Digital sovereignty: regaining control in France and Europe

SKILLS, CYBERSECURITY AND LOWER CLOUD LAYERS

JANUARY / 2024

Synthesis report by the ANRT FutuRIS 2023 working group

Working group chaired by Gérard Roucairol, Honorary President of the French Academy of Technologies
Author: Pierre Bitard
Director of the publication: Clarisse Angelier

This work received financial support from FutuRIS subscribers:

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

The content is the sole responsibility of ANRT as author and not of the institutions that support it.

List of experts who participated in the working group

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

CONTENTS

INTRODUCTION

The digital platformization of enterprises involves using communicating clouds, which constitute the infrastructure. The quality of this digital infrastructure depends on the scientific and ICT skills of companies and administrations, including public laboratories and universities.

The key cloud computing skills concern operating systems. Cloud security also involves the hardware domain, in particular the microprocessor, which carries out instructions and processes program data.

For France and Europe, the main opportunity to regain digital sovereignty involves attaining the autonomy of operating systems and microprocessors. Cybersecurity sovereignty would give European industrial companies a real opportunity to appropriate the uses of the cloud.

European companies will not obtain genuine strategic autonomy in industrial data and services without controlling the cloud security chain. And the security chain of the industrial cloud cannot be controlled without appropriating the lower layers of the cloud, including operating systems and microprocessors[1]. In this area, the key challenge for the next few years is to train sufficient people with quality core cloud computing skills. This concerns digital platformization, meaning we need to join the race fast.

Most of the industrial cloud clientele in France and globally is in the hands of three large US companies, Amazon, Microsoft and Google (GAM). Nevertheless, the appetite for academic training on these "lower layers" to meet the challenge of regaining sovereignty appears insufficient in numerous regards. In the France 2030 programme, the national cybersecurity acceleration strategy aims to create 37,000 jobs by 2025 (doubling current numbers). Investments in training on the lower cloud layers need to be significantly increased if France, within Europe, wants to regain control of the industrial cloud. The aim being to impose alternative European solutions for a secure cloud.

This report is divided into five chapters. The first chapter describes the importance of the cloud as an infrastructure for circulating industrial data in France and Europe. At present, the volume and quality of these data are still relatively inconsequential in France, which implies that adopting a sovereignty path is in fact an urgent opportunity. The second chapter stipulates the need for an industrial cloud policy aimed at supporting and encouraging both supply, generally already the case, and demand. Once this complementary choice is made, the next step involves identifying, characterizing and devising a possible pathway towards a desirable level of sovereignty. The description and analysis of a key historic reference – the end of large proprietary systems – proves useful here. Digital sovereignty takes hold in the cloud's deep layers, as shown by the analysis in chapter 3, which introduces the notion of the cloud security chain. Chapter 4 sets out the necessary role of the microprocessor in the cybersecurity chain and its complementarity with a sovereign open source operating system. The final chapter summarizes the diagnosis and suggests concrete courses of action.

[1] Components of the 'lower layers' that are the object of the developments that follow.

01 The cloud, infrastructure for circulating industrial data

The data that are characteristic of industrial production systems' functioning and performance, including conception and logistics, are vital. They are also increasingly mobilized systematically by companies as sources of value creation. As our previous studies have illustrated[2], data from different sources gain value when they are combined for the benefit of a job, solution or innovation. Processing transforms them from information into knowledge. Only knowledge that can be acted on with a defined goal gains value.

1 / THE INDUSTRIAL CLOUD

The cloud is a technical system for storing, processing and pooling digital data through which computing resources can be externally managed. The 'cloud service provider' supplies paying access to hardware and/or software capacities to clients in shared mode. Given the growing production of data and the new interest in exploiting them massively, at a pace that can be difficult to anticipate, industrial companies are increasingly turning towards these external clouds.

Manufacturing companies today are equipped with their own server networks frequently linked up to cloud services (i.e. an external commercial offer). To do so, they must call on an infrastructure operating several clouds, which are heterogeneous because they do not all correspond to the same technical prerequisites, standards and performances. Contractors and sub-contractors have no particular reason to use the same cloud provider, and it is even common for a single company to use several cloud service providers (called multiclouds). Thanks to interconnecting clouds, companies can combine data sets from different origins and analyse them, or solicit complementary services from different providers. In this way, everyone follows their own interests, which are not necessarily in competition with those of its partners.

As companies evolve towards smart manufacturing[3], increasing quantities of industrial devices and equipment are connected (IoT), and the volume of data obtained during a product's different life cycle phases is growing. New applications and new services involve analysing massive quantities of data.

In practice, the cloud infrastructure is composite and constantly evolving. It is undeniably "(...) the basis of a systemic transformation of the economic and societal space[4]" in which a very wide variety of economic activities take the form of online services, i.e. XaaS (anything as a service). For us, it constitutes the basis of the digital platformization of socioeconomic activities.

2 / USING THE CLOUD IN COMPANIES

At international scale, enterprises are increasingly using the cloud infrastructure[5]. Almost one-third (30%) of companies declared that 41% to 60% of their data were stored in an external cloud, and 22% indicated that more than 60% of their data were. Many companies use several cloud service providers, referred to as a 'multicloud strategy'.

Companies frequently employ several infrastructure as a service (IaaS) providers. In 2021-2022, 48% of companies questioned declared that they used AWS as their IaaS provider, followed by Microsoft Azure at 47%. In 2020-2021, 53% of companies declared that AWS was their IaaS provider, while 41% used Microsoft Azure, with a considerable overlapping between Google Cloud, IBM Cloud, Oracle and Alibaba. The use of SaaS is more diverse. 34% use at least 50 SaaS applications and 17% use 100 or more SaaS applications.

[2] Cf. *"5G in data value chains – The technological and industrial challenge ahead of us"*, Les cahiers de FutuRIS, ANRT, March 2021 ; *"Data price and value in digital platformization – Key pointers for business-to-business relations"*, Les Cahiers de FutuRIS, ANRT, October 2019.

