Clingendael
Netherlands Institute of International Relations

Policy Brief

Alexandre Gomes & Maaike Okano-Heijmans

MARCH 2024

Too late to act? Europe's quest for cloud sovereignty

As European governments start adopting cloud services, the notion of cloud sovereignty is still largely underexplored. The future of the governments' information technology landscape lies in hybrid cloud solutions, but the European cloud market is dominated by American providers. European alternatives are scarce in quantity and in what they can offer. Cloud sovereignty requires quality technology, but also trust, security and diversification – three elements that are not necessarily ensured by the current American offers. Making proper data classification and finding talent to manage such landscapes are other important challenges. Reducing cloud vulnerabilities requires giving European providers the ability to grow and develop fitting and specialised solutions, including via tailored public procurement that can, over time, contribute to building minimum viable clouds in EU Member States.

Introduction

In recent years, the Netherlands and the European Union (EU) have started to act on their desire to be more resilient and less subject to geopolitical tensions. Next to strategic autonomy in the defence and energy domains, digital economic security is high on the political agenda.[1] Amid a rapidly evolving geopolitical landscape and the rising disruptive potential of technology, vulnerabilities in the digital sphere are proliferating.

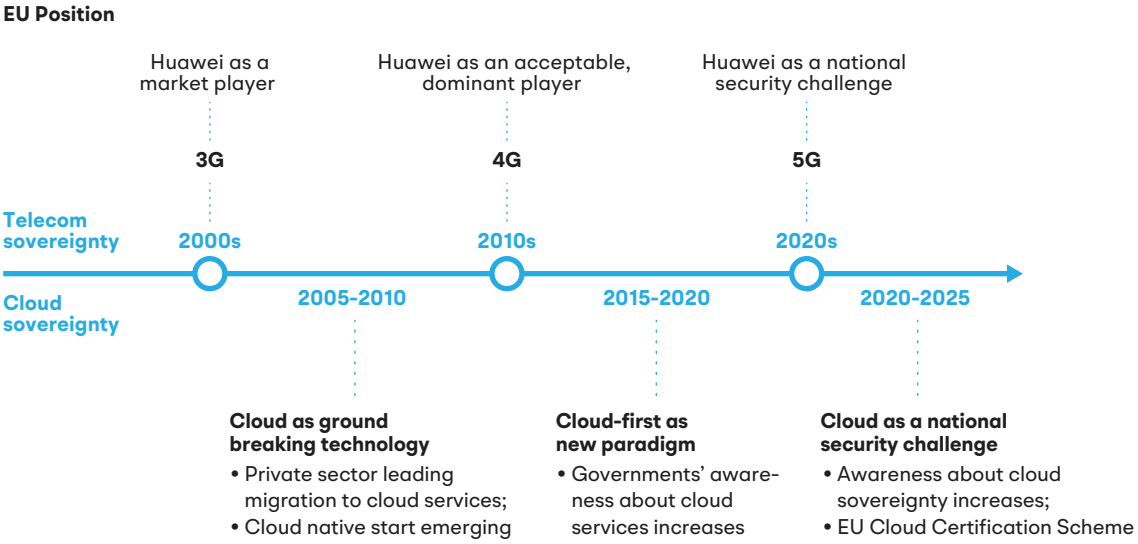
Reducing dependencies on external actors is a key step towards enhancing the European bloc's (digital) economic security and the EU's ability to make its own decisions. Since the late 2010s, European governments have thus been pushing for reduced reliance on China's Huawei for critical parts of telecommunication networks in the shift from 4G to 5G networks. Today, the EU stands at a similar juncture with regard to cloud services (see Figure 1 below). As not only companies but also governments are shifting to cloud-based IT services, data protection and protection against external interference must be central in the debate.[2] This time, however, the EU's dependence is not on Chinese companies, but on American Big Tech.

The authors are grateful to the many experts who contributed their inputs to this Clingendael Policy Brief.

1 Maaike Okano-Heijmans, Alexandre Gomes and Daniel Kono, *Strengthening digital economic security in Europe*, October 2023.

2 The 2013 revelations by whistleblower Edward Snowden about US surveillance programmes abroad rang the initial alarms. As of the end of 2023, nine of the ten highest fines applied because of noncompliance with the EU's General Data Protection Regulation (GDPR) were enforced on American Big Tech companies, and one on a Chinese company.

Figure 1 **Is the EU living its '5G moment' on cloud?**



Source: authors' compilation

The three biggest universal cloud service providers (CSPs) operating in the EU – Google, Amazon and Microsoft – have a combined market share of 70 per cent. European alternatives to these American CSPs – also known as hyperscalers – are limited, both in number and in scale.

As growing numbers of consumers, companies and government institutions move their data to the cloud, now is the time for the EU and its Member States to develop a unified view on how to balance technologically enabled efficiency with public interest and national security. EU Member States such as France, the Netherlands and Estonia have different understandings of what cloud sovereignty means, and of the national (security and economic) interests that underpin cloud sovereignty. Clarity about the desirable level of cloud sovereignty can inform finer decision-making on how to address current dependencies on non-European CSPs. This must involve a mix of better protection, bolder regulation and stronger European alternatives.

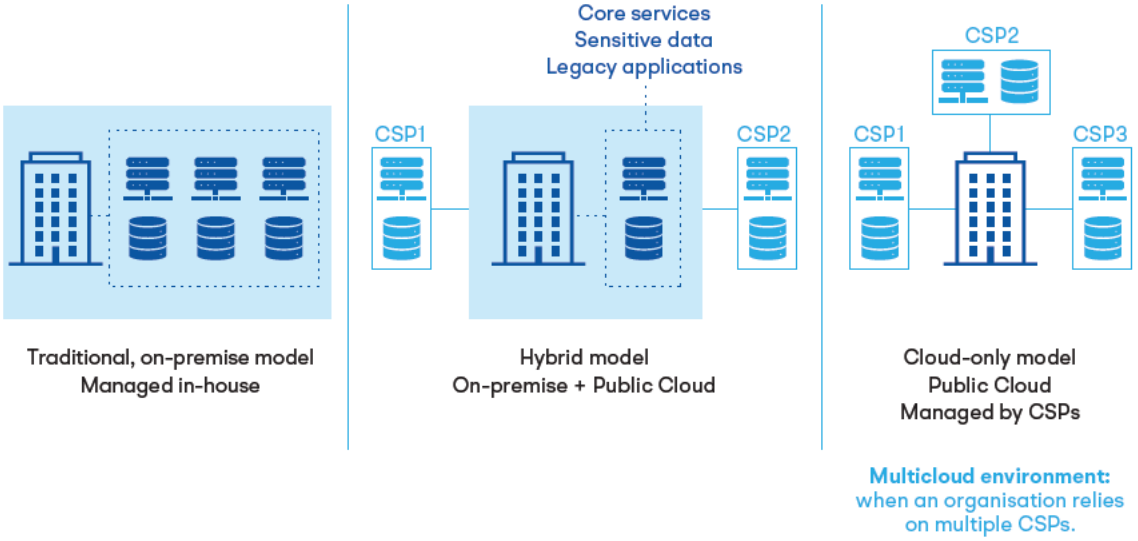
The Dutch government is well aware of the growing importance of cloud services. Cloud is one of ten policy priorities highlighted in the October 2023 Dutch Agenda for Digital Open Strategic Autonomy (DOSA).[3] The main justification for this focus on cloud is the wish to maintain control over strategic and sensitive data. In addition, the Dutch government's January 2024 report on the *State of the digital infrastructure*[4] details access to cloud services as one of five critical elements of digital infrastructure.

This Clingendael Policy Brief seeks an answer to the question: what steps must be taken to promote and to protect Europe's technological sovereignty? In doing so, it starts by detailing the most important international policy developments on cloud services, especially in the EU and in the Netherlands. Building on this, the policy brief then outlines key considerations that EU governments must ponder before ramping up their usage of cloud services. As the EU is currently living its '5G moment' on cloud, now is the time to act to uphold Europe's tech sovereignty, also in the cloud domain.

3 The weak European position in the market is among the reasons indicated for cloud becoming a focus of attention. See: Government of the Netherlands, *Agenda Digitale Open Strategische Autonomie*, 17 October 2023 (in Dutch).

4 Government of the Netherlands, *State of the digital infrastructure: the backbone of our digital economy*, report, 22 January 2024.

Figure 2 **Three cloud models: traditional, cloud-only and hybrid**



Source: authors' compilation

The rise of cloud services

The emergence of cloud services in the early 2000s was a major breakthrough in information technologies (IT). IT infrastructure and services[5] used to be hosted on the premises – that is, 'in-house' at any specific company, school or government agency. The private sector, which is typically more inclined to take risks and test new solutions, moved to cloud services first. Businesses started transitioning their IT services to virtual environments, delivered remotely and externally managed by CSPs. Doing so offered much sought-after relief from management by the in-house IT staff of increasingly large and complex systems, thereby allowing companies to focus on their core business. Cloud computing also enables the growing use of adjacent disruptive technologies, such as the Internet of Things and artificial intelligence (AI).

Figure 2 depicts the conceptual difference between the traditional, on-premise model (on the left) and the cloud-only model, where all IT services are managed by CSPs (on the right). The hybrid model (at the centre) is currently the most common model used by companies. When an organisation relies on multiple CSPs, it is said to have a multicloud environment.

A special form of hybrid cloud emerges with community clouds. A community cloud is hybrid cloud computing infrastructure that is built by and accessible to a more or less restricted group of organisations with common interests or requirements. Community clouds often have a sectoral nature (see the section on Promote, below).

Balancing efficiency and sovereignty

Cloud models come in different forms, each of which has a specific balance between (tech-enabled) efficiency and ownership of the system – that is, sovereignty, or ownership and the ability to manage the system and the data that run on it. 'Cloud services' typically refer to public clouds, which are owned and developed by CSPs. The best-known examples are Google Cloud Platform, Amazon Web Services and Microsoft Azure. Most CSPs also offer private clouds, which resemble the on-premise model but additionally offer some of the benefits of the public cloud.

5 IT infrastructure and services include: (1) hard infra-structure services, such as hosting and storage; (2) soft infrastructure and development environments and services, such as databases and middleware; and (3) mature applications services. CSPs differentiate these by offering, respectively, Infrastructure as a Service (IaaS); Platform as a Service (PaaS); and Software as a Service (SaaS).

Cloud benefits

Cloud services offer three important advantages over on-premise IT management. First, by providing access to a larger range of management and intelligence services than non-cloud alternatives, cloud services enable quicker and more flexible applications development. In addition, cloud services enable much more scalability, because they can easily adjust to peaks in demand. Finally, cloud services can be financially attractive to small and medium-sized enterprises (SMEs) – especially start-ups. Cloud services allow them to have basic infrastructure without, or with very limited, initial capital costs that can be a big barrier to starting a new business.

Although cloud services are not necessarily cheaper than on-premise IT services, the 'pay-as-you-go' cloud pricing model has democratised access to cutting-edge technology. With *cloud-first* being the current status quo in IT infrastructure management – whereby companies and organisations aim to run all their IT infrastructure and services using cloud services, unless there is no alternative – established enterprises no longer have the strategic advantage that they had in the past.[6]

Cloud challenges

Migrating from the traditional on-premise model to cloud services raises important questions. Technical considerations and changes required in IT procurement, management and skill sets are substantial. With a view to cloud sovereignty, organisations must decide what infrastructure, applications and data they wish to keep on-premise and what to move to the cloud, and with how many and which CSPs to engage. These considerations must go hand in hand with a robust data classification mechanism. Only by properly classifying data (that is, identifying what is restricted, confidential or public) can organisations make well-informed decisions about what must remain on-premise and what can be moved to a (safe) cloud.

Governments to the cloud?

As government institutions are moving to the cloud, they need to tackle these questions with due consideration of public interests. On the one hand, they must tailor their actions to citizens' expectations of more and better e-government – much as consumers demand innovation and better functionality from the private sector. Governments themselves want to improve their efficiency, namely by increasing interoperability within their services and with the outside world.

On the other hand, governments' IT landscapes and responsibilities are more complex than those of most companies. After all, they also face critical national security considerations. Next to data privacy and cybersecurity, espionage (challenges that companies also face) – that is, unlawful (foreign) access to citizens', businesses' or governments' sensitive data – is a particularly challenging risk to manage. After all, citizens do not necessarily share their data voluntarily: to hold an ID card, file taxes or to benefit from social services, citizens are *de facto* forced to share their data. In addition, governments face growing political scrutiny from lawmakers, who want to ensure that citizen's rights are protected. This makes it even more important for governments to guarantee proper data management.

American CSPs are attentive to this discussion, and several have announced sovereign cloud offers. However, it is still early to assess their viability for two reasons. Firstly, these offers have not yet been sufficiently tested, and the extent to which they respond to all concerns and serve governments' interests are yet to be proven. Secondly, these sovereign cloud offers may prove too costly for CSPs in the long-run, in which case they could have an incentive to de-invest in sovereign cloud offers and leave European governments in a vulnerable position.

For their part, Chinese companies are by definition excluded from hosting applications and data deemed sensitive, as the country is identified as running a structural, offensive cyber offensive against the Netherlands and Dutch interests.[7]

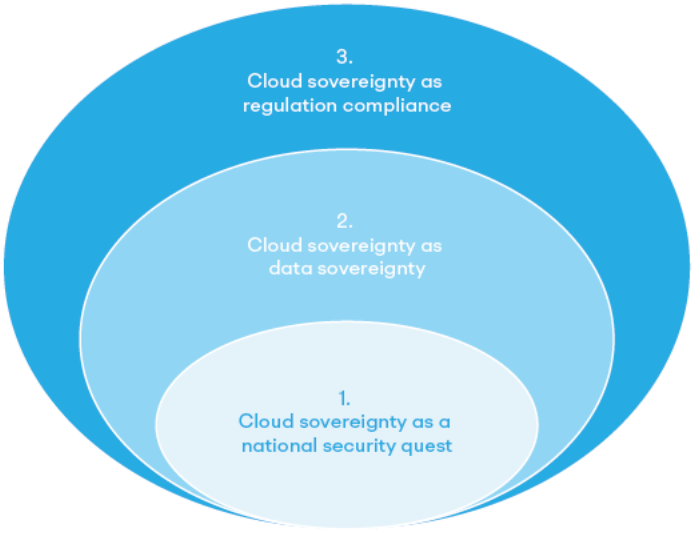
6 In fact, established companies may be at a disadvantage, as they need to make large investments to migrate from their traditional model to cloud services.

7 National Coordinator for Counterterrorism and Security, *Cyber Security Assessment Netherlands*, CSAN 2022.

Box 1. The upcoming 'email problem'

The many governments and organisations that currently manage Microsoft Outlook on-premise and are considering moving to the cloud need to be aware of the upcoming 'email problem'. Microsoft owns one of the most popular email services worldwide, ***Microsoft Outlook****. If current trends persist,* ***Microsoft is expected to push for all email servers to be migrated to Outlook's cloud counterpart, M365****. This would mean that governments' email servers would be hosted on Microsoft's cloud. Such a move would most likely attract greater attention from (state and non-state) hackers, making it a* ***tempting target*** *to gain access to governments' – potentially sensitive – data.*

Figure 3 **Three layers of cloud sovereignty**



Source: authors' compilation

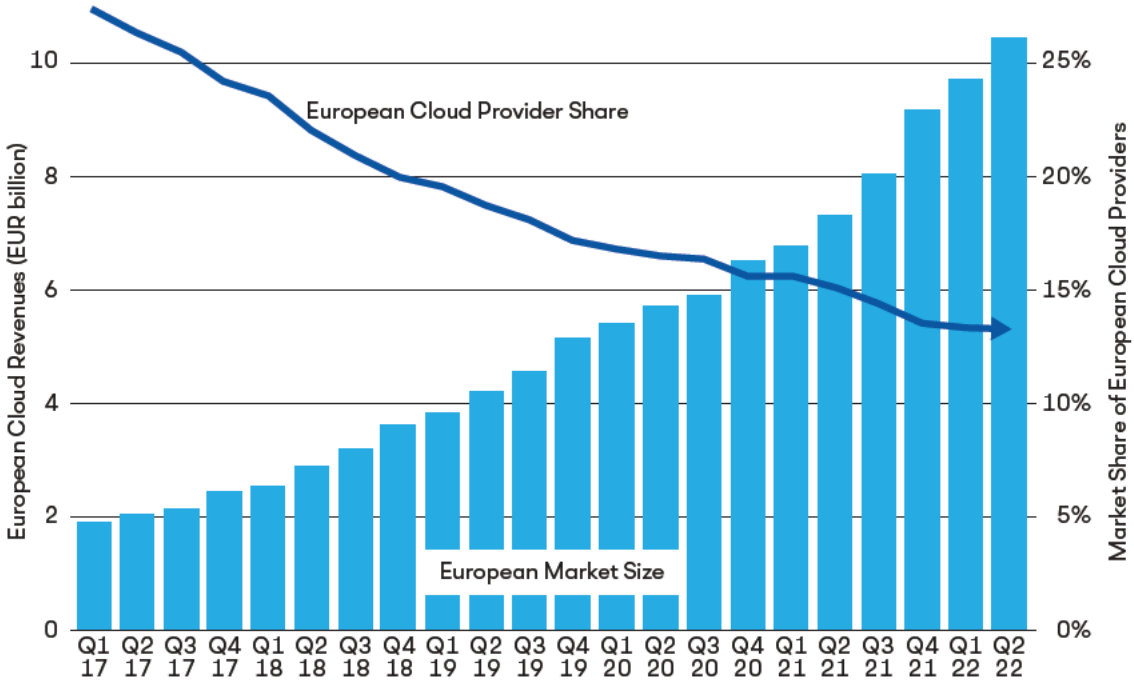
As detailed in Box 1 above, governments already have less sovereignty over their data than they might realise, because of (over)reliance on a single foreign software company that can unilaterally decide to move its services to the cloud.

A key point to consider for governments' tech sovereignty is thus how to deal with (highly) classified data. This is the heart of the discussion on cloud sovereignty: how to balance new technical efficiency while not jeopardising national security?

Set against this backdrop, cloud sovereignty is of paramount importance for governments. Seeking to unpack this broad concept, it is useful to envisage a model with three layers of sovereignty (see Figure 3). The inner layer of the model is *cloud sovereignty as a national security matter*: when cloud sovereignty is regarded as a matter of national security, raising the highest standards of requirements on data location and the country of origin of the CSPs that host the data. The middle layer is that of *cloud sovereignty as data sovereignty*: when the highest requirement is to ensure data privacy, security and local storage, regardless of the CSPs' origins. In the broadest sense, cloud sovereignty may be regarded as a matter of *regulation compliance*: the ability to get CSPs to comply with local regulations, regardless of where data is located.

A first step to enhancing European digital economic security in the long term is to develop and act on a clearer understanding of cloud

Figure 4 European CSPs' market share as a percentage of total European cloud revenues



Source: Synergy Research Group

sovereignty: as a national security matter, as a data sovereignty question, as a regulation compliance challenge – or as a mix of the three. Having such clarity will enable governments to make informed decisions as they contemplate investments to take their own data to the public cloud as well as to enhance the competitiveness of European cloud companies and environments.

(Geo)Politicisation of cloud services?

The EU is at a crossroads. Like most developed economies, EU institutions and Member States are shifting to cloud-based IT services.[8] This move raises concerns about dependencies on non-EU CSPs, in similar ways as during the rollout of 5G networks in 2017. Then, the United States pushed the global debate on the national security implications of Huawei's role in 5G networks, in which the Chinese company was a leader. Helped by a newly created EU toolbox for 5G security,[9] many European governments ended up formally or informally banning Huawei from (parts of) their 5G networks based on concerns about possible espionage and cyberattacks carried out through Huawei's networks.[10]

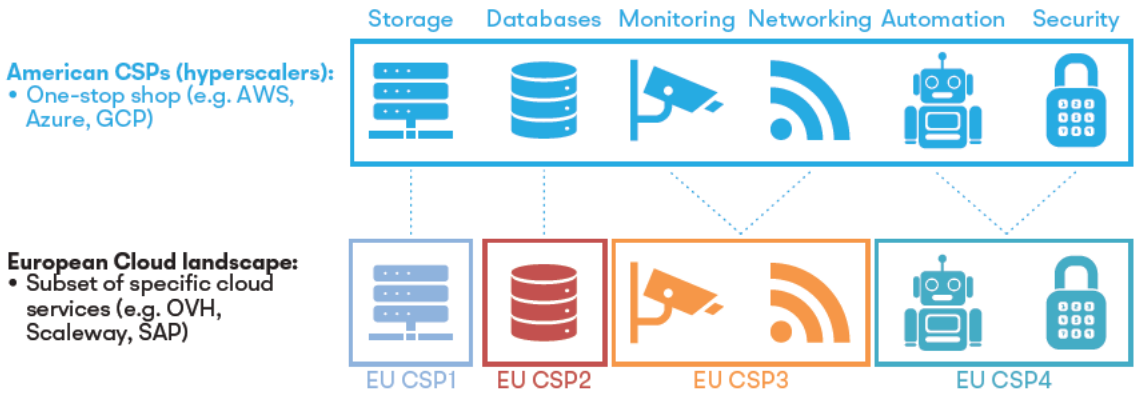
Today, the EU stands at a similar juncture with regard to cloud services. This time, however, the dependence is not on a Chinese company but on American Big Tech. Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) have a combined market share

8 The United Kingdom, in particular, has been a leader in the use of public cloud applications in government organisations for many years, with the UK G-Cloud initiative. See: Government of the United Kingdom, *Guidance: applying to the G-Cloud framework*, last updated in March 2022.

9 European Commission, *The EU toolbox for 5G security*, 29 January 2020.

10 In 2022, the Biden administration banned Huawei and ZTE's telecommunications equipment altogether. See: CNET, *Huawei ban timeline: detained CFO makes deal with US Justice Department*, 30 September 2021; and Reuters, *US bans new Huawei, ZTE equipment sales, citing national security risk*, 1 December 2022.

Figure 5 **Conceptual difference between what the American hyperscalers and European CSPs can offer**



Source: authors' compilation

of 70 per cent in the EU.[11] American companies IBM and Oracle rank fourth and fifth largest. The biggest European CSPs, Deutsche Telekom and SAP, only hold about 2 per cent market share each – and their scope is not comparable to their American counterparts. Indeed, as illustrated in Figure 4, the share of European CSPs' cloud revenue has been diminishing in the past five years and is now below 15 per cent.

The strategic advantage of American CSPs lies in their all-encompassing offering of services and features. Functioning much like an 'IKEA for computing', they are a one-stop shop where customers can buy all the IT services they might possibly need – ranging from hard infrastructure to artificial intelligence tools.[12] As illustrated in Figure 5, their European counterparts, by contrast, are only able to offer subsets of cloud services.

The difference in scale and scope between American and European CSPs is so vast that most in the industry are of the view that there is no real competition between them – and that it is too late to change the situation. A loose analogy with the aeronautical industry illustrates the current state of affairs in cloud services: if Europe did not have Airbus to compete with Boeing, how long would it take today to build such an enterprise?

The EU and its Member States must now consider which dependencies make for critical vulnerabilities, and how to reduce or manage those. This involves acting on the question: (how) can European CSPs reach the scale, breadth of services and relevance required to ensure the EU's digital economic security? Or, given the enormous gap between European and American CSPs, can Europe still build 'minimum viable clouds' – that is, trusted European cloud environments with sufficient and secure capabilities to host and run European governments' most sensitive data?

To inform the answers to these key questions, the next section looks at recent developments and initiatives in the cloud domain in Europe – and specifically, the Netherlands – and in other countries of relevance, namely the United States.

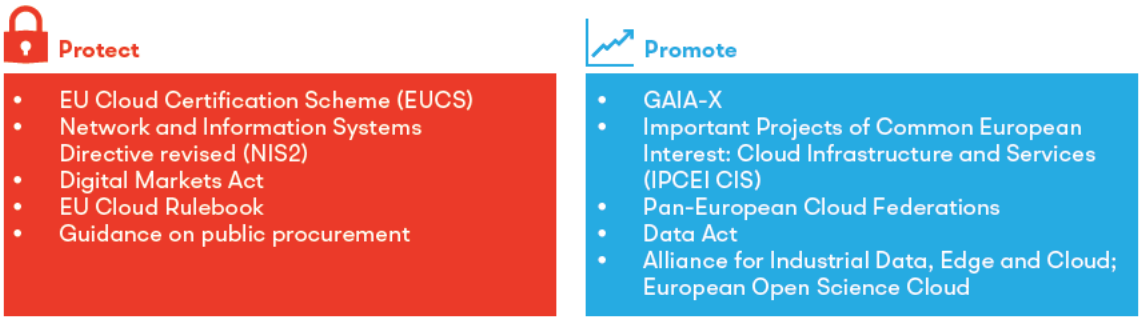
Recent developments and initiatives

Aiming to enhance European cloud sovereignty, the EU and its Member State governments in recent years have started to act, broadly speaking, on two policy lines. First, the aim is to

11 Synergy Research Group, *European cloud providers continue to grow but still lose market share*, 27 September 2022.

12 Bert Hubert, *Taking the Airbus to the IKEA cloud*, 11 January 2024.

Figure 6 **EU policies and initiatives with an impact on cloud services, set against the Protect–Promote framework**



Source: authors' compilation

'protect' both consumers and European cloud businesses from the dominating American cloud players – including addressing concerns on data protection and privacy, cyberattacks, and unlawful access to data by foreign parties to European citizens, businesses and governments. In addition, they also seek to 'promote' the European cloud ecosystem to grow. Figure 6 presents the main EU regulations and initiatives related to cloud services, set against the Protect–Promote analytical framework that will be elaborated upon below.[13]

Protect

Seeking to enhance European cloud sovereignty, the EU is preparing the EU Cybersecurity Scheme for Cloud Services (EUCS). With this voluntary certification scheme – developed within the European Cybersecurity Act (CSA) – the EU aims to harmonise the security of cloud services with EU regulations.[14] Negotiations about the new scheme illustrate the EU's growing attention for cloud sovereignty. At the same time, they are a vivid illustration of divergences between EU Member States on what this should entail.

The EUCS foresees four assurance levels for CSPs: high plus; high; substantial; and basic.[15] It requires cloud contracts to be governed by an EU country's law for all EUCS assurance levels. For the 'high plus' and 'high' levels, data must be located within the EU. The new level of 'high plus' is designed to be met exclusively by Europe-based CSPs, and aims at building trust, unlocking growth and enhancing European sovereignty. Crucial herein is the extent to which the European subsidiary of a cloud provider can be considered as falling under the parent company's or group's control. France, in particular, pushed for a clause that would require CSPs to be operated only by EU-based companies, with no non-European entity exerting effective control. A group of EU Member States, led by the Netherlands and also including Germany, successfully pushed for a softening of this text.[16]

Figure 7 summarises the links between the cloud sovereignty layers proposed in Figure 3 and the draft EUCS assurance levels.

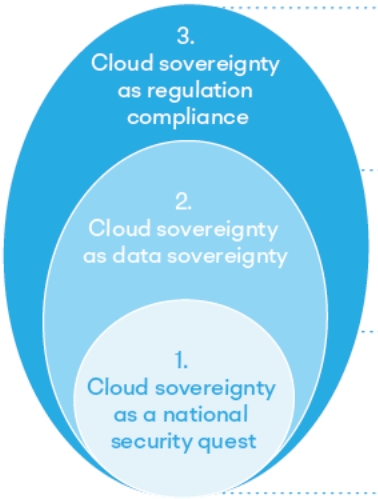
13 Maaike Okano-Heijmans, *Open strategic autonomy: the digital dimension*, January 2023.

14 The CSA is a cybersecurity certification framework to standardise information and communication technology (ICT) products, services and processes. In place since 28 June 2021, implementation is monitored by the EU agency for cybersecurity (ENISA). See: European Commission, *The EU Cybersecurity Act*, April 2023.

15 See: ENISA.

16 The new text adds the possibility for CSPs to 'demonstrate that they have put in place effective technical, organisational and legal measures that prevent non-EU companies linked with the cloud provider from exerting a decisive influence in decisions related to investigation requests'. See: Euractiv, *EU cloud scheme slightly tones down sovereignty requirements*, 22 November 2023.

Figure 7 The draft EU Cloud Certification Scheme (EUCS) levels in relation to cloud sovereignty



Source: authors' compilation based on the EUCS draft text of November 2023

While the EUCS – if enacted – can be expected to enhance Europe's cloud sovereignty, two challenges persist. First, European CSPs are unlikely to obtain certification for the 'high plus' assurance level, because of the vast resources and effort required. Second, the potential extraterritorial effect of US legislation seems to undermine EU regulations that seek to strengthen cloud sovereignty. As detailed in Box 2 below, three US regulations in particular enable the US government to force American CSPs to hand over their customers' data: the Clarifying Lawful Overseas Use of Data Act (CLOUD Act); the Foreign Intelligence Surveillance Act (FISA); and the Defense Production Act.

This suggests that the EU cannot just regulate itself out of the problem: diversification of European solutions is not a luxury but a necessity. Hence, it is in EU governments' interest to invest in developing European 'minimum viable clouds' – that is, trusted cloud environments in all EU Member States that meet the necessary technical requirements to operationalise the vision of cloud sovereignty as a national security quest.

European capitals could opt to use tailored public procurement tools to invest in European CSPs and co-create European cloud solutions that are compatible with the core (high plus) assurance level of the EUCS, which covers state-secret information or intelligence services data. Since the trend among CSPs to replace on-premise solutions with cloud alternatives seems inevitable in the long term, investments in European cloud solutions are a necessary step to uphold European cloud sovereignty.

Although not directly related to cloud sovereignty, the proposed expansion of the Network and Information Security Directive (NIS) is also important for cloud services. NIS2 provides a framework for the level of cybersecurity that secure and trustable CSPs must have and requires that they establish incident response plans and promptly notify authorities and affected parties in the event of a breach.

To limit the market power of Big Tech companies and to encourage a level playing field, the European Commission in 2022 adopted the Digital Markets Act (DMA). The DMA is designed to protect European companies and platforms

Box 2. The CLOUD Act, FISA and the Defense Production Act

*The **CLOUD Act**, adopted by the US Congress in 2018, obliges 'US service providers to preserve and produce data they control regardless of where it is stored'.*

*The **FISA** is a US federal law that governs the surveillance and collection of foreign intelligence information. It defines foreign intelligence information as 'information relating to a foreign power or that generally concerns the ability of the United States to protect against international terrorism or a potential attack by a foreign power or agent of a foreign power'.*

A legal expert analysis made for the Dutch Cybersecurity Centrum (NCSC) concludes that only in two conditions can EU entities avoid falling under the CLOUD Act, even if located outside the US:

> *(1) If there is no 'corporate relation to any company with a presence in the US (such as a US subsidiary)' and if there are 'no sufficient contacts with the US such that it is reasonable for the US to assert jurisdiction over the EU Entity/non-US entity';*
> *(2) When there is a 'corporate relationship with a company based in the US, the US company must not have possession, custody, or control over the data that is stored in the EU. In no case can the EU Entity have a US parent company, as the parent would be considered to have possession of or control over the data of its subsidiary'.*

The analysis goes as far as to recommend CSPs that wish to be completely out of the CLOUD Act's scope 'not to employ US nationals who have access to relevant data'.

*The **Defense Production Act**, which was first enacted in 1950 during the Korean War, gives the US President authority to expand and speed up the supply of materials and services from the US industrial base as needed to promote the national defence. Although not specifically mentioning cloud services, the Act is broad in scope and flexible enough to accommodate it, should an attack on American CSPs occur. Theoretically, such an event could have negative consequences in the availability of cloud services to European customers and governments, as American needs would be prioritised.*

See: Eurojust, *The CLOUD Act*, 22 December 2022; US Congressional Research Service, *Foreign Intelligence Surveillance Act (FISA): an overview*, 10 March 2020; US Federal Bureau of Investigation, *Foreign Intelligence Surveillance Act (FISA) and Section 702: news and updates*; Dutch Ministry of Justice and Security – National Cyber Security Centre, *Memo Cloud Act*, 16 August 2022.

from antitrust mechanisms by American Big Tech companies. None of the six so-called gatekeepers that fall within the DMA are European.[17] Since the definition of gatekeeper does not cover the specifics of cloud services at the infrastructure and platform layers, the DMA applies to cloud services only insofar as these function as (large) online platform gatekeepers. As such, the DMA is unlikely to protect, or to help promote, European CSPs – or indeed to enhance cloud sovereignty.

Beyond regulatory action, the EU seeks to foster cloud sovereignty by two other forthcoming initiatives: the Guidance on public procurement of data-processing services; and the EU Cloud Rulebook. The Guidance will indicate

17 A gatekeeper is a platform or a service with a monthly user base of 45 million (corresponding to 10 per cent of the EU's population), among other conditions. European Commission, *Digital Markets Act: Commission designates six gatekeepers*, 6 September 2023.

best practices and define common European standards and requirements for the public procurement of data-processing services. The Rulebook aims to create a single European framework of binding and non-binding rules for both cloud service users and providers.[18] Both initiatives are being developed together with the European Alliance for Industrial Data, Edge and Cloud, which includes EU Member States' representatives.[19] These blueprints aim to support European governments and users to procure, operate and interact safely with CSPs; and to set best practices for CSPs in terms of security, energy efficiency, interoperability and competition.

In the Netherlands, certain government services have been allowed to use public cloud services since the 2022 update of the government-wide cloud policy.[20] State-secret classified information and the whole Dutch Ministry of Defence fall outside this policy's scope. The policy bans suppliers or services from countries with an active cyber programme aimed at Dutch interests. Notably, each department is required to formulate its own cloud migration strategy.[21] Such dispersion has a negative impact on the leverage and negotiation power that could otherwise be achieved. Moreover, the distance between the IT staff responsible for implementing government cloud migration and the policymakers responsible for foreign and national security interests is a challenge. IT staff looking for cost-efficiency or proven and state-of-the-art solutions are more prone to prefer established CSPs, without much consideration of their country of origin. If governments are to be serious about cloud sovereignty, they should sensitise their IT teams and engineers to geopolitical considerations and educate policymakers about technological developments in order to balance the diverging visions and responsibilities of both sides.

Promote

Seeking to strengthen the position of European CSPs in the cloud market, the EU is focusing on two lines of action. The first is about fostering and empowering European solutions. Second, the EU is seeking to advance greater interoperability between CSPs, in order to avoid vendor lock-in with the big American players.[22]

The first axis is best exemplified by initiatives such as Gaia-X and the Important Project of Common European Interest on Cloud Infrastructure and Services (IPCEI CIS), which developed around the notion of community cloud. Gaia-X was initiated in 2020 to build an ecosystem of multiple community clouds linking end-users and businesses, creating a safe environment for sharing data. Little progress has been achieved, however, and few in the industry still believe that Gaia-X can deliver on its promise. Differences between government and industry players in the rationale and structure of Gaia-X played a big – and negative – role in this development: while some wished it would be a tool to enhance technology sovereignty, others pushed to engage US hyperscalers in the project. French cloud provider Scaleway left the project citing, among others, foreign influence reasons.[23]

The group of fourteen EU Member States, led by France and Germany and including the Netherlands, that are cooperating in the IPCEI CIS has similarly been struggling to deliver since its creation in 2020.[24] Projects developed within this framework are geared towards

18 The Rulebook is likely to include, among other things, standard contractual clauses for cloud computing contracts. See: European Commission, *Practical guidance for businesses on how to process mixed datasets*, 29 May 2019.

19 European Commission, *European Alliance for Industrial Data*, Edge and Cloud.

20 Dutch Ministry of Foreign Affairs, *Rijksbreed cloudbeleid 2022*, 29 August 2022 (in Dutch).

21 This is done under the guidance and implementation support of the Dutch central government's Chief Information Office (CIO Rijk).

22 Vendor lock-in occurs when a company faces (severe) challenges in switching to a different provider.

23 Euractiv, *Cracks appear as Gaia-X celebrates its progress*, 19 November 2021.

24 German Federal Ministry for Economic Affairs and Climate Action, *IPCEI next generation cloud infrastructures and services: Europe on the path to the cloud infrastructure of the future*.

data-processing infrastructure and tools for data sharing, via federated and secure cloud infrastructure and services. However, these projects are still limited in terms of visibility, scope and concrete results.

Alongside attempts to build European-wide solutions, the EU has in recent years focused on ensuring greater interoperability between CSPs. Instrumental to this end is the European Data Act, designed to regulate data sharing and usage within the EU. If implemented correctly following its adoption in November 2023, the European Data Act will simplify the transfer of data and applications between different CSPs, diminishing barriers for users to switch more easily between them and avoid vendor lock-in.

Two other initiatives stand out for aiming to promote a greater European role in the cloud landscape: the Alliance for Industrial Data, Edge and Cloud; and the European Open Science Cloud. The Alliance for Industrial Data, Edge and Cloud is a forum for European companies to co-create and develop ideas to increase Europe's share in the cloud space, facilitated by the European Commission.[25] The European Open Science Cloud is a pan-European initiative that aims to provide researchers, the private sector and citizens with access to a federated environment, where they can use data and services for research, innovation and educational purposes.[26]

An underexplored mechanism to stimulate European CSPs is public procurement. Rather than being driven only by technical considerations, public procurement of cloud services should also include clauses related to diversity and business continuity. On the one hand, such processes may allow governments to test and experiment with cloud services, as they initiate their cloud journeys. On the other hand, European CSPs would have the chance and the incentive to develop their technical solutions further. Public procurement to promote the industrial base has been widely used in the United States for decades, and American CSPs themselves have benefited greatly from the contracts they have been awarded. Long-term thinking may recommend European governments to follow a similar approach, to reduce dependencies that otherwise will only increase.

As a leading digital EU Member State, the Netherlands has defined the goal to maintain its engagement with all the major aforementioned EU initiatives: to quickly implement the Data Act, and to continue its participation in Gaia-X, IPCEI CIS and in the European Alliance for Industrial Data, Edge and Cloud. In Brussels, the Netherlands is pushing to assign a Dutch seat in a European standardisation body on cloud interoperability or data standards. At home, the Netherlands has allocated funds to national projects like the establishment of a Centre of Excellence for Data and Cloud, through the Dutch Applied Science organisation TNO. The development of national sectoral data-sharing legislation is also underway, as well as research into possible mitigating measures to reduce cloud dependency in the Netherlands – including the possibility and feasibility of a sovereign Dutch cloud.

Concluding remarks

Cloud services have changed how businesses and other organisations manage their IT infrastructure, applications and data. The European cloud market is dominated by American CSPs, and the strategic advantage those have in relation to European alternatives seems insurmountable – both in scale and the scope of services offered.

The EU sets the global benchmark in terms of regulation, but referees do not win matches. The EU has been able to introduce guardrails, by forcing the American CSPs to host their hardware – and hence, the physical location of the data – in Europe. But we cannot 'regulate ourselves' out of current cloud dependencies. Either we take this last window of opportunity

25 European Commission, European Alliance for Industrial Data, Edge and Cloud: shaping Europe's digital future, 4 July 2023.

26 European Open Science Cloud, About.

to boost European CSPs, such as by using public procurement to develop minimum viable clouds in EU Member States, or we have to learn to live with the circumstance that the benefit of using the cloud involves giving away full ownership of our data. Since such risks are not quantifiable in numbers, governments have to consider the associated political risks.

The apparent consensus about the shift of EU governments – including the Netherlands – to cloud services should not be taken lightly. European capitals have to consider national security concerns seriously. Public discussion about what such migration represents, and about the roadmap to do so, is desirable. Furthermore, the notion of cloud sovereignty is still underexplored at the EU level. Member States have different interpretations of cloud sovereignty, driven by different national (security and economic) interests. This points to yet another challenge: the need to invest in intra-European trust, which is required to strengthen European CSPs. The question of how to ensure that EU Member States trust each other more than they trust the US is yet to be addressed.

The future for governments' IT management will lie in hybrid cloud solutions, based on a combined approach that considers the three layers of sovereignty proposed in this policy brief. Data classification is a sensitive and key process, which will determine the technical solutions chosen to store data and ultimately the security of such data.

But cloud is no silver bullet. Accountability and security are shared responsibilities of CSPs and their customers. Nevertheless, companies and governments are ultimately responsible for implementing their systems and securing their data themselves. Cloud security features often have high and unexpected cash costs. Knowledge and resources capable of managing such hybrid (and multicloud) systems are thus of paramount importance to ensure any successful cloud migration. Furthermore, greater engagement between policymaking circles and government IT teams is fundamental to bridge the current gap in priorities and preferences between those responsible for securing national interests and those responsible for IT systems.

Cloud sovereignty is not only about questioning to what extent EU Member States trust the US government and American companies – given the potential extraterritorial effects of US national security legislation – but is also about diversification of providers, having a proper regulatory environment in place, and developing our own capabilities and resources.

About the Clingendael Institute
Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84

@clingendaelorg
The Clingendael Institute
The Clingendael Institute
clingendael_institute
Clingendael Institute
Newsletter

About the authors

Alexandre Gomes is a Research Fellow at the Netherlands Institute of International Relations 'Clingendael' in The Hague, where he is part of the EU and Global Affairs Unit and of the 'Geopolitics of Technology and Digitalisation' programme. His research focuses on the role of technology in geopolitics.

Maaike Okano-Heijmans is a Senior Research Fellow at the Netherlands Institute of International Relations 'Clingendael' in The Hague, where she leads the 'Geopolitics of Technology and Digitalisation' programme. She is also a Visiting Lecturer in the Master of Science in International Relations and Diplomacy (MIRD) programme of the University of Leiden.

Disclaimer: Research for, and the production of, this policy brief was commissioned by the Netherlands National Communication Security Authority (NLNCSA), part of the General Intelligence and Security Service (AIVD). Responsibility for the content and the opinions expressed rests solely with the authors and does not constitute, nor should be construed as, an endorsement by NLNCSA.