution, librairies, outils et fichiers. Eléments assemblés de manière cohérente et prêts à être déployés sur un serveur par son système d'exploitation.

A la différence de la virtualisation de serveurs et de l'usage d'une machine virtuelle, le conteneur n'intègre pas de noyau (ou kernel), il utilise directement celui de l'ordinateur sur lequel il est déployé. Par conséquent, en termes de sécurité, le maillon faible est la vulnérabilité du kernel lui-même. Le choix entre virtualisation et usage de conteneur renvoie ainsi au dilemme entre mutualisation (virtualisation) et sécurité[20].

3.2 / DU RÔLE DU MICROPROCESSEUR EN MATIÈRE DE CYBERSÉCURITÉ [21]

Dans le monde de la cybersécurité du cloud, le caractère décisif du microprocesseur ne va pas encore de soi. Aussi, il y a lieu de rappeler plusieurs prérequis essentiels.

En premier lieu, il convient de s'entendre sur ce recouvre exactement la cybersécurité. Il est ainsi bon de se souvenir de l'adage « sans menace, nul besoin de sécurité ». Ainsi, les solutions et architectures de cybersécurité répondent à la nature des menaces. Les solutions de cybersécurité dépendent des cibles explicites : le fabricant, les règlementations, l'utilisateur final, etc.

En second lieu, les menaces varient selon le domaine d'applications : à telle menace, tel type de sécurité et de défense. Selon les marchés, les menaces, les attaques et les solutions de sécurité diffèrent. À titre d'exemple, prenons les deux domaines polaires sui-

19 Cf. l'incendie du site d'OVH de Strasbourg le 11 mars 2021.

20 Le kernel Linux est connu pour sa faille 'dirty pipe' (Classée comme CVE-2022-0847 et un score de sévérité CVSS de 7.8, sur une échelle qui en compte 10). *Dirty pipe* se traduit par « une élévation de privilèges : les processus non privilégiés peuvent injecter du code dans les processus racines ». La faiblesse se situe dans la façon de gérer les pipelines, mécanismes de communication inter-processus unidirectionnel.

21 Ces développements s'inspirent largement des interventions de M. Thierry LELEGARD, Chef de la sécurité de la plateforme, chez SiPEARL, au cours des réunions du GT. Les erreurs, simplifications ou émissions éventuelles sont uniquement imputables à l'auteur.

vants : le cloud dans des centres de données d'un côté, les systèmes embarqués et les IoT de l'autre. Dans le premier cas, il s'agit de multi-clients qui nécessitent une isolation horizontale. L'environnement est bruyant et imprédictible, avec des centaines de milliers de serveurs qui hébergent chacun des centaines de machines virtuelles. Ils sont soumis à des menaces logiques : malware, infections, solutions de cyber sécurité globales, avec ancrage hardware éventuel. Le système est statique, l'environnement stable. Alors, qu'il s'agisse de systèmes très isolés comme les HPC ou des systèmes potentiellement exposés comme le *edge*, les attaques physiques restent peu probables. Sont concernés des systèmes génériques comme tous types d'OS, d'utilisateurs, d'activités. De plus, l'environnement réseau est ouvert : tous types d'applications et de protocoles réseaux et donc tous types de malwares et autres virus présent sur internet. Les attaques logiques sont quotidiennes et le Système sur une puce (System on a Chip, ou SoC) est de fait « immergé » dans le système.

Le second cas concerne les systèmes embarqués et l'internet des objets (IoT) qui sont gérés par un dépositaire de sécurité unique, « maitre des secrets » et procèdent d'une mono-activité. Ils nécessitent une défense verticale en profondeur. L'environnement est prédictible, l'accès physique aisé, les utilisateurs et les attaquants sont d'ailleurs souvent les mêmes. De manière générale, c'est donc à des menaces physiques que sont exposés ces systèmes tels les injections de fautes, les attaques en *side-channel,* le reverse-engineering du hardware.

Retenons donc qu'à la variété des menaces qui dépendent des domaines d'application –les deux castypes sont les serveurs d'un côté et les systèmes embarqués de l'autre–, doivent répondre des solutions de cybersécurité pertinentes et cohérentes. Garantir la cybersécurité du cloud implique donc aussi bien une dimension logicielle qu'une dimension matérielle.

Une approche pratique et conceptuellement raisonnée de la cybersécurité du cloud implique de reconnaître deux notions fondamentales. D'une part, la sécurité doit se concevoir comme une chaîne ; d'autre part, la sécurité est une stratégie systémique.

