SAMF.SUBSTACK.COM – 5 MARZO 2026

# Sovereignty for sale

*di Sam Freedman*

Elon Musk's decision to block Russia from using Starlink satellites has proved a serious setback for Moscow; hampering troops' use of drones and artillery. Putin's reliance on tech controlled by a foreign company has left him badly exposed.

The Ukrainians have had their own issues with Starlink. Musk provided thousands of terminals in the first days of the war, after Russia blocked access to the Viasat satellite communications systems. But since then he's limited Ukraine's ability to use it to attack Russian territory; starting after he spoke to Putin in autumn 2022.

Musk's ability to change the course of the conflict raises questions that go far beyond Ukraine. Private businesses have a long history of participating in wars, and providing public services, as contractors and suppliers. But the power that major tech companies have over nation states is something new.[1]

Even the US is dependent on Musk's SpaceX, which now controls two thirds of all global low earth orbit satellites, and performs the majority of the world's annual orbital launches. NASA needs its rockets for resupplying the International Space Station, and Starlink is increasingly integrated into military equipment (as we've seen in Iran).

For the Americans the risk is in exposure to a single point of failure rather than sovereignty. SpaceX is a US company and, in extremis, the government can force it to comply via regulation or economic threat (as they are currently trying to do with Anthropic over its insistence on retaining control over the use of its AI tools).[2] For other countries, though, reliance on foreign companies is a serious threat to independence, as Russia and Ukraine have found.

The risk goes well beyond SpaceX. Tech firms are integrated into military and governmental systems worldwide; as fundamental to the functioning of societies as

water or electricity. Trump's increasing disdain for allies has pushed this issue up the agenda in Europe, where debates about "tech sovereignty" are increasingly heated. In the UK we are particularly exposed. Governments here have blocked Chinese companies from providing critical infrastructure but to date have been less worried about reliance on US firms, and indeed are continuing to court them in their search for economic growth.[3] But the problem is becoming hard to ignore.

So in the rest of this post I'll look at the key vulnerabilities created by state dependence on tech companies in the UK and how other governments are starting to mitigate these. I'll finish with some thoughts on steps we should be taking.

**UK exposure**

In Britain, Palantir is the company most often identified with sovereignty risks due to its increasingly prominent role in managing data for the NHS, military and police. Its leadership is also openly political, with close ties to the Trump administration, making the danger more obvious. ICE's use of Palantir technology for its brutal crackdowns in American cities, while CEO Alex Karp makes ever more alarming public statements, hasn't helped.[4]

In a recent article David Allen Green set out how Palantir has managed to gain so much influence over military operations in the UK, using the classic "land and expand" sales technique. They secured an initial £75 million contract in 2022 to integrate their software with MoD systems so as to make better operational use of data. This was done without a competition, presumably because Palantir were able to argue no one else could provide these services on the same timescale. Once MoD systems were dependent on the company's software they were tied in. Another contract was awarded in 2025 for £240 million, also without a competition, because, according to the official notice:

"MoD's data analytics capabilities use Palantir data analytics architecture that only Palantir is able licence, and which only Palantir has the design familiarity and technical expertise to fully support."

As Green notes it's not clear why this new contract, for the same number of years and a similar service, is three times more expensive. There may be good reasons –

including the greater emphasis on digital warfare in the most recent Strategic Defence Review. But either way the MoD seems to have had little choice but to continue with the partnership.

Something similar happened with the NHS. Palantir "landed" by providing pro bono support during Covid to improve central oversight of limited resources like ventilators and protective equipment. Success here led to a series of further contracts and a knowledge of NHS data that helped them secure a £330 million deal to run a "federated data platform" (FDP). This identifies ways to use hospital trust's existing data to boost efficiency by combining databases that were sitting separately. (For instance, it has helped trusts clean their waiting lists by finding patients who are on it twice, or have died – this accounts for around two thirds of the fall in elective waiting lists since Labour came to power).

There is some unhappiness within the NHS over the value of the FDP – around half of trusts are still not using it – but even if we assume it works well, the Department for Health has the same problem as the MoD. When the initial seven year contract ends the NHS will be dependent on Palantir technology and will need to sign on again, at a potentially higher price, to keep the FDP going. And the company will be in prime position to win other data related contracts.

Being locked-in to these deals, at rising prices, is bad in itself (though not an entirely new problem – as I discuss in my book one of the reasons for British state failure is an overdependence on a small number of private companies).

But it is also threatens sovereignty in a way that previous procurement failures do not. Departments keep giving contracts to Capita and Serco, regardless of performance, because there's often no one else who can provide outsourced services. These companies are, though, ultimately dependent on the British government to survive, and if necessary the state can step in to cover, as when Carillion collapsed. Whereas Palantir's control over MoD or NHS data gives them leverage over systems that no one else has the capability to support.