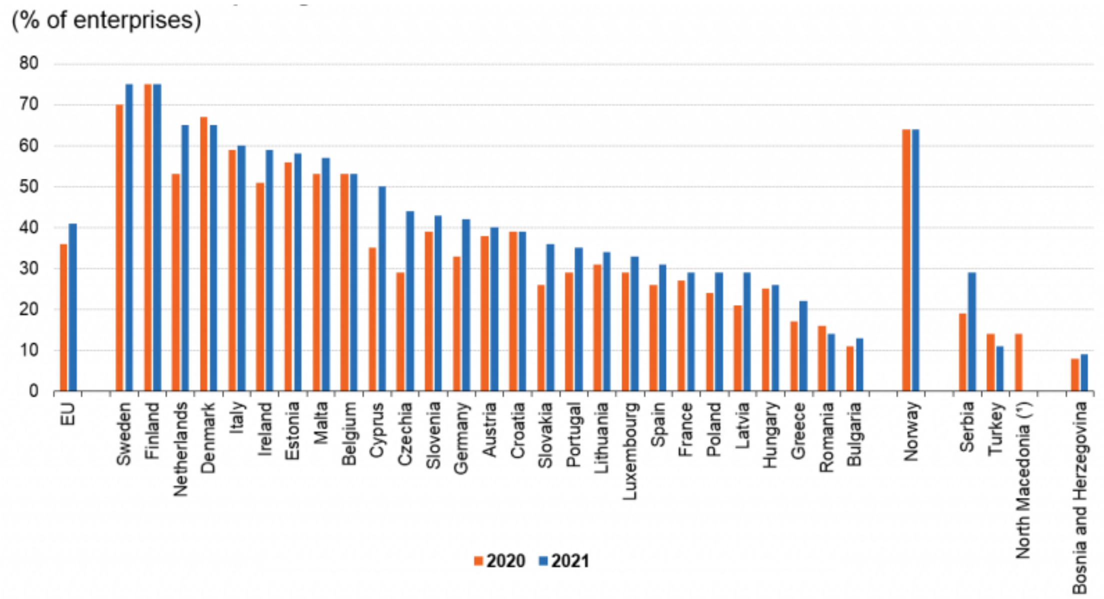
[3] Cf. *"The move to smart manufacturing. Proposal for a national plan"*, Les cahiers de FutuRIS, ANRT, May 2022.

[4] As written by Gérard Roucairol in *"Développer l'infrastructure de la société numérique. Réseaux de clouds et circulation vertueuse des données"* [Developing the infrastructure of digital society. Multicloud networks and virtuous circulation of data – not translated], French Academy of Technologies, 2022, unpublished.

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

Companies located in France are among those with the lowest cloud service use rates in Europe. With a little under 30% of cloud use in 2021, French companies rank among the lowest users in the European Union, coming between Spain and Poland, compared to the European average of 41%.

Figure 1 - Use of cloud computing services in Europe in 2020 and 2021



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

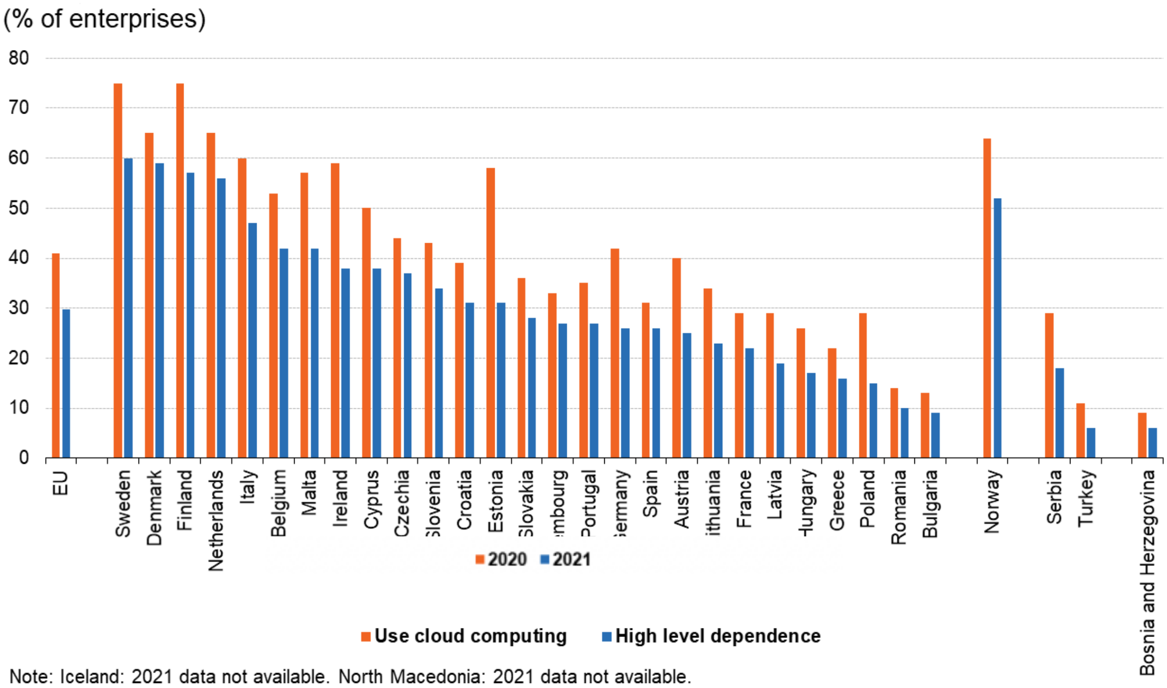
The same Eurostat survey illustrates the intensity of cloud use by companies, known as 'dependence on cloud computing services'[6]. The degree of dependence is related to the level of sophistication of the services used: the more sophisticated services the company uses, the greater the dependence. The types of service are split into three levels: basic, intermediate and sophisticated cloud services.

Companies using basic cloud services are those that use at least one of the following: e-mail as a cloud service, office software as a cloud service, storage of files or computing power to run the enterprise's own software, and do not use any other of the services covered. Companies that use intermediate services purchase at least one of the following: finance or accounting software application as a cloud service, ERP a software application as a cloud or CRM software application as a cloud service, but none of the sophisticated services. Companies that use sophisticated cloud services include those that purchase at least one of the following: security software applications, hosting of company databases or computing platform providing a hosted environment for developing, testing or deploying applications.

Only about one French company in five uses the most sophisticated cloud services (including cybersecurity software). They are therefore among the least cloud-dependent in the EU (ranking 21st).

[6] The survey also indicates that on average in Europe use of the cloud varies depending on company size: 38% in small firms, 53% in medium-sized enterprises and 72% in large companies.

Figure 2 - Use of cloud computing services and high-level dependence on the 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

Apart from this European survey, which also provides points for comparison, both the level and degree of sophistication of cloud computing use in industrial companies in France are insufficiently documented. Very few academic studies contribute to the public debate and inform public decision-makers. In fact, they have become even rarer over the last five years. Nevertheless, several government plans attempt to promote and reinforce the French cloud ecosystem and its components.

In addition, as the Eurostat survey shows, cloud security is considered to be a ‘very sophisticated service’, involving a high level of dependence.

The moment seems particularly ripe for France to make the right move by taking strong action to encourage the adoption of secure, sovereign cloud service solutions.

02 Moving towards an industrial policy for the cloud

When industrial policy sets out to make big changes and promotes a paradigm shift (e.g. the switch from combustion engines to electric vehicles), it needs to be approached 'from both ends', i.e. supply and demand[7]. This is typically the case in terms of a cloud industrial policy.

1 / COMPREHENSIVE INDUSTRIAL POLICY

Public policy mobilizes a range of instruments to support companies in a sector, in this case cloud service providers, and those contributing technologies or products and services to the sector. What are the ways to foster their development and growth so that they can prosper in the country (turnover, jobs) and beyond? The answer is, through a classic 'techno-push' policy, which consists in supporting the cloud ecosystem. The latter comprises companies that compete with the dominant cloud service providers and a whole range of enterprises of different sizes, including start-ups, in a position to provide technology bricks, or perhaps services, to national champions. With this approach, national economic sovereignty should 'naturally' result from state action to the benefit of the ecosystem identified.