La sécurité s'inscrit dans une chaine continue. La sécurité du système entier dépend de celle du maillon le plus faible de la chaine. La sécurité impliquant tous les éléments du système, identifier la valeur ajoutée du processeur et sa place au sein de la chaine de sécurité est clé. Cette lecture s'applique de manière pertinente au cloud, monde où le processeur n'est qu'un élément parmi d'autres. Ceci contraste nettement avec le monde de l'embarqué (de l'IoT) où le SoC est le principal élément du système, voire le système à lui tout seul.

Comme la sécurité est une programmation systémique, il convient d'adopter une approche globale qui combine 'top-down' et 'bottom-up'. La *security-by-design* relève de l'approche top-down qui consiste à *prévenir* les intrusions de sécurité dès la conception du système. Les domaines de sécurité et leur isolation sont définis dès l'origine : confidentialité, intégrité, authentification, chaine de confiance, etc. La sécurité-by-design consiste en la segmentation de l'exécution et des accès mémoire. Le modèle de sécurité pour les serveurs défini par ARM[22] est le Confidential Compute Architecture (CCA)[23]. Le CCA comprend le concept de *realms* (royaumes) qui dupliquent certaines zones fonctionnelles de l'architecture normale *via* quatre niveaux d'exception (utilisateur, noyau/Kernel, hyperviseur et moniteur). Par l'attaque logique, l'intrus est déjà à l'intérieur de la machine.

La sécurité dite défensive relève de l'approche bottom-up. Elle consiste à *répondre* aux intrusions de sécurité. Il y a toujours des bugs, que les hackers transforment en vulnérabilités et en intrusions. Des cyber-attaques finissent toujours par se produire, il s'agit de les comprendre et de fournir des capacités de réaction et de réponse. Dans cette approche, la valeur ajoutée du processeur provient de son rôle dans le contrôle de l'exécution, dans la détection et le contre d'activités suspectes. Ces attaques en injection de code et infection de malware font partie de ces activités suspectes que le processeur peut détecter et bloquer au plus tôt. Ces attaques depuis un logiciel qui s'exécute sur le processeur sont les principaux vecteurs des cyber attaques et ransomwares qui mettent à mal hôpitaux, institutions publiques et privées.

22 L'entreprise britannique ARM Ltd. développe des processeurs d'architecture 32 bits et d'architecture 64 bits. Mais elle ne les fabrique ni ne les vend sous forme de circuits intégrés : elle vend les licences de ses processeurs à des fabricants (qui les gravent dans le silicium). Presque tous les fondeurs de puces proposent des architectures ARM.

23 Plus récent et moins connu que la TrustZone pour les systèmes embarqués.

04

La chaîne de la cybersécurité du cloud, du système d'exploitation au microprocesseur

Les couches basses d'intérêt comprennent le middleware, le système d'exploitation, l'architecture du système et le microprocesseur. Si l'on vise la souveraineté, le microprocesseur constitue un élément clé au sein d'une pile qui comprend aussi le système d'exploitation, les compilateurs et l'architecture. Les défis des couches basses portent sur ces deux maillons fondamentaux liés que sont le système d'exploitation – le logiciel qui permet aux programmes de fonctionner – et le microprocesseur, a fortiori lorsqu'il s'agit de systèmes informatiques en nuage. Par conséquent, la quête d'un système européen de cloud alternatif passe par des efforts d'ampleur sur ces deux maillons complémentaires. Le point clé est le suivant : sans enveloppe logicielle et architecturale adéquate, un nouveau microprocesseur souverain peinera à s'installer largement dans les serveurs du cloud. Une approche intégrée de la souveraineté du cloud se décline donc aux échelles fondamentales du microprocesseur, et d'une conception renouvelée de son rôle en matière de cybersécurité, et des éléments logiciels profonds.

1 / COMPLÉMENTARITÉS TECHNOLOGIQUES ENTRE LA PUCE ET LE CLOUD OPEN SOURCE EUROPÉENS

Créée en juin 2019, SiPearl vise à concrétiser le projet de l'Initiative pour un Processeur Européen (EPI) : favoriser le déploiement de technologies microprocesseur haute performance, basse consommation et sécurité sans faille. L'entreprise bénéficie du soutien du Conseil européen de l'innovation[24] pour développer et mettre sur le marché le microprocesseur européen qui accompagnera les supercalculateurs européens vers la puissance exascale. Elle travaille en étroite collaboration avec ses 27 partenaires d'EPI. Le consortium regroupe des acteurs de la communauté scientifique et des centres de supercalcul, des grands de l'informatique, ainsi que des futurs clients et utilisateurs finaux, de l'électronique et de l'automobile par exemple.