Cloud computing is another point of weakness for the British state, exacerbated by procurement failures. 60% of public sector IT systems now operate on the cloud and

around 80% of the these rely on just two provides: Microsoft and Amazon Web Services (AWS). A lot of contracts for cloud services were agreed without competition and, again, once locked in its difficult to move without incurring significant cost.

This represents a significant risk, regardless of sovereignty concerns, because a major outage at one provider, due to a hack or damage to a cable, could knock out 30% of the public sector for a considerable period. But it also gives these companies, and the US government, enormous power over the British state should they wish to use it, especially as there are no national cloud providers. Trump has a number of tools he could use to force US companies to disable services in other countries, including export controls and emergency powers. His 2018 Cloud Act allows the American government to demand any data held by companies under US jurisdiction, even if that data is held abroad.

The French government has been more active in mitigating these risks, by building up a domestic cloud service (OVHcloud), which is the largest provider for the public sector there. By contrast our potential domestic alternative, UKCloud, went bust in 2022.

All of these risks are further heightened by the rapidly growing importance of AI, given all the major LLMs are US based. The UK has an impressive array of AI startups, led by talented people, but they are usually dependent on underlying US technology, and the best are acquired by US companies due to a lack of domestic funding for scale. There remains much uncertainty about the extent to which AI will transform the labour market and society, or the speed with which it will do so. But if the more bullish projections are even partially true this is an urgent issue.

The government did set up a "sovereign AI unit" last year, with £500 million of funding to seed British companies and agreements to work with US firms on security concerns. Earlier this week it announced £40 million for a state-backed AI "blue sky" research lab. But these interventions feel underpowered given the extent of the challenge. It can do little to mitigate the dependence on US infrastructure without both regulation and coordinated investment across the UK public sector. There was an agreement signed with chipmaker Nvidia last year through which they will provide chips to a new

company called Nscale to build datacentres in the UK. But it turns out Nscale is owned by Australians. Similarly the MoD has signed a contract with Google to build a "sovereign cloud" service for defence based in UK datacentres, but it's still dependent on a US company.

**The debate elsewhere**

France is not the only European country to take a more robust approach to the challenge of tech sovereignty. An investigation published last month revealed the Swiss have turned down multiple advances from Palantir over a seven year period, due to concerns about value and data security. An internal report from the Swiss army highlighted the risk of confidential military data being passed to US intelligence agencies. Intriguingly, the investigation also found that Palantir made the same offer to the Swiss health authorities to support them during Covid as they did in the UK, but they were turned down. (Palantir are now suing the magazine that published the report).

In Germany, Palantir's progress has been hampered by a 2023 constitutional court ruling that put restrictions on Hamburg state government's use of their policing technology. This wasn't about the company per se, but rather data privacy issues. It has, though, led to a lot of pushback against other states working with them. So far the federal police have not contracted with them, in part due to public concerns.

Palantir have made some progress in Europe, working with a number of police forces, including the French domestic intelligence services and other health agencies in Greece and the Netherlands (in both cases they also used Covid as their "in") but generally have had a lot less joy than in the US. Karp recently complained about "lack of adoption in Canada…and in Europe" with a growing proportion of the companies' revenue coming from the US.

European concerns extend beyond data protection, to the wider challenge of sovereignty over tech infrastructure. It was a hot topic at last month's Munich Security Conference, with Emmanuel Macron talking of independence in defence and technology and Ursula von der Leyden promising a "tech sovereignty package" in the Spring.

But the EU has a similar problem to the UK in that there are few companies, like OVHcloud, able to provide these services. One report estimates that 80% of digital products and services in the EU are provided by non-EU companies. There is a big debate as to whether the solution to this is to try and create sovereign infrastructure or to put in place regulation that forces US companies to abide by different rules.

Until recently regulation has been the focus, with legislation like the Digital Services Act (2022) to police social media companies, to the chagrin of the Trump administration and owners like Musk (whose X platform has already been fined).[5] An Artificial Intelligence Act, providing similar rules around AI, is being phased in at the moment.

Increasingly, though, the EU is taking a more direct approach, as regulation can be circumvented, or undermined by US pressure. In the absence of EU alternatives, sanctions lack teeth. Initial measures have focused on infrastructure. The first foray was the EU Chips Act in 2023, which was partly a response to Joe Biden's investment in US chipmaking. In the last year we've seen an "InvestAI" initiative, to try and corral €200 billion in private investment into infrastructure, including four AI "gigafactories" that would allow European businesses and researchers to develop models under EU jurisdiction. Deutsche Telekom has already opened the first of these of Munich.