It can be pertinent and effective for the state to supplement its industrial policy with measures to stimulate demand. In such a case, the public policy will attempt to contribute to the adoption of a new technical system whose advantages are considered desirable for improving national industrial performance. At the same time, it will ensure that the industrial providers of the targeted goods and services – in this case national cloud service providers – are given the opportunity to grow and move upmarket. The choice of instruments for this demand policy, which must crucially complement the supply policy, is not easy. The design phase of the policy requires acquiring an in-depth understanding of user/consumer needs – i.e. of uses – and therefore also of the capacities and performances of the technical system in the state of the art, such as it can be produced by national industrialists. The public powers then set out to develop an infrastructure policy, in the strongest sense. It can be seen as a major investment in framework conditions to the benefit of industrialization. National economic sovereignty springs here from a judicious coming-together of political ambitions and industrial capacities and needs. This form of sovereignty is by no means mechanical, and does not therefore simply result from a state decision. To the point that it begs the question, for both the state and companies, of the level of sovereignty attainable.

For a country like France within the European Union, the path to reach the desired level of sovereignty pertaining to the cloud is a narrow one and will necessarily rely on the judicious combination of industrial policy actions aimed at supply and demand.

2 / TOWARDS A DESIRABLE LEVEL OF SOVEREIGNTY

Companies collect, store and manipulate immense quantities of data. From the company's point of view, data sovereignty[8] consists in being capable of determining the precise conditions according to which, if they want to, other companies can use some of their data: when, how, and perhaps at what price.

Attaining a high level of transparency in the supply chain generates gains that are divided between the actors in the chain; data sharing involves the participation of new companies likely to provide a specialized service on a link of the chain. An example in the automobile industry is companies supplying 3D printing services. Security and confidentiality are preserved thanks to the implementation of tools facilitating the circulation of models of (virtual) parts, for example. With this acceptation of 'data sovereignty' terms, the companies that possess the data can protect those of the users. Sovereignty becomes synonymous with data use that is guaranteed to comply with strictly

[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] Reference to the approach of the International Data Space Association: *"Sharing data while keeping data ownership. The potential of IDS for the data economy"*, White Paper, IDSA, October 2018.

defined protective rules. At the scale of French and European companies, reaching a desired level of sovereignty corresponds to their technical control[9] of their data environment.

The value of data results from their circulation. The European Union constitutes a remarkable global exception in this area: it has established this principle as a source of economic development in a series of laws (GDPR, DMA, DSA and DGA) and coordinated initiatives[10]. The EU's legal system proceeds from these institutions – i.e. the laws and regulations in which these principles and values are embodied – which take on a double role of protecting and encouraging economic initiatives: because rules that are collectively adopted and implemented express the principles on which sovereignty is based. The European legal and regulatory framework creates favourable conditions for the circulation of industrial data.

In terms of digital use (confidentiality, privacy, interoperability, etc.), the US model is fragmented: federal states come under different rules and, in particular, the major companies in the sector – GAM (Amazon, Microsoft, Google) – assert and implement their own rules. This fragmentation of the US digital space is connected with the propensity to position their law at international scale. Through the risks, even threats, that it attaches to the use of data circulating via US actors, the extraterritoriality of US digital law makes up for its lack of intrinsic coherence. It is as if the standards and technologies battle had been won on another field, the law field. The network comprising users of GAM, the companies that dominate the sector, makes up three-quarters of the global cloud market, constituting an arsenal for US sovereignty.

In this context, what is the most strategic avenue for France in order to attain the level of industrial digital sovereignty that it can legitimately aspire to?

3 / PATHWAY TOWARDS THE SOVEREIGNTY LEVEL TARGETED

The history of technology can help to identify a strategy to attain the sovereignty level targeted. A historic parallel can be made with the end of the domination of IBM mainframes and the emergence and spread of Unix between the mid-1970s and the early 1990s. The way the shift took place can usefully guide national and European strategies in order to draw all the benefits to be had from regained sovereignty.

IBM central computers, colloquially known as 'big iron', and generally referred to as 'IBM mainframes', dominated the computer sector from the 1950s to the mid-1970s. The ground-breaking System/360 was the first computer to include hardware dedicated to the use of operating systems, programs and instructions in supervisor mode, and applications, along with integrated memory protection functions. This integrated system therefore comprised a machine equipped with a program that piloted the use of resources and application software. This meant that users were subject to a lock-in effect. Distinct but complementary parts of the system were encapsulated in an inseparable, specific way in the product, making a whole. Technically, users could therefore only buy the components and applications required to use the central computer directly from IBM. Moreover, technical interoperability was not ensured, which was clearly stated in the contractual and guarantee conditions.

This lock-in corresponds to the current cloud and GAM situation. Service offers from Amazon Web Services, Microsoft Azure and Google Cloud vertically integrate de facto all of the layers, which are presented as integrated. All of the services available on the cloud can be carried out with each of the brands: computing, storage, network, database management, data analysis, application services, deployment, system management, etc. Just like for IBM's System/360, once purchased, access to a (virtual) machine comprises a layer of applications of different levels. We can therefore say that cloud computing is the victim of a new ownership lock-in.

Due to their closed nature, in the long term, these proprietary mainframes suffered from their inadequate capacity for innovation. The operating systems ended up on machines that were not powerful enough.

The irruption of the standard UNIX operating system changed the game. UNIX offered interoperable, transparent communication protocols, known as 'open systems'. While UNIX started out as a platform for software developers, the system progressively extended when the operating system (BSD and 'System V(5)'[11]) began to spread around university circles and users started to add their own tools and share them with colleagues. An entire open-source ecosystem then developed following the first sale of a UNIX licence by Bell Labs, in 1975, to the computing department of the University of Illinois. Numerous start-ups adopted and adapted it, until it became the most common system in the 1990s, notably including the free European version, Linux. UNIX contributed to dismantling the ownership of operating systems, computer OEMs, and software developers, etc. Android and MacOS were both developed based on UNIX.

A similar approach should be taken to developing a new European cloud operation system to compete with GAM. Like the UNIX example, a key could be found in IaaS, infrastructure as a service. The end of total dependency on GAM clouds could involve rolling out an 'IaaS Linux': a standard operating system for the cloud developed in open source. European control of this kind of operating system and the associated components is our best chance to regain strategic autonomy and desired innovations.

[9] Both legal and in terms of organization.

[10] Cf. EC, 2020, "Shaping Europe's digital future", Communication, February.

[11] Cf. In the 1980s and early 1990s, UNIX System V and Berkeley Software Distribution (BSD) were the two main version of UNIX, https://en.wikipedia.org/wiki/UNIX_System_V.