En 2018, l'Union Européenne s'est lancée dans la course au supercalculateur exoflopique, en installant EuroHPC JU, l'entreprise commune européenne de calcul à haute performance. Au sein de cette entreprise commune, SiPearl conçoit le microprocesseur Rhea1, pièce maîtresse des futurs supercalculateurs exascales européens. Depuis 2022, EuroHPC s'est engagée dans une nouvelle phase de développement du microprocesseur européen ; la puce Rhea va être améliorée, garantissant son meilleur emploi au sein du futur supercalculateur Européen (augmentation du nombre de cœurs, accroissement de la bande passante mémoire, ajout de l'accélération, etc.).

Une étape importante dans le développement de SiPearl au profit du supercalculateur européen a été franchie début octobre 2023, la société ayant remporté le contrat fondateur pour équiper JUPITER, le premier supercalculateur exascale européen[25].

A terme, les puces de SiPearl, souveraines et dotées de propriétés avancées en termes de consommation énergétique et de cybersécurité, seront destinées à équiper des serveurs cloud.

Ainsi, depuis janvier 2023, SiPearl participe activement au projet européen AERO (Accelerated EuRopean clOud)[26], dont la mission consiste à assurer la possibilité du déploiement de la future infrastructure de clouds hétérogènes de l'UE. Projet clé, présenté comme le « complément indispensable à l'EPI », qui doit structurer et amplifier l'écosystème open source favorisant l'intégration du processeur dans le cloud. AERO améliorera les performances et l'efficacité en matière d'énergie et de sécurité du processeur au sein d'un écosystème adapté. Cela devrait encourager la migration des utilisateurs vers la plateforme, l'infrastructure et l'écosystème clouds européens.

24 SiPearl a bénéficié d'une subvention de 2,5 millions d'euros et d'un investissement en fonds propres de 15 millions d'euros.

25 Le supercalculateur d'EuroHPC sera installé sur le campus du centre de recherche de Jülich en Rhénanie du Nord-Westphalie. Il sera construit par un consortium composé d'Eviden, la branche d'activité du groupe Atos leader dans l'informatique avancée, et de ParTec, la société allemande de supercalcul modulaire.

26 Projet d'une durée de 3 ans, débuté en janvier 2023.

2 / ET COMPLÉMENTARITÉ VIS-À-VIS DES COUCHES BASSES DE L'ENVIRONNEMENT LOGICIEL

Comme nous l'avons souligné, c'est bien par une stratégie d'échappement à « l'enfermement propriétaire », via *l'open source*, qu'il redeviendra possible aux entreprises établies en Europe d'adopter ces technologies (européennes) de cloud avancées (cf. chapitre 2). Il s'agit d'une voie prioritaire pour renforcer la souveraineté et la compétitivité de l'Europe dans le numérique.

Le frein au déploiement à grande échelle d'un nouveau microprocesseur est d'ordre économique. L'usage d'une puce est optimisé au regard de la pile logicielle environnante. Or, il est beaucoup trop coûteux pour une entreprise de microprocesseur de développer aussi le système d'exploitation ajusté à sa puce. C'est pourtant à cette condition que se gagne la souveraineté numérique, en introduisant de l'hétérogénéité au sein d'un système intégré monopolistique. Linux, en développant en open source son propre système d'exploitation a autorisé des innovations y compris à l'échelle du hardware (cf. Chapitre 2, Point 3.).

Ainsi, au début de sa montée en puissance, l'entreprise BULL ne disposait pas de la taille suffisante pour porter la pile logicielle d'accueil sur ses propres serveurs. Le prix de développement d'un tel environnement, nécessaire à la vente des serveurs, n'était pas atteignable par BULL seul. L'irruption de Linux a brisé la logique propriétaire intégrée des serveurs IBM en fournissant un standard à tous les services qui porteraient Linux (cf. Chapitre 2, Point 3.). Ce faisant, le coût de l'innovation a drastiquement diminué. A l'époque, offrir un tel service nécessitait un investissement de 1 milliard de dollars auquel s'ajoutait le coût de la R&D. Linux a réduit fortement les coûts logiciels, permettant ainsi aux nouveaux venus d'introduire des innovations hardware pour un coût acceptable (200 millions au lieu d'un milliard)[27].