There's also an upcoming "Cloud and AI Development Act" that will aim to deal with planning and other constraints on building data centres. Another Act will provide funding for quantum technologies. And there is pressure to go further. One group has proposed a so-called "Eurostack" that would involve building a complete sovereign foundational backbone from chip manufacturing, to cloud services and network infrastructure.

The big US companies are taking different approaches to this challenge. Many of the major players like AWS, Microsoft, Google are seeking to assuage concerns by taking measures to protect data and invest in national infrastructure. They argue, unsurprisingly, that overly protectionist approaches will harm competitiveness and aren't necessary. At the Munich Security Conference these companies and a dozen others launched the "trusted tech alliance" to lobby for this position.

Meanwhile, more insurgent companies like X are taking a more hostile approach, complaining about the burdens of EU regulation while looking to their friends in the Trump administration to threaten Europe with dire consequences if US tech companies are blocked. While the American government is acting with such disdain for European interests it seems likely the EU will continue to try and push for sovereignty, while working, out of necessity, with non-EU companies that seem like they want to be responsible.

**Taking sovereignty seriously**

Whether or not these EU initiatives succeed, the UK will be stuck outside them. Talk to senior people in the government and they will argue this gives us an advantage, as we can offer US companies a more hospitable environment for investment. They see this as critical to growing the economy, as illustrated by the appointment of a former Amazon executive to Chair the Competition and Markets Authority (CMA).

There's a fatalism about the sovereignty risks if the US government turns on us. Our military and intelligence services are so intertwined with the Americans that we're already too vulnerable for meaningful mitigation in the short to medium term, so, the argument goes, we might as well lean into the risk. European militaries are also dependent on US equipment, but not quite to the same extent (the French, in particular, have always made more of an effort to retain autonomy over weaponry, including their nuclear deterrent, emphasised in Macron's speech on defence this week).

But our uniquely exposed position doesn't mean we should do nothing to mitigate. The lack of domestic firms and infrastructure is an unnecessary vulnerability. Academics working on AI at the Bennett School of Public Policy based in Cambridge University have made two policy suggestions that seem eminently achievable as a starting point, without burning our existing relationships or putting growth at risk.

First, they propose mandating a "sovereign public sector" that would see a growing proportion of tech procurement spend across central and local government directed towards UK-owned and based firms (e.g. for cloud computing). By offering a predictable cashflow we could create the conditions for investment into UK

companies and retain talent, with knock on effects for the private sector. That would also leave public services less exposed to a major outage outside of our control.

Secondly, they recommend building a "middle powers" technology alliance (this was before Mark Carney made his speech at Davos urging something similar at a broader level). This could build on the success of the UK's AI Security Institute, creating standards for safety and transparency across a set of markets big enough that US and Chinese companies would need to engage. We need to start somewhere because these challenges are only going to get more acute.

It's also a political opportunity for moderate parties to highlight a major fault line in the radical right. Nationalist parties believe that power should sit at the level of the state and handing it to international organisations – from the EU to the ECHR and the WHO – is the root cause of our problems. Yet at the same time radical right politicians tend to have close ties to the technology companies, like X, that are the most dismissive of national sovereignty concerns.

We're starting to see the fractures created by this contradiction in, say, National Rally in France distancing from MAGA. But in the UK, given sovereignty from the US has historically been less of an issue, politicians like Nigel Farage and Rupert Lowe have not been challenged on this contradiction. Ultimately, though tech sovereignty is a much bigger risk than membership of global organisations. We can always choose to quit international agreements, but if our core infrastructure is run by foreign companies that seeks to do us harm, or exploit us economically, we're stuck.

1 Or at least new in the modern era. Trade monpolies like the East India Company caused plenty of problems for governments in past centuries.

2 To illustrate the point - Anthropic AI is embedded in Palantir's Maven Smart System being used in Iran to identify targets. Trump has said the government will phase out use of Anthropic tech but according to Pentagon sources: "Military commanders have become so dependent on the AI system that if [Anthropic CEO Dario] Amodei directed the military to cease, the Trump administration would use government powers to retain the technology until it can be replaced".

3 In 2020 Chinese company Huawei was blocked from participating in the rollout of 5G due to security concerns and heavy pressure from the US. Subsequently the 2021 National Security and Investment Act has been used to block several attempts by Chinese companies to invest in UK tech companies where that technology could be used for intelligence or military purposes.

4 In the context of the row between Anthropic and the Pentagon, Karp has warned other tech companies they should cooperate with government even on issues like surveillance or risk nationalisation. He's presumably worried about Palantir technology that incorporates Anthropic AI.

5 X was fined 120 million Euros last December for three violations, including deceiving users with a verification system that doesn't provide any verification and failing to make data available t researchers.