03 Deep layers of the cloud: the place for defining digital sovereignty

Cloud security is currently mostly covered by service providers, essentially GAM (Amazon Web Services, Microsoft Azure and Google Cloud). These three are also increasingly systematically the developers and owners of the underlying technologies[12]. This strong technical interdependence creates interference that reinforces the lock-in and constitutes a greater threat for sovereignty.

1 / THE CLOUD CYBERSECURITY CHAIN

The cybersecurity chain is sovereignty's weak link for two reasons, the first being technical and the second economic. Technically, attention focuses on the process (the path taken by the 'viral load' of the attack), yet the solution can be found in the heart of the system (the microprocessor).

The second reason is the fact that the cloud market is an oligopoly made stronger by lock-in effects. Thus, some cloud service providers go so far as to design their own microprocessors[13]. The performance of services rendered by the cloud, whether IaaS, PaaS or SaaS, or a combination, is therefore presented as optimized due to the hardware/software imbrication specific to GAM, selling the services[14].

This new situation, where cybersecurity is encapsulated in the operating systems and service provider offers, is part of the strategy of the dominant players. The oligopoly in place benefits from the situation, while emerging companies proposing innovative solutions on one of the segments of the numerous markets involved fight against it. Numerous barriers to entry result from this situation on the many niches and market segments that the cloud service chain comprises, including security.

Students in France and Europe know that obtaining cybersecurity certification from GAM is likely to guarantee them a job. Although basic training on low layers counts, obtaining employment in one of these companies 'only' requires the right certification. The current shortage of human resources specialized in cybersecurity is met by growing demand.

Along with the operating system, the processor is a key link in the cybersecurity chain (see above) and should not be the source of a risk of breach. A European company has designed and is currently developing a processor that intends to provide greater security than what can be attained using standard cloud processors: SiPearl. A European ecosystem needs to be set up around SiPearl and several other processors to offer training on designing and producing microprocessors. One of the main global companies in the sector is ASML, in the Netherlands, which manufactures machines making microchips from layered silicon wafers, the raw material for microprocessor producers.

The cloud's architecture results from modular developments based on microservices[15]. The capacity of France to provide training on cybersecurity to deal with this problem should be questioned. As a reminder, companies located in France are among the lowest users of cloud services in Europe (one of the bottom 7 European countries, at the same level as Spain and Latvia).

[12] In doing so, they directly compete with cloud technology providers like Intel and AMD.

[13] In July 2022, Google Cloud announced that it had started to adopt computer chips based on ARM technology. While Amazon (and Alibaba) design their own chips based on ARM and have them made by chip manufacturers, Google has turned to the Altra chips developed by Ampere Computing, an American fabless company that designs cloud native processors. With the announcement of Microsoft Azure Cobalt 100 chips equipped with ARM cores in mid-November 2023, Microsoft is now one of the cloud operators that develop their own microprocessors for their internal needs.

[14] This tendency can be found in OEMs outside the computer sector. The automobile manufacturer Tesla sells electric vehicles offering assisted driving, which requires considerable computing power to train the models and manage the data mass required. Tesla announced that it had created its own chip in August 2021: the 'Tesla Dojo D1' was specifically designed to train self-driving AI models, and has a processing power of 360 TFLOPS.

[15] According to Microsoft, microservices architecture is a style of architecture used to develop applications. Modern cloud-native applications are generally built as microservices using containers. Cf. https://cloud.google.com/learn/what-is-microservices-architecture?hl=fr

2 / CYBERSECURITY, THE KEY TO SOVEREIGNTY

The rising use of the cloud has seen an increasing number of cyberattacks, some of them spectacular. New threats have developed that are particularly dangerous for organizations and infrastructures with a strategic, or vital, importance. The huge presence of cloud services in all sectors of the national economy makes cybersecurity the cornerstone of sovereignty. The work, action and initiatives of ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) point in this direction, along with the work of researchers and academics. The capacity of the French system to access highly skilled people in sufficient numbers to boost cybersecurity efforts lies with these researchers and academics.

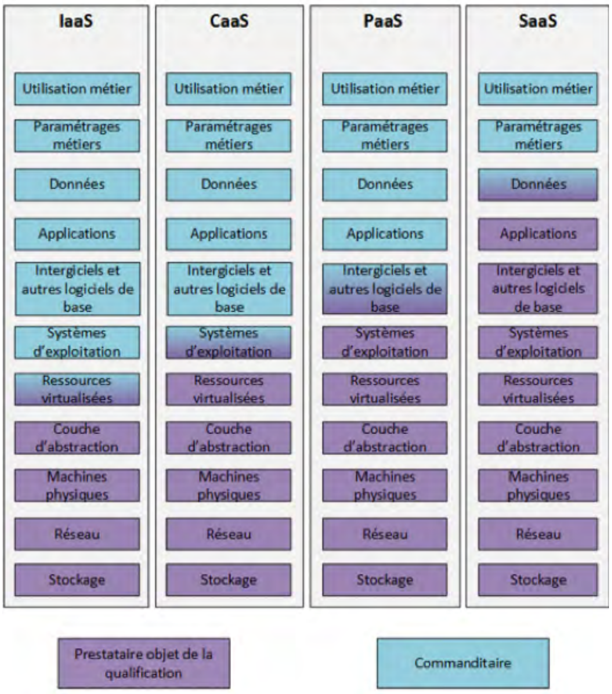
2.1 / ANSSI AND THE SECNUMCLOUD REPOSITORY

ANSSI has a mission to "assist the Prime Minister in carrying out his or her defence and national security responsibilities". The scope of its authority on cybersecurity has continuously grown since its creation by decree in July 2009[16]. ANSSI follows a doctrine based on the following basic principles of information security: confidentiality, integrity and availability. Applying these principles, the technical components of infrastructure cybersecurity have been reinforced in response to the new challenges related to the cloud.

The SecNumCloud[17] repository was developed in 2016 by ANSSI to certify cloud service providers. The aim is to promote, enrich and improve the range of trustworthy service providers available for public and private entities seeking to externalize the hosting of their data, applications or information systems. The qualification certifies the quality and robustness of the service, the competency of the service provider, and its trustworthiness. The respect of the SecNumCloud repository requirements guarantees the storage and treatment of sensitive data (i.e. for the order giver).

Four types of service provided by cloud service providers are concerned: SaaS (applications hosted on a cloud platform), PaaS (application-hosting platforms), CaaS (availability of tools to deploy and orchestrate containers), and IaaS. ANSSI defines IaaS as a service that "makes abstract computer resources available (e.g. CPU power, memory, storage, etc.). The IaaS model means that the order giver can obtain externalized, potentially virtualized, resources. The order giver maintains control over the operating system (OS), storage, the applications deployed, and some network components (e.g. firewall)".

Figure 3 – Model of breakdown of responsibilities by type of service (ANSSI typology)



SecNumCloud features a nomenclature of cybersecurity domains/activities to monitor: information security and risk management policies; information security organization; human resources security; asset management; access control and identity management; cryptology; physical and environmental security; operation-related security; communication security; acquisition, development and maintenance of information systems; relations with third-parties; management of information security incidents; activity continuity; compliance.

