Cloud Defence

An exposed European flank

FOTI

Cloud Defence:
An exposed European flank

Executive Summary

As Europe moves to shore up its domestic defence from a growing range of threats, it must ensure that its critical infrastructure can weather geopolitical shocks. One of the major vulnerabilities today is cloud computing, which powers vital systems for Europe's armed forces, from weapons to logistics to personnel management.

The sheer scale of Europe's cloud dependency is hidden from public view because many defence and security contracts are classified; but a review of open contracting databases already indicates significant risk. Our open-systems research shows that **more than three-quarters of European states depend on US Big Tech companies for critical national security functions,** dangerously exposing Europe through this flank. National security systems in 23 of the 28 countries studied seem to rely on US tech, either through direct procurements or via relationships with European firms whose products themselves rely on US cloud providers.

All cloud providers that dominate these European systems—including Google Cloud, Microsoft, and Oracle—have aligned with the Trump administration. US firms hold, by most estimates, close to 80% share of the European cloud market. At the same time, the US government has aggressively pursued user information about its perceived adversaries from American tech companies. This fuels well established European concerns over the US CLOUD Act, which allows US law enforcement to compel American companies to provide access to data stored abroad; in 2022, the Swiss military restricted official communications to Swiss messenger Threema, banning WhatsApp to protect its operations from the Act's extraterritorial reach. But recent events have expanded the "threat model" for European cloud beyond surveillance to the looming potential that access to key services will be lost altogether.

The current state of play exposes Europe's defence and security systems to the same risk of a legal 'kill switch' that disrupted the International Criminal Court last year. It raises the prospect that access to critical defence systems could be used as a geostrategic lever—as the US government now uses its technological dominance as a geopolitical weapon.

With hyperscale cloud firms' profit margins hovering around 40 percent, these contracts also represent a significant diversion of tax revenue toward foreign

businesses. The EU has pledged to invest in domestic defence contractors and increased its overall defence spend to €381bn in 2025 from €262bn in 2022, highlighting an opportunity to redirect funds into boosting Europe's cloud industry.

A transition to sovereign, cost-effective alternatives is possible. Beyond resilience, this would keep strategic investment within Europe and could catalyse a virtuous cycle: state investment in European cloud providers would stimulate more domestic business in Europe.

Migration will take time. However, national authorities are already paving the way by shifting to cloud systems that offer greater sovereignty and resilience.

Reassessing cloud exposure

Recent events illustrate how technological dependencies, once weaponised, can disrupt access to critical services. Since taking office the Trump administration has shown its willingness to do exactly this.

Last year, a Reuters investigation showed that US negotiators suggested they might remove Starlink access for Ukraine if it failed to accede to the terms sought in a minerals deal. That same year, referring to an order from the Trump administration to stop military intelligence sharing, US-based MAXAR Technologies restricted Ukraine's access to key satellite imagery. This 'kill switch' move coincided with President Trump publicly pressing on Ukrainian president Zelensky to accede to a peace deal with Russia's Vladimir Putin. The night after the US halted intelligence sharing, Russian forces attacked Zelenskyy's hometown of Kryvyi Rih, killing at least four people and wounding more than 30. Ukrainian officers described the Maxar shutoff as a bitter blow, reducing their air defences and hampering their drone pilots' ability to hit Russian ammunition depots and other targets.

Another, non-military case of digital kill switches raised public attention last year: Nicolas Guillou, a French judge at the International Criminal Court (ICC), was one of six judges and three prosecutors sanctioned by the Trump administration for authorizing arrest warrants for Israeli Prime Minister Benjamin Netanyahu. Under US sanctions law, American persons or companies, including their overseas subsidiaries, may not provide services to designated individuals. The result is akin to instant banishment from the global financial system. This included Expedia cancelling travel reservations, forcing him to call hotels and request to pay in cash, and an inability to take the train in his hometown. Guillou describes the sanctions' impact on his daily life as like 'being sent back to the 1990s'. The same sanctions allegedly led Microsoft to cancel the ICC's top prosecutor Karim Khan's email. Microsoft has since disputed their responsibility for the events without explaining in detail how Khan's email was disconnected.

The risks of cloud dependency are no technical footnote. It is no longer unthinkable that what happened to Guillou, Khan and fighters in Ukraine could happen to Europe again.

In the wake of January's Greenland crisis, European leaders have voiced the need to shore up this risk. At the Munich Security Conference, European Commission President Ursula von der Leyen acknowledged that Europe had recently taken "some shock therapy" and that "some lines have been crossed that cannot be uncrossed anymore."

