CENTRE FOR EUROPEAN REFORM
LONDON ★ BRUSSELS ★ BERLIN

Insight

Should the EU's tech sovereignty package make Europe richer or safer?

by Zach Meyers, 7 July 2026

The European Commission's Tech Sovereignty Package focuses on mitigating risk, rather than actively promoting European technological strengths.

The US government has just prohibited the American AI firm Anthropic from allowing foreigners access to its cutting-edge Fable and Mythos models, fearing they would be used for cybersecurity attacks. The episode is only the latest reminder that Europe is heavily dependent on foreign digital technologies – from AI and cloud computing to online platforms. Access can be constrained by political decisions taken elsewhere, leaving EU countries vulnerable to foreign pressure. The US has previously imposed sanctions on officials of the International Criminal Court, for example – cutting off judges' access to electronic payments and services, severely impacting their everyday life. Under pressure from Washington, US payment systems suspended services for WikiLeaks in 2010, blocking Europeans from making donations – illustrating that the EU's dependencies go far beyond AI.

But reducing dependencies is only half the challenge. At the same time, Europe faces a 'competitiveness crisis': its low economic growth is consistently outpaced by the US. Economists often agree this is largely driven by European businesses being too slow to adopt new technologies, and Europe's struggle to generate globally successful, high-tech firms.

This creates dilemmas. How far can the EU press its companies and governments to cut out foreign dependencies, without compromising the bloc's competitiveness? And what is the right balance between building 'defensive' domestic capabilities for security and resilience, and supporting the next generation of innovators?

The European Commission recently unveiled its Tech Sovereignty Package: an attempt to grapple with these problems. It promises support for AI and chip-making firms. But its centrepiece is a set of new rules for cloud computing. These rules aim to drive more public sector spending towards IT providers that give

stronger protection to European interests. The rules also reserve some government cloud contracts solely for European providers. The package represents a symbolically significant step towards acknowledging and confronting Europe's tech weaknesses. But it leaves unresolved Europe's strategic dilemma: is Europe trying to become richer or safer, and how should policy-makers balance those objectives when they come into conflict?

The Tech Sovereignty Package at a glance

'Cloud computing' is a service which gives customers access to computing resources like data storage and software remotely. Cloud offers many advantages to customers over running all their own IT infrastructure on their own premises: cloud computing is often cheaper, more easily scalable, and can offer more features and higher levels of cybersecurity. Because of its importance to competitiveness and increasing efficiency, the Commission has set a target of 75 per cent of EU enterprises using the cloud by 2030.

The European cloud computing market is dominated by US companies. The biggest three – Amazon, Google and Microsoft – collectively hold about 70 per cent of the European cloud market. European firms' share has dropped from nearly 30 per cent in 2017 to about half that today. Policy-makers are alarmed, since many firms and public sector organisations are dependent on their cloud provider to access their data and deliver basic business or government functions – making cloud computing a strategic asset.

The proposed Cloud and AI Development Act (CADA), a key part of the Tech Sovereignty Package, aims to mitigate the risks from this situation. The proposal would require member-states to assess the risks of public sector activities which use cloud computing being disrupted – such as by the US president ordering the cessation of services in retaliation for Europe not following his wishes – or of foreign governments snooping on Europeans' data.

Each government activity under CADA must be assigned one of several 'assurance levels', with higher levels used for more sensitive areas like defence. To attain a basic assurance level, which is needed for lower risk use cases, the cloud computing provider must process and store data in the EU. Higher 'assurance levels' would require the cloud computing provider to demonstrate increasingly rigorous independence from third countries.

Foreign firms can qualify for at least some of the assurance levels – particularly if the firm comes from a 'trusted' third country. These countries will probably include close European countries outside the EU, like the UK and Switzerland, and the US. Under CADA, however, the Commission estimates that non-EU cloud computing providers will be excluded from between 1 and 10 per cent of government cloud contracts, depending on how the law is implemented.

What does the Tech Sovereignty package hope to achieve?