On European scale, and with the participation of ANSSI, the European Union Cloud Services Scheme (EUCS) is being developed. A preliminary version of the European Cybersecurity Certification Scheme for Cloud Services was published in December 2020. The text was the object of a public consultation, and is still subject to discussion, with the final version not yet available. Beyond time difficulties, the following points are worth noting. Nothing prevents the cloud majors in the USA and elsewhere from aiming at EUCS certification. Often, they are among the very first to obtain this kind of certification. When companies are from the USA, as mentioned earlier, even when hosting data in Europe and employing European personnel in subsidiaries subject to European law, they are obliged to answer any requests from US authorities under the Cloud Act. Hyperscalers possess top legal competencies that enable them to fulfil all of the technical-legal criteria of certification. Which pertains to the form and not the content.

The importance attached to cybersecurity in France does not depend on the authority of a national agency. Several recent political initiatives, for example as part of the France 2030 programme, have been

[16] Its staff increased from 120 at its creation in 2009 to almost 600 in 2021, with a target of 750 people.

[17] 'SecNumCloud' is the requirements repository for cloud service providers. https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf

launched to improve, through skills, the national capacity for dealing with cyberattacks. Engineering schools, universities and public research institutions take active part in these initiatives.

2.2 / THE INVOLVEMENT OF THE CEA

US and Israeli actors dominate the industrial cybersecurity sector. In order to guarantee their security and sovereignty in the digital domain, France and Europe started to launch numerous initiatives from 2016. They pursue several objectives: emergence of a world-class cybersecurity industry, achievement of breakthroughs and sovereignty in several key technologies, and creation of a cyber shield. In line with their values of democracy and human rights, they aim to increase the security of the digital society.

Since the early 2000s, the CEA has been putting together top-level cybersecurity research teams that contribute to the development of a sovereign French cybersecurity industry. The CEA's position results from the construction of operational expertise in cyber defence and technological research into cybersecurity. Currently, close to 160 engineers and researchers are developing new tools for analysing the security of equipment and software, along with technologies to make information systems (IS) secure against present and future risks and threats. The CEA runs several advanced research programmes corresponding to the needs of national industrialists in terms of sovereign technologies. The cybersecurity of operating systems is an important part of this. Research activities are organized into two areas: analysis of vulnerabilities and protection of systems, with research led by its two leading institutes on these subjects, CEA-Leti in Grenoble and CEA-List in Saclay (Paris region).

CEA-Leti carries out research on equipment security. Its laboratories working on securing components and electronic systems deal with security for the lower layers, proposing bricks and new component architectures intrinsically secured against attacks. CEA-Leti also hosts one of the three centres for evaluating the security of information technologies (CESTI), which deal with hardware for the French certification process, directed by ANSSI. The CESTIs evaluate the security of hardware components, like chips and HSM-type (Hardware Security Materiel) secure boxes, which are indispensable to secure digital infrastructures.

CEA-List carries out research on software and data security. It develops tools to analyse the vulnerability of software systems, like Frama-C and Binsec and new security technologies, like homomorphic encryption, intrusion detection, and new embedded operating systems (Xanthos).

The CEA is the scientific co-pilot of all of the research programmes (PEPR) for digital acceleration strategies (Quantum, Cybersecurity, AI, Cloud, 5G, Electronics) and the exploratory PEPRs NUMPEX and SPIN, which means it has a consolidated vision of the cybersecurity challenges in the system approach, combining equipment, software and data mentioned above. In the national cybersecurity strategy, it works alongside the Université Grenoble Alpes and the Institut Mines Télécom in their training action financed by the initiative Compétences et Métiers d'Avenir.

The CEA also works with the CNRS and Inria to pilot the Cybersecurity research programme (PEPR), with a budget of € 65M over six years, and is responsible for the programme. In this PEPR, the following three projects on system security have been running since 2022:

- SUPERVIZ (security supervision and orchestration) targets the detection, response and remediation of computer attacks, grouped together under the term 'security supervision', and attempts to reinforce preventative protection mechanisms and redress their shortfalls.
- SECUREVAL, coordinated by the CEA, aims to design new tools drawing from new digital technologies to verify the absence of material and software vulnerabilities, and carry out the required compliance demonstrations.
- ARSENE, coordinated by the CEA, aims to accelerate research and development of sovereign, industrializable security solutions in a coordinated, structured manner. The implementation of the ASIC and FPGA demonstrators integrating the bricks studied and developed will involve a final stage to test and showcase this research.

2.3 / TRAINING AND EDUCATION IN UNIVERSITIES AND SCHOOLS

Several schools and universities in France teach L- or M-level courses on the fundamental aspects of operating systems and their interactions with hardware to provide training on cybersecurity leading to a diploma. Apart from the cases mentioned here, these fundamental aspects do not however appear to be a major part of the curriculum. Or at least, not on a level to meet the challenges of national sovereignty.

The EPITA School of Engineering and Computer Science offers courses on cybersecurity and, since 2019, has been a partner of the French National Defence in this area. More recently, its cybersecurity bachelor's degree was granted the status of 'Grade de Licence' and from the start of the 2024 academic year, it will be working with Ecole Polytechnique to prepare some students for a career at the French Ministry of Armed Forces. The school has a research team in its laboratory working on cybersecurity and operating systems. Operating systems constitute the core of their expertise, from the kernel to the interface between the software and hardware, and including pooling and middleware. In addition to lectures on these themes, students specializing in security participate in a 'security workshop' that takes the form of an intensive lesson on basic vulnerabilities and operating techniques, with exercises to practise operating and participation in life-size ComCyber DEFNET exercises.

Ensimag (École nationale supérieure d'informatique et de mathématiques appliquées de Grenoble) offers courses combining applied mathematics and computing skills. Lectures are given on security in the first, second (code analysis for safety and security) and third years (information systems security, material safety and security, construction of secure infrastructures, and computer security and confidentiality).

IMT Nord Europe offers a master's course specializing in cybersecurity engineering, which is accredited by ANSSI's SecNumedu. Of the 45 ECTS credits, 2 relate to 'operating systems/Unix' and 'cloud computing and cloud security'.

Public actors are quite proactive in terms of cybersecurity. While cybersecurity is a relatively old subject, as shown by the Defence White Paper of 2008[18], things are moving fast. Much more powerful attacks are taking place, mobilizing cutting-edge technologies that are very expensive but profitable. Of note is the development of OSINT (open source intelligence) and its employment for national security, application of the law, and economic watch. On the other side, GAM companies are spending huge amounts of money to attempt to guarantee the security of their systems and those of their clients, up to three billion euros in 2021. That same year, Google Cloud acquired Mandiant for 5.4 billion dollars. Mandiant, for a long time one of the service providers favoured by the US government, provides information on threats. With this acquisition, Google, which already owns Chronicle and Security Command Center, ranks equal to Microsoft in terms of cloud services. Cybersecurity competition is raging between the three majors: Amazon WS, Microsoft Azure and Google Cloud.