But because IT contracting is fragmented - and some quarters of the public sector are resistant to change - the shift to more sovereign tech remains sluggish. Europe must move more boldly and swiftly to reduce these critical dependencies. This need not involve hastening a "rupture" with a longstanding ally. Nor does it imply the immediate elimination of US tech from Europe's public sector 'stack.' Instead, it proceeds from the sensible basis that defence modernisation requires greater resilience and empowering domestic industrial production - including in tech. Cloud should be at the forefront of this effort.

Europe has options

Some European countries have already begun reducing their tech dependencies. Already in 2015, Italy's Ministry of Defence began a migration of 150,000 PC workstations to open source tool LibreOffice. This, the largest migration project at the time, was projected to save 26 - 29 million Euros from budget normally spent on expensive hyperscaler suites, such as Microsoft Office. Last year, the Austrian military finalised a migration of over 16,000 workstations to LibreOffice.

These match similar migrations in other state agencies. In 2024, the German state of Schleswig-Holstein began its migration to open source tools. Baden-Württemberg's 60,000 teachers are using the open source suite OpenDesk, developed by ZenDiS (responsible for digital sovereignty in Germany's public administration). After last year's Microsoft episode, so is the ICC. Meanwhile France, which had already installed LibreOffice on half a million government PCs, is rolling out their own open-source work platform LaSuite, co-developed by the french DINUM and Germany's ZenDiS. Ministries in Denmark are moving to LibreOffice and Linux.

American cloud hyperscalers have responded to stanch the flow of investment away from themselves with what they term 'sovereign cloud' offerings. However, this branding label fails to address the underlying dependencies: "air-gapping" and similar offers from hyperscalers do not necessarily stop the extraterritorial reach of the US CLOUD Act, nor entirely mitigate the risk of the sanctions that blacklisted ICC officials. Hyperscalers, and their outriders, have also started to argue that moving away from monopoly cloud will be expensive, impractical, or both. But these arguments all fail to engage the fundamental idea that resilience comes from *diversity of supply* - procuring more sovereign solutions reduces geostrategic exposure, improves competitors' offerings, *and* exerts competitive pressure on monopoly cloud firms. It is, in that sense, win-win.

As part of this research, we conducted a review of public European defence procurement contracts to assess the depth of US cloud dependency. This picture is a partial one: some of the relevant contracts are classified, and details of the contracting partner are not publicly available. Nonetheless, these findings are deeply concerning, with critical national security systems and armies all subject to an increasingly unpredictable geopolitical actor.

Methodology

We conducted a preliminary review of national defence cloud systems by identifying each country's defence ministry website and searching each site for references to "cloud," "Microsoft," "Google," "Amazon Web Services," and "Oracle." We also searched local media for the name of the defence ministry in each country's native language alongside these key terms. We used Google Translate to translate pages not written in English. We also reviewed recent literature on European defence cloud systems.

We cross-referenced our findings from this preliminary review with contract data from Tenders Electronic Daily (TED), a supplement to the Official Journal of the EU that includes all procurement notices for government contracts in excess of €143,000. We searched for all contracts mentioning "Microsoft," "Google," "Amazon Web Services," and "Oracle" awarded by a government agency whose main activity is national defence. When a preliminary review suggested that a government used another US-linked provider, we searched for contracts mentioning those providers as well. Because the UK does not publish procurement data on TED, we used the UK Contracts Finder as an alternative.

We then audited the contract results for each country and eliminated false positives, such as contracts that sought to hire individuals proficient in Microsoft and Google technology with no acquisition attached. We also identified missing data, where government sources suggested that a cloud system was in use but no corresponding contract could be found. We supplemented missing contract data with information from government procurement websites, official budgets, and press releases.

Where possible, we recorded contracts that were explicitly for the acquisition of the US-linked technology. In many cases, however, contracts also included other services, such as consulting fees for a third-party implementer. Where granular contract data was not available, we reported the value of framework agreements for cloud systems that relied in some part on US technology. All values are reported in euros using exchange rates from February 2026.

Our findings nevertheless represent a conservative estimate. Subcontracting relationships make it difficult to identify every contract that implicates US technology. In many cases, we were unable to find contracts that corresponded to government announcements about tech acquisitions.

Findings[1]

1. European security is deeply intertwined with US tech infrastructure

78.5% of European countries studied (23 of 28) depend on US tech companies for national defence applications. This includes a mix of direct partnerships with US companies and European companies who function as the service providers but rely on infrastructure provided by US companies. More than half of the EU27 + UK have formed an explicit partnership with a US tech company to run their defence systems.[2]

2. Most European countries are classified as "at high risk" due to their exposure to US cloud providers

16 of 28 national defence agencies or ministries are at high risk to a potential US 'kill switch', as they are either directly contracting a US tech company for cloud services or it remains unclear whether the US technology they rely on is effectively "air-gapped".