The Package as a whole addresses two different types of problem. The first is to manage certain types of risk. Hence, when CADA excludes non-EU companies, this is not justified as a mandate to 'buy European' or to promote European cloud computing firms. Its justification is that it is the only way to sufficiently mitigate the risk of a 'kill switch' or of foreign snooping. This explains why the Commission has emphasised the proposal is not about excluding foreign firms and remains rooted in openness. This framing is pragmatic since – at least compared to alternative approaches the Commission could have

taken – it minimises transatlantic tension, assuages concerns from member-states which are squeamish about protectionism, and should relieve many foreign countries with whom the EU is seeking to deepen its trade relations. It instead positions CADA as comparable to various cybersecurity initiatives which constrain the role of Chinese firms in European tech supply chains.

The second rationale is more French: the Commission describes the Package as delivering a "rapid shift of the EU's posture from a reactive focus on resilience and risk mitigation to an assertive and proactive approach". This seems to echo the calls of some European tech firms seeking more public support (such as through public procurement) to help build Europe's tech base. Initiatives such as EuroStack – a group of European tech executives arguing for a more ambitious tech industrial policy – for instance, have increasingly framed the tech sovereignty challenge in terms of value capture: how can Europe ensure that a greater share of the economic benefits of digital technologies accrues to European firms, investors and workers?

Of these two rationales, the proposal leans more towards the 'risk management' approach. This is not only because the CADA rules on cloud computing are oriented entirely around mitigating two specific risks (the 'kill switch' and foreign authorities' access to data) – but also because the parts of the package that aim to actively support other parts of the European tech industry like chips and AI lack much new funding. Whether the package will substantially mitigate risk is an open question. Insulating a small proportion of public cloud computing contracts from foreign interference would still leave Europe open to enormous economic and social disruption. And the application of the rules to AI seems unclear, particularly given Europe's weakness in building cutting-edge language models. Would this 'light touch' approach to risk mitigation lead to more economic competitiveness for European cloud companies or the broader European economy?

The impact on European cloud companies

In theory, CADA could support European cloud companies. Pushing some public sector demand to European cloud firms could help those firms enjoy economies of scale, build their reputation, attract more capital, gain know-how, and eventually become competitive with the US giants. However, delivering this outcome is not guaranteed.

First, CADA's positive impact would be modest. Public procurement is a relatively slim proportion of the overall demand for cloud services in Europe. For example, the European Commission recently concluded a €180 million procurement exercise for sovereign cloud solutions. In comparison, member-states have agreements worth at least €10.8 billion with the US cloud giants, and the size of the combined public and private cloud computing combined is expected to reach €200 billion by 2028. Even within that subsection of the public sector cloud market, European firms will likely only enjoy a slither of guaranteed demand. The proposal does allow the Commission to extend the rules to private sector firms in areas of 'high criticality' – such as for privatised utilities like energy systems – but any extension would also be tightly targeted and, as noted below, restricting private sector purchasing decisions would come with its own risks.

Second, similar national schemes to CADA have simply led the EU's largest countries to benefit their own national cloud providers, rather than one or two genuinely European champions. CADA will be implemented largely by member-states themselves, which means many may choose to buy American,

and others may choose the best national provider rather than a European solution. A perception that CADA artificially advantages European companies means that European governments then feel more empowered to pursue 'buy national' rules. The EU will need to consider how to avoid continued national fragmentation, which would lead to European cloud companies needlessly missing out on scale.

Third, for European cloud companies aiming to achieve the highest assurance levels (and therefore compete for contracts where foreign firms are entirely excluded), the package imposes large costs. The European Commission has partly recognised this: in a recent exercise to procure 'sovereign' cloud services, the Commission found that no European firms could meet the most stringent requirements of having no non-European controlled hardware among their components. The CADA proposal relaxes this requirement. CADA still demands, however, that European providers which want the most sensitive contracts must ensure no foreign country or company controls "the design, development, maintenance, and evolution" of any software components. Today, European cloud firms are unlikely to be able to be able to provide this assurance without significant work. At best, this will impose a large burden on European cloud computing companies to access a relatively small part of the market. At worst, it could lead to member-states exercising a right to ignore CADA's rules on the basis that they impose 'disproportionate cost'.