3 / CLOUD CYBERSECURITY

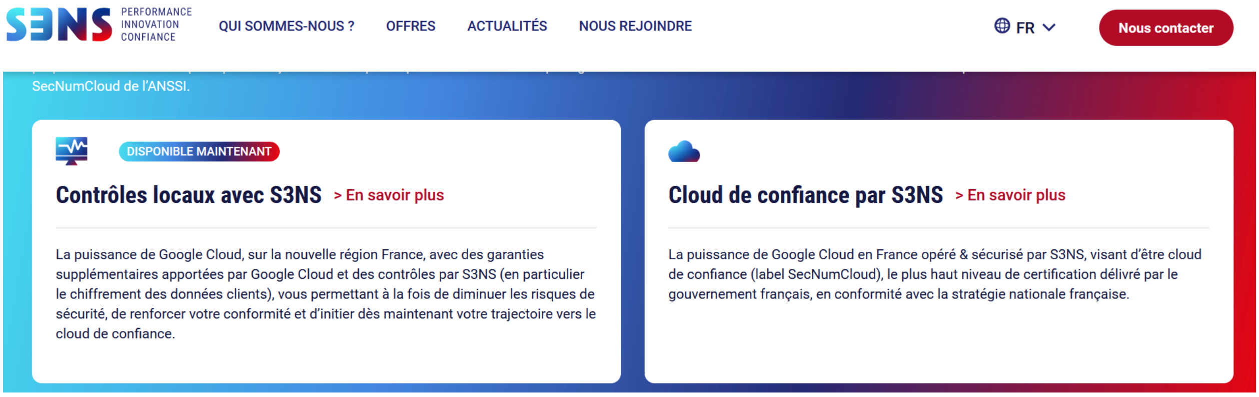
Each category of cloud services relates to a specific security context, and to different security issues. In datacentres, the physical environment (location, organization, feed stream, etc.) constitutes a major focal point. IaaS security is mainly a hardware issue. Concerning PaaS, the primary security area concerns controlling the runtime environment and supply chain of the software. For SaaS, it involves services and software security.

3.1 / DIFFERENT CLOUD SERVICES SUBJECT TO DIFFERENT CYBERSECURITY ISSUES

The challenge of digital sovereignty can initially be seen as concerning the location of computing resources (and data): the location of servers and cloud services and/or datacentres. In France, several 'trusted sovereign clouds' are being developed: BLEU gathers Orange, Cap Gemini and Microsoft; S3NS for Google Cloud and Thales; NUMSPOT covers Docapost, Dassault Systèmes, Bouygues and the CDC.

[18] Cf. White paper "Défense et sécurité nationale", Odile Jacob, June 2008, https://www.diplomatie.gouv.fr/IMG/pdf/0000.pdf

Figure 4 – Services offered on the S3NS website (Google Cloud & Thales), May 2023



SecNumCloud de l'ANSSI.

Contrôles locaux avec S3NS

La puissance de Google Cloud, sur la nouvelle région France, avec des garanties supplémentaires apportées par Google Cloud et des contrôles par S3NS (en particulier le chiffrement des données clients), vous permettant à la fois de diminuer les risques de sécurité, de renforcer votre conformité et d'initier dès maintenant votre trajectoire vers le cloud de confiance.

Cloud de confiance par S3NS

La puissance de Google Cloud en France opéré & sécurisé par S3NS, visant d'être cloud de confiance (label SecNumCloud), le plus haut niveau de certification délivré par le gouvernement français, en conformité avec la stratégie nationale française.

When it comes to 'controlling the physical environment', sovereignty concerns the cybersecurity conditions of the setup, the architecture of the buildings and the datacentre equipment. An accident that occurred in one of the datacentres of a cloud service supplier has raised awareness of the issue of physical vulnerability[19].

Two approaches to digital sovereignty stand out, as shown by discussions during the preparatory phase of GAIA-X and its launch. Sovereignty can be mainly approached as a question of the geographic location of equipment and data. Alternatively, it can be considered as a question of adhering to and respecting rules, which themselves translate values. Given the extraterritorial nature of the US legal system, in reality, location is of little importance: when an American company, or a company employing an American, or that has an economic activity on American soil, is involved in using data, the US state can, under certain conditions, obtain access (cf. Clarifying Lawful Overseas Use of Data Act or the C.L.O.U.D. Act, 2018). Therefore, a location approach to digital sovereignty turns out to be ineffective. Reciprocally, standards relating to cybersecurity and data circulation override the question of location.

The quality of the service provided by a datacentre firstly depends on its physical characteristics, followed by its energy system, the robustness of its material protection of information and humans, its surface area, spatial configuration, hardware, the chain of execution and software development, and its Continuity Plan in times of crisis.

When it comes to controlling the software runtime environment and supply chain, at the interface between IaaS and PaaS, the container comes into play. The container is a virtual envelope that is used to distribute an application along with all of the elements that it requires to operate: source files, runtime environment, libraries, tools and files. These elements are assembled in a coherent manner and ready to be deployed on a server through its operating system.

Unlike for the virtualization of servers and the use of a virtual machine, containers do not contain a kernel, they directly use that of the computer on which they are deployed. Consequently, in terms of security, the weak point is the vulnerability of the actual kernel. The choice between virtualization or using a container thus results in a dilemma between pooling (virtualization) and security[20].

3.2 / ROLE OF THE MICROPROCESSOR IN CYBERSECURITY [21]

In the cloud security domain, the decisive character of the microprocessor is not self-evident. A number of key prerequisites therefore need to be made clear. Firstly, it is worth establishing what cybersecurity covers exactly, bearing in mind the adage: 'no threat, no need for security'. As a result, cybersecurity solutions and architectures respond to the nature of threats. Cybersecurity solutions relate to explicit targets: the manufacturer, regulations, the final user, etc.

Secondly, threats vary depending on the domain of application: a particular threat is met by a particular type of security and defence. Different markets correspond to different threats, attacks and security solutions. As an example, consider the following two very different domains: the cloud in datacentres on the one side, and embedded systems and the IoT on the other. The first case involves multi-clients requiring horizonal isolation. The environment is noisy and unpredictable, with hundreds of thousands of servers each hosting hundreds of virtual machines. They are vulnerable to logical attacks: malware, infections, global cybersecurity solutions, and possible hardware anchoring. The system is static and the environment is stable. Physical attacks, whether involving highly isolated systems like HPCs or potentially exposed

[19] Cf. Fire at the OVH site in Strasbourg on 11 March 2021.

[20] The Linux kernel is known for its 'dirty pipe' flaw (ranked as CVE-2022-0847 with a CVSS severity score of 7.8 on a scale of 10). Dirty pipe means a local privilege escalation vulnerability in the Linux kernel that could potentially allow an unprivileged user to inject a code into the root processes. The flaw lies in the management of the pipelines, which are one-way inter-process communication mechanisms.

[21] These developments are largely inspired by the presentations made by Thierry LELEGARD, Security Manager of the platform at SIPEARL, during working group meetings. Any errors, simplifications or omissions are the sole responsibility of the author.

systems like the edge, are therefore unlikely. The systems concerned are general, like all types of OS, users and activities. In addition, the network environment is open: all types of applications and network protocols, and therefore all types of malware and other viruses present on the internet. Logical attacks occur all the time, and the System on a Chip (SoC) is ‘immersed’ in the system.

The second case concerns embedded systems and the Internet of Things (IoT), which are managed by a single depository of security, a ‘master of secrets’, and relate to a mono-activity. They require deep vertical defence. The environment is predictable, physical access is easy, and users and attackers are often one and the same. These systems are therefore generally exposed to physical threats, like fault injections, side-channel attacks, and hardware reverse engineering.

The important point here is that the variety of threats that depend on the areas of application –the two typical cases being servers on one side and embedded systems on the other – need to be met by pertinent, coherent cybersecurity solutions. Guaranteeing the security of the cloud therefore involves both a software dimension and a physical dimension.

A practical and conceptionally thought-through approach to cloud security involves recognizing two key notions. On the one side, security needs to be conceived as a chain; on the other, security is a systemic strategy.

Security is part of a continuous chain. The security of the entire system depends on the security of the weakest link in the chain. Since security involves all components of the system, it is vital to identify the processor’s value added and its place in the security chain. This approach applies in a pertinent way to the cloud, where the processor is only one component among others. This situation is clearly very different from the embedded world (IoT), where the SoC is the main component of the system, or even constitutes the entire system.

Since security is a systemic programming, a global approach needs to be taken that is both top-down and bottom-up. Security by design is a top-down approach that consists in *anticipating* security intrusions in the design of the system. The security areas and their isolation are defined from the start: confidentiality, integrity, authentication, chain of trust, etc. Security by design consists in segmenting the runtime and memory access. The security model for servers defined by ARM[22] is called Confidential Compute Architecture (CCA)[23]. CCA applies a concept of ‘realms’ that duplicate certain functional areas of the normal architecture via four exception levels (user, kernel, hypervisor and monitor). When a logical attack takes place, the intruder is already inside the machine.

So-called defensive security takes a bottom-up approach. It involves *responding* to security intrusions. Bugs will always occur, transformed by hackers into vulnerabilities and intrusions. Cyberattacks are inevitable, and the aim is to understand them and provide capacities to react and respond. Taking this approach, the value added of the processor lies in its role in controlling the runtime, and in detecting and reacting to suspicious activities. Attacks involving code injections and malware infections are some of these suspicious activities that the processor can detect and block at an early stage. Attacks from software running on the processor are the main vectors of the cyberattacks and ransomwares that sabotage hospitals and public and private institutions.

[22] The British company ARM Ltd develops 32-bit and 64-bit architecture processors. However, it does not manufacture or sell them in the form of integrated circuits, but rather sells licences for its processors to manufacturers (which engraves them on silicon). Almost all chip manufacturers offer ARM architectures.

[23] More recent and less well known than TrustZone for embedded systems.

04 The cloud security chain, from operating system to microprocessor

The low layers of interest include the middleware, operating system, system architecture and microprocessor. When aiming at sovereignty, the microprocessor is a key component in a stack that also includes the operating system, compilers and architecture. The challenges of the lower layers relate to two fundamental connected links: the operating system – the software that allows the programs to operate – and the microprocessor, in particular where cloud computer systems are involved. Consequently, the pursuit of an alternative European cloud system involves focusing efforts on these two complementary links. The key point is the following: without an adequate software and architectural envelope, a new sovereign microprocessor would have difficulty widely positioning itself in cloud servers. An integrated approach to cloud sovereignty is therefore broken down into the fundamental scales of the microprocessor, and a new conception of its role in terms of cybersecurity, and deep software components.

1 / EUROPEAN CHIPS AND OPEN SOURCE CLOUDS ARE TECHNOLOGICALLY COMPLEMENTARY

SiPearl was created in June 2019 with the aim of accomplishing the European Processor Initiative (EPI): encourage the deployment of high-performance, low-power microprocessor technologies with watertight security. The company receives funding from the European Innovation Council[24] to develop and market the European microprocessor that will accompany European supercomputers up to exascale level. It works closely with its 27 EPI partners. The consortium gathers actors from the scientific community and supercomputer centres, IT majors, future clients and final users of, for example, electronics and automobiles.

In 2018, the European Union joined the race to produce an exoflop supercomputer, when it set up EuroHPC JU, the European High Performance Computing Joint Undertaking. As part of this joint company, SiPearl is designing the microprocessor Rhea1, the centrepiece of the future European exascale supercomputers. Since 2022, EuroHPC has entered a new development phase of the European microprocessor; the Rhea chip will be improved for better use in the future European supercomputer (higher number of kernels, increased memory bandwidth, more acceleration, etc.).

An important step in the development of SiPearl to the advantage of the European supercomputer dates from early October 2023, when the company won a contract to equip JUPITER, the first European exascale supercomputer[25].

In the long term, SiPearl chips, which will be sovereign and feature advanced energy consumption and cybersecurity properties, will be used to equip cloud servers.

Since January 2023, SiPearl has been actively participating in the European project AERO (Accelerated EuRopean clOud)[26], whose mission is to ensure the possibility of deploying the EU's future heterogeneous cloud infrastructure. This key project, put forward as an "indispensable complement to the EPI", should structure and amplify the open-source ecosystem enabling the processor's integration into the cloud. AERO will improve the performance, security and energy efficiency of the processor within an adapted ecosystem. As a result, it should encourage users to migrate to the European platform, infrastructure and ecosystem.

2 / AND COMPLEMENTARY VIS-À-VIS THE SOFTWARE ENVIRONMENT'S LOWER LAYERS

As we have pointed out, it is by applying a strategy to get round 'ownership lock-in', through open source, that companies established in Europe will be able to adopt these (European) advanced cloud

[24] SiPearl received a subsidy of 2.5 million euros and an equity investment of 15 million euros.

[25] The EuroHPC supercomputer will be installed on the campus of the Jülich research centre in North Rhine-Westphalia, Germany. It will be built by a consortium comprising Eviden, the business branch of the Atos group, a leader in advanced computing, and ParTec, a German company specializing in modular supercomputing.

[26] Three-year project that started in January 2023.

technologies (cf. Chapter 2). This is the priority avenue to reinforce European sovereignty and competitiveness in the digital field.

The obstacle to rolling out a new microprocessor on a wide scale is financial. Chip use is optimized in terms of the surrounding software stack. Yet it is much too expensive for a microprocessor company to also develop the operating system corresponding to its chip. Nevertheless, this is the condition for gaining digital sovereignty, by introducing heterogeneity into a monopolistic integrated system. Linux, by developing its own operating system using open source, led to innovations, including at hardware level (cf. Chapter 2, Point 3).

Thus, at the start of its development, the company BULL was not large enough to carry the host software stack on its own servers. The cost of developing this kind of environment, required to sell servers, was too high for BULL to meet on its own. The irruption of Linux broke the ownership rationale of IBM servers by providing a standard to all services that featured Linux (cf. Chapter 2, Point 3). As a result, the cost of the innovation dropped dramatically. At the time, offering this kind of service required an investment of one billion dollars, along with the cost of R&D. Linux greatly reduced software costs, which gave newcomers the opportunity to introduce hardware innovations at an acceptable price (200 million dollars instead of one billion)[27].

The proprietary character of Microsoft systems is still apparent in microprocessors that feature encryption keys designed to operate with Microsoft software.
To have a chance to regain sovereignty in the cloud, the first step involves successfully establishing an 'IaaS Linux' (the equivalent of the cloud operating system). This standard (open) software base would allow the development of hardware innovations like a sovereign microprocessor, such as that of SiPearl. In the absence of an open IaaS standard, the cost of developing the software environment required for improved microprocessor functioning would be extortionate.

At the scale of a European cloud service provider, getting round proprietary lock-in will involve taking back control of specific cloud service management tools.

3 / BACK TO THE MICROPROCESSOR, THE STRONG LINK IN THE CLOUD CYBERSECURITY CHAIN

To ensure that the microprocessor – in this case sovereign – upholds its security value added in the cloud cybersecurity chain requires changing our point of view on the source of the threat. Traditionally, cybersecurity teams have focused on detecting malicious 'payloads'. Classic techniques applied during an attack aim at neutralization: perimeter security at entry (e.g. firewall), internal detection network, behaviour-based security (e.g. software integrity), application security (code resistance in case of intrusions). The key moment when the processor is solicited, i.e. when the program is run, is generally not considered. It is as if running a program were at best imponderable, at worst inexistent, a black box.

In a sovereign approach to cloud cybersecurity, where the operating system gets round lock-in, thanks to advanced qualities, and where the processor also represents a guarantee of autonomy, the focus moves from the 'payload' to the 'vector'. In this new cybersecurity setup, the function of preventing non-standard runs and therefore preventing intrusions, comes down to the processor. A microprocessor that is designed to be secure, like that of SiPearl, provides physical security that protects the entire platform. And it does so right up to the level of the firmware responsible for starting up the system. If the latter is 'infected', access to it is simply refused. In this kind of model, each layer of the security infrastructure completes the next one.

The SiPearl approach to cybersecurity at the microprocessor scale is part of a branch of applied research to which ARM contributes. It also contributes to the project 'CHERI' (Capability Hardware Enhanced RISC Instruction). CHERI started out as a joint research project involving SRI International and the University of Cambridge in 2010, financed by the DARPA programme, Clean-slate design of Resilient, Adaptive and Secure Hosts (CRASH). Participants in the programme worked on rethinking the material/software stack to improve security. In January 2022, ARM announced that the first chip supporting the prototype architecture Morello[28] was available on a limited series of demonstration cards. They were sent out to partners in the industry for trials[29]. Morello is the first high-performance implementation of CHERI extensions.

[27] The value added of the machine lies in its classic architecture known as 'Von Neumann', which relies on a memory pool as a unique place for storing instructions and data required or produced by the computing. This means that each individual microprocessor participates in the structure. BULL had developed a cache coherency algorithm – guaranteeing processors a consistent overview of memory – that was more efficient than other options available. BULL therefore benefited from a free OS (Linux) to develop a microprocessor system based on its supercomputers.

[28] Morello is a research project aimed at radically changing the way that processors are designed and programmed in the future to improve integrated security. It was originally financed by the British government's Digital Security by Design (DSbD) programme, Industrial Strategy Challenge Fund (ISCF) and directed by ARM. Cf. https://www.arm.com/architecture/cpu/morello

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

05 Courses of action, conclusive reflections

Taking a problem of prime importance, in other words strategic autonomy or digital sovereignty, and breaking it down in an instructive manner – at a level that can lead to action – is the very purpose of the 'For an Industrial Digital Policy' working group.

The wide range of public and private participants, all with a high level of technical skills, promoted the establishment of a shared diagnosis and encouraged the development of a targeted, differentiating approach to the problem. This shared diagnosis not only stemmed from the actual work of the group over the year, it also fits in with previous reports. For example the identification of the structuring character of digital platformization, in particular for industry. This infrastructural component, which comes from interdependent, heterogeneous clouds, constitutes the dynamic framework of our approach. The digital platformization of European industrial companies, thanks to cutting-edge European skills and technologies, is the desirable horizon of solid sovereignty.

By focusing on the lower layers of the cloud, our approach suggests a way to successfully get away from the 'proprietary lock-in' endured by European companies. Three US multinationals hold three-quarters of the cloud market, with a similar pattern of interdependent proprietary technologies on all of the layers. Similar to what happened at the end of the domination of IBM mainframe systems, we need to once again find the necessary mobilization to push through 'de-proprietarization'. Starting where it is logically possible and technically pertinent, i.e. at the scale of the operating system and the key component of servers, the microprocessor.

We therefore propose to establish the conditions for an open source European alternative to the cloud operating systems developed by GAM (Amazon Web Services, Microsoft Azure, Google Cloud). The Gaia-X initiative moves in the right direction. It needs support to go further and ensure the interoperability of all cloud service providers. Thus, operating systems and virtualization capacity need to be equipped with open source offers. In addition, we need to encourage and support the use of a European microprocessor in the servers of European cloud service providers. This microprocessor should be seen as the central operator of the cybersecurity chain. The success of the SiPearl European chip – its largescale roll-out in the servers of cloud service providers – constitutes a key step.

In these two domains, we suggest stepping up efforts, with our European partners, to implement a European platform for an open source cloud infrastructure. Public projects and programmes (French research organizations and those of other Member States) and companies and consortia have been launched but risk lacking ambition due to insufficient mobilization. The vectors of interest of these public-private efforts would be very usefully oriented by a public order for cloud services featuring servers equipped with secure European microprocessors that would operate on an open source IaaS platform. The needs are enormous, in France and elsewhere in Europe, in numerous domains where public services play a major role, like health, research, education, transport, and energy, among others.

Lastly, in the face of the deleterious effects of proprietary lock-in, the solution also involves mobilization on sovereignty issues in higher education and digital research institutions. A lot more university courses need to cover the lower layers in terms of cybersecurity and sovereignty. Over-specialization in development of high software layers, including in terms of cybersecurity, tends to feed into the lock-in situation. Beyond significant efforts made as part of the France 2030 programme, the French state could usefully create specific finance measures (to complement Compétences et Métiers d'Avenir) that support the evolution of secondary and higher education courses in France to include targeted teaching on operating systems.

ASSOCIATION NATIONALE
RECHERCHE TECHNOLOGIE

33, RUE RENNEQUIN - 75017 PARIS
PHONE : +33 (0)1 55 35 25 50
WWW.ANRT.ASSO.FR