While the term "air gapped systems" often refers to systems that are physically disconnected from the internet, in this context it refers to their disconnection from the hyperscaler's global cloud infrastructure.

Examples include AWS "Sovereign Cloud" and Delos Cloud. The latter is a cloud run by SAP and Deutsche Telekom using Microsoft Azure software. These systems are managed by European staff, often through European companies or local subsidiaries, but use US-hyperscalers technology. The *theory* and the sales pitch is that they run independently of their US tech providers global network and may therefore keep working under sanctions, for a time.

Updates and patches are checked for safety by independent bodies. This reduces the risk of data access by foreign governments under laws like the CLOUD Act or FISA. Any access to the data by US based companies delivering technology would essentially require hacking the cloud software through malicious patches.

While European oversight over patches and updates is a welcome step towards sovereignty, even nominally air-gapped systems still require regular updates and

[1] For the table of findings from open contracting data, see Appendix 1.
[2] We defined explicit partnership as any cooperation agreements with a US tech provider or direct government purchases of software licenses from a US tech company.

depend on maintenance from their US service provider. If such maintenance is cut off by sanctions, the long-term reliability and safety of the technology is at risk.

In seven cases we found a medium risk due to dependence on US technology, as European countries either have defence agencies who are contracting with European providers who themselves rely on US infrastructure (eg airgapped systems), or we found sources stating that systems run on a base of US-hyperscaler technology.

Only one European country is seen as a low risk case as they have already implemented significant sovereign solutions for their military cloud and no indication for US-hyperscaler dependency was found: Austria, while the Netherlands appear to be moving.
For Bulgaria, Cyprus, Malta and Sweden, we could not find any reliable information regarding their defence cloud.

Exposure level (per open data)	Contracting national defence agencies
High risk	Croatia, Czech Republic, Denmark, Estonia, Finland, Germany, Hungary, Ireland, Latvia, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, United Kingdom
Medium risk	Belgium, France, Greece, Italy, Luxembourg, Spain, The Netherlands
Lower risk (using what appears to be sovereign solutions, no indication of US-hyperscaler dependency found)	Austria
Unknown	Bulgaria, Cyprus, Malta, Sweden

3. Local contractors often still highly depend on US tech

In contracts with the Belgian, German, Italian, Luxembourgian, Spanish and British defence agencies, cloud services were described as ‘sovereign’ solutions yet were still reliant on US companies. In Belgium, Denmark, Finland, France, Italy, Luxembourg, Slovenia and Spain the immediate contractor of the national defence agency is a European company, which then contracts with a US provider to build on their cloud infrastructure. These cases show the complex nature of the European cloud market, where US dependencies are not always immediately obvious and can even be hidden from plain sight.

4. Microsoft, Google and Oracle are the main beneficiaries of European defence partnerships

Microsoft dominates the cloud market amongst European defence agencies with several countries with partnerships that seem to rely primarily on its infrastructure and overall, 19 deployments. Google is involved in four partnerships. Both in Germany and Italy it is part of a multi-cloud strategy. Oracle is involved in five defence cloud contracts. Like Italy and Germany, various other defence agencies rely on several US tech companies for their cloud infrastructure.

Cloud provider	Contracting national defence agencies
Microsoft	Belgium, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Latvia, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, United Kingdom
Google	Germany, Italy, Luxembourg, The Netherlands
Oracle	Ireland, Italy, Poland, Spain, United Kingdom
Sovereign solutions and no clear dependency found	Austria
Unknown	Bulgaria, Cyprus, Malta, Sweden

5. Critical arms, dangerously exposed: Case studies

Explicit cooperation

Some European countries have pursued explicit cooperation agreements with US cloud providers despite the Trump administration's hostile approach toward its European allies. Many governments deepened their ties with US cloud providers even after President Trump said that he would "encourage" Russia to attack NATO allies who do not pay sufficiently to the alliance.

The UK

The United Kingdom's Ministry of Defence signed agreements with Google Cloud in 2025, despite the company's cooperation with the Trump administration. Furthermore, the UK's Ministry of Defence's IT contracts include Google, Oracle, Amazon Web Services and Microsoft to a total of 1.099 billion euros.