Le caractère propriétaire des systèmes Microsoft se manifeste aujourd'hui encore dans les microprocesseurs qui disposent de clés de codage destinés à fonctionner avec des logiciels Microsoft.

Pour avoir une chance de regagner en souveraineté dans le cloud, le premier jalon consiste à parvenir à instaurer un « Linux de l'IaaS » (équivalent du système d'exploitation du Cloud). Cette base logicielle standard (ouverte) autorisera le développement d'innovations hardware comme un microprocesseur souverain, incarné par celui de SiPearl. A défaut d'un standard ouvert d'IaaS, les coûts de développement de l'environnement logiciel nécessaire au meilleur fonctionnement du microprocesseur s'avéreraient rédhibitoires.

A l'échelle d'un fournisseur de services de cloud européen, échapper à l'enfermement propriétaire passera par la reprise en main d'outils de management des services de cloud spécifiques.

3 / RETOUR SUR LE MICROPROCESSEUR, MAILLON FORT DE LA CHAÎNE DE CYBERSÉCURITÉ DU CLOUD

Pour que le microprocesseur – ici souverain – fasse prévaloir sa valeur ajoutée sécuritaire au sein de la chaîne de cybersécurité du cloud, il convient de changer de point de vue sur la source de la menace. Traditionnellement, l'attention des équipes de cybersécurité se focalise sur la détection de la « charge utile » malveillante. Les techniques classiques appliquées lors du processus d'attaque entendent la neutraliser : sécurité paramétrique à l'entrée (firewall par exemple), réseau interne de détection, sécurité comportementale (intégrité des logiciels par exemple), sécurité applicative (résistance du code en présence d'intrusions). Le moment clé où le processeur est sollicité, celui de l'exécution du programme, n'est généralement pas considéré. Tout se passe comme si l'exécution était au mieux un impondérable au pire inexistante, une boîte noire.

Dans une approche souveraine de la cybersécurité du cloud où le système d'exploitation échappe à l'enfermement propriétaire, grâce à des qualités avancées, et où le processeur représente lui aussi un garant d'autonomie, le focus se déplace de la « charge utile » vers le « vecteur ». Dans ce nouveau schéma de cybersécurité, la fonction d'empêcher les exécutions non standards et donc d'empêcher les intrusions revient alors au processeur. Les microprocesseurs sécurisés, et conçus comme tels, comme ceux de SiPearl, fournissent une sécurité matérielle qui protège l'entièreté de la plateforme. Et ce, jusqu'au niveau du microgiciel chargé du démarrage. Si ce dernier est 'vérolé', son accès même est refusé. Dans un tel modèle, chaque couche de l'infrastructure de sécurité complète la suivante.

L'approche de SiPearl en matière de cybersécurité à l'échelle du microprocesseur s'inscrit dans un courant de travaux de recherche appliquée, auxquels contribue ARM. Ainsi en va-t-il du projet « CHERI », pour Capability Hardware Enhanced RISC Instruction. CHERI a débuté en tant qu'effort de recherche conjoint de SRI International et de l'Université de Cambridge en 2010, financé par le programme DARPA Clean-slate design of Resilient, Adaptive and Secure Hosts (CRASH). Le programme engageait les participants à repenser la pile matérielle/logicielle afin d'améliorer la sécurité. Et, en janvier

27 La valeur ajoutée de la machine résulte de son architecture classique dite de 'Von Neumann', architecture qui repose sur la 'mutualisation de la mémoire' comme lieu de stockage unique des instructions et des données demandées ou produites par le calcul. Cela implique que chaque microprocesseur participe de cette structure. BULL avait mis au point un algorithme de cohérence de cache – garantissant aux processeurs une vue cohérente de la mémoire - plus efficace que les autres. BULL a donc bénéficié d'un OS libre (Linux) qui lui a permis de développer un système microprocesseurs à la base de ses supercalculateurs.

2022, ARM a annoncé que la première puce prenant en charge l'architecture prototype Morello[28] était désormais disponible sur une série limitée de cartes de démonstrations. Elles ont été expédiées aux partenaires de l'industrie pour essais[29]. Morello est la première implémentation haute performance des extensions CHERI.

28 Morello est un projet de recherche qui vise à radicalement changer la façon dont sont conçus et programmés les processeurs à l'avenir afin d'améliorer la sécurité intégrée. Il est à l'origine financé par le programme Digital Security by Design (DSbD) du gouvernement britannique, Industrial Strategy Challenge Fund (ISCF) et dirigé par ARM. Cf. https://www.arm.com/architecture/cpu/morello

29 Cf. https://www.thegoodpenguin.co.uk/blog/introducing-arm-morello-cheri-architecture/

05

Pistes d'action, réflexions conclusives

Décliner de manière pédagogique – à un niveau permettant l'action – une problématique d'importance capitale, celle de l'autonomie stratégique ou de la souveraineté numérique, constitue la raison d'être du groupe de travail « Pour une politique industrielle du numérique ».

La variété des participants, publics et privés, d'un haut niveau de maîtrise technique, favorise en premier lieu l'établissement d'un diagnostic partagé ; il encourage le développement d'une approche ciblée, différenciante, du problème. Ce diagnostic partagé ne procède pas uniquement du travail propre du groupe de l'année mais s'inscrit dans la lignée des rapports précédents. Ainsi en va-t-il de l'identification du caractère structurant de la plateformisation numérique, en particulier pour l'industrie. Cette composante infrastructurelle, qui procède de *clouds* hétérogènes interdépendants, fournit le cadre dynamique de notre approche. La plateformisation numérique des entreprises industrielles européennes, grâce aux compétences et technologiques européennes de pointe, est l'horizon désirable d'une souveraineté solide.

En s'attachant aux couches basses du cloud, notre approche suggère une façon de sortir par le haut de l'« enfermement propriétaire » subi par les entreprises européennes. Trois entreprises multinationales américaines détiennent les trois quarts du marché du cloud, selon un schéma semblable d'interdépendances de technologies propriétaires sur la totalité des couches. A l'instar de ce qui s'est produit pour la fin de la domination des systèmes mainframes d'IBM, il faut à nouveau, par la mobilisation nécessaire, faire prévaloir la « dépropriétarisation ». En commençant là où c'est logiquement possible et techniquement pertinent, i.e. à l'échelle du système d'exploitation et du composant fondamental des serveurs qu'est le microprocesseur.

Nous proposons donc de mettre en place les conditions d'une alternative européenne open source aux systèmes d'exploitation du cloud des AMG (Amazon Web Services, Microsoft Azure, Google Cloud). L'initiative Gaia-X va dans le bon sens. Elle doit être accompagnée pour aller au-delà d'assurer l'interopérabilité de tous les fournisseurs de services de cloud. Ainsi, il convient que les systèmes d'exploitation et la capacité de virtualisation disposent toutes deux d'offres open source. De manière complémentaire, doit être soutenu et promu l'emploi du microprocesseur européen dans les serveurs des fournisseurs de services de cloud européens. Ce dernier doit être envisagé comme opérateur central de la chaîne de cybersécurité. Le succès de la puce européenne de SiPearl – son déploiement à grande échelle dans les serveurs des fournisseurs de services de cloud – constitue donc un jalon important.

En ces deux domaines, nous suggérons de redoubler d'efforts, avec nos partenaires européens, pour mettre en œuvre une plateforme européenne d'infrastructure clouds open source. Des projets et programmes publics (organismes de recherche français et des autres Etats membres) et entreprises et consortia sont lancés qui, faute de mobilisation suffisante, risquent de manquer d'ambition. Les vecteurs d'intérêt de ces efforts public-privé seraient très utilement orientés par une commande publique de services de clouds dont les serveurs seraient équipés de microprocesseurs européens sécurisés, et qui fonctionnent sur une plateforme IaaS open source. Les besoins sont immenses, en France, comme ailleurs en Europe, dans de nombreux domaines où les services publics jouent un rôle majeur comme la santé, la recherche, l'éducation, les transports, l'énergie pour ne citer qu'eux.

Enfin, face aux effets délétères de l'enfermement propriétaire, la réponse passe aussi par mobilisation autour des enjeux de souveraineté dans les établissements d'enseignement supérieur et de recherche du numérique. Beaucoup plus de formations doivent porter sur les couches basses comme sièges de la cybersécurité et de la souveraineté. La surspécialisation sur les développements dans les couches logicielles hautes, y compris en matière de cybersécurité, a tendance à contribuer au refermement du piège propriétaire. Au-delà des efforts importants faits dans le cadre de France 2030, l'Etat serait avisé d'accompagner, par des financements spécifiques (complémentaires aux Compétences et Métiers d'Avenir de France 2030), l'évolution des formations secondaires et supérieures en France vers des enseignements ciblés en matière de systèmes d'exploitation.

33, RUE RENNEQUIN - 75017 PARIS
TÉL. : 01 55 35 25 50
WWW.ANRT.ASSO.FR