In the meantime, US cloud companies have been designing their own 'sovereign cloud solutions'. These include various commitments – such as to keep data in Europe, use encryption technologies to prevent the cloud provider seeing the customer's data (and handing it over to foreign governments), and sometimes to roll out services through EU-controlled joint ventures with local firms. Given their experience and resources, it seems plausible that CADA's rules could largely prove easier in most cases for US firms to meet than for smaller European companies, outside of the small minority of contracts reserved specifically for European firms.

So while CADA provides a small tangible benefit for European cloud providers, the costs and risks it imposes mean that the overall effect is less certain. If competitiveness of the European tech industry was the primary goal, then CADA would likely look very different – either more explicitly adopting a 'buy European' approach for cloud, or focusing less on reducing the EU's cloud dependencies and more on building out Europe's tech strengths.

Does the package support broader European innovation objectives?

Outside the European cloud sector, and looking at the broader European tech ecosystem, a similar dilemma exists. Many member-states and the Commission clearly wish to shift demand towards European tech services, by encouraging customers to change their buying behaviour. However, currently, European firms rely heavily on US chips, AI, cloud, operating systems and applications. Since many European tech services cannot currently offer the same functionality or value-for-money as US equivalents, pushing European businesses to buy European tech could in some cases drive down those firms' competitiveness. Supporting EU tech firms in this way is not necessarily wrong. But it involves a bet that more demand will help European tech firms become more efficient, innovative and – eventually – fully competitive vis-à-vis their US equivalents. It also involves a bet that the benefit to EU tech firms will outweigh any damaged competitiveness European customers have to suffer in the meantime.

Whether the short-term pain creates long-term gain will depend on various factors, such as the type of technology, how strong existing European players providing that technology are, and the extent

to which extra demand would provide EU tech firms with a meaningful 'leg up'. Absent a detailed assessment, the Package takes a wise approach by focusing almost solely on public procurement, rather than interfering in private firms' purchasing decisions – which could reduce those firms' competitiveness. It also takes a wise approach by focusing at first on one product, cloud computing.

Conclusion

The Commission has taken a bold, and much needed, step by proposing a definition of 'technological sovereignty' – and by recognising that Europe needs drastic change to gain a meaningful position in high-tech sectors. The Tech Sovereignty Package reveals two different ways of thinking about the problem: mitigating dependencies, on the one hand, and strengthening Europe's own competitiveness and technological capabilities, on the other. The difficulty for policy-makers is that measures designed to achieve one objective do not always advance – and sometimes are in conflict with – the other.

The two approaches can be aligned, however, if the focus of sovereignty shifts away from managing risk, and more towards maximising European strengths. The global sector is characterised by regional specialisation, which means all countries – even the US – have dependencies on other parts of the world. Europe's weakness is that it commercialises too few disruptive technologies of its own – so its technological dependencies are one-sided, and an antagonistic US administration has little need to factor in European responses to its decision-making. Europe can address this by focusing more on how to build out its existing strengths and develop new capabilities which will be indispensable parts of global supply chains – rather than focusing solely on replicating foreign services. Ironically, that can be a tough message for many of today's European tech firms: only a small minority of these firms are likely to prove globally successful and indispensable, and industrial policy should not try to indefinitely support all of them.

Shifting public sector demand can be a stopgap to help mitigate risks, and in some cases it may also help build support for a stronger EU tech sector. But – as the Tech Sovereignty Package acknowledges – much more important are fundamental reforms to boost European innovation – such as building deeper capital markets and allowing innovative firms more labour flexibility and the ability to scale quickly across the EU. The success of the Package should not be judged on whether European tech firms can carve out a marginally larger market position replicating US services. The real test is whether the Commission's strategy allows Europe to dominate globally in technologies of the future.

Zach Meyers is director of research at CERRE, the Centre on Regulation in Europe, and a non-resident associate fellow at the Centre for European Reform.