Germany

Germany's Bundeswehr is contracting its internal IT services provider BWI GmbH to a total value of 1.6 billion euros, which includes cloud services from Google. Germany's Bundeswehr is running a multi-cloud strategy, building on stacks from US-based

VMWare, Google's airgapped cloud solution and open-source solutions, developed in close collaboration with the NeoNephons Foundation. It is not possible to determine Google's share of the total contract value.

A 2024 digitalisation report shows the Ministry of Defence relies on Microsoft Sharepoint and Exchange, without providing details about how they are hosted.

Poland
In February 2025, Poland's Ministry of Defence signed a cooperation agreement with Microsoft to deepen the country's collaboration with the cloud provider on artificial intelligence, quantum computing, and other emerging technologies. In April, the Polish military signed a similar agreement with US cloud provider Oracle for cybersecurity services, while it also holds contracts with Oracle.

Hidden dependencies

Some countries have tapped European cloud providers for national security applications, but these agreements can introduce hidden dependencies on US technology. These partnerships could place European data in the hands of US-owned processors.

Denmark
In 2025, the Danish government announced that some public agencies would drop the Microsoft Office suite in favour of open-source alternatives. However, it is unclear if and when the Ministry of Defence will join this move. Officials celebrated the move as a cost saving measure as dependency on a single cloud provider can lead to cost overruns, but the move may be driven by factors other than cost: The Trump administration's belligerence towards Greenland has strained Denmark's relationship with Microsoft's home country.

Moving away from Microsoft-branded software will not necessarily eliminate all dependence on Big Tech infrastructure. Danish military contractor SitaWare recently launched BattleCloud, a tool intended to provide continuous access to satellite imagery, communications, and intelligence. According to SitaWare, BattleCloud software typically runs on Microsoft Azure cloud infrastructure. A company executive said in April 2025 that this is not the case for the Danish Home Guard, without providing more details.

Other Danish defence systems appear to rely on Microsoft for back-end services. The Danish Home Guard website runs on Microsoft Azure infrastructure.

Spain
In 2024, Spain awarded domestic telecommunications provider Telefónica an €80.3 million contract to build its comprehensive defence information infrastructure system, known as I3D.

However, some of that investment will benefit US Big Tech companies. Telefónica migrated its cloud offerings onto Oracle infrastructure in 2022. The Spanish defence ministry has spent more than €7.6 million on contracts that include Oracle licences for I3D and other national security systems.

Italy
Italy recently moved its defence systems onto Polo Strategico Nazionale (PSN), the country's sovereign cloud solution. PSN runs on Google Assured Workload and Oracle Alloy technology. Italy has spent more than €313 million on PSN.

France
France seems also exposed to US technology. Besides broad use of Microsoft Software, which is set to be phased out more and more, the country's defence ministry uses Nexium, a defence cloud solution originally developed through a partnership between French defence contractor Thales and US tech company Microsoft.

Google has also partnered with Thales to form S3NS, a "trusted cloud" solution intended for government use, recently achieving the highest sovereignty certification issued by France's cybersecurity agency ANSSI, disappointing hopes this certification scheme would effectively ban US-hyperscalers.

Leading Europe's sovereign cloud solutions for security and defence

Years of procurement from monopolies is difficult to reverse overnight. Yet only few European countries have begun the work of moving to more defensible and resilient solutions.

Austria
In 2025, Austria began a government-wide move away from proprietary cloud providers. Government agencies have abandoned Big Tech companies for the open-source cloud provider NextCloud and Microsoft alternative LibreOffice. Austria's armed forces reportedly completed a transition away from Microsoft Office of around 16,000 workstations in 2025.

Moving forward: The Netherlands

While the current architecture is based on Microsoft and Amazon Technology, and therefore the Netherlands are classed as a middle risk case, the Ministry of Defence has recently partnered with the Dutch telecoms company KPN and French defence contractor Thales. The goals is to build a sovereign defence cloud, without reliance on US cloud providers,

Conclusion and recommendations

Europe's security and defence environment has changed rapidly. Two years ago, it was unthinkable that Europe would be sending troops for a defence exercise to Greenland to discourage any territorial offenses from a NATO ally. While the immediate threat to NATO's territorial integrity has subsided, the fundamental risk is permanent. It would be imprudent to wait for the next crisis to safeguard more resilient digital systems.

Some European nations - such as Finland - have reportedly engaged in 'scenario planning' for the risk of a US technology shutdown. It has become common in some quarters to hear arguments that "full independence" is unrealistic. However, while a total shift may well be impractical, it is equally foolish to keep this flank so exposed without introducing greater resilience. Early trailblazers demonstrate that greater resilience is achievable with sustained focus and political commitment.

European leaders should more systematically assess these critical digital dependencies and act to reduce the geostrategic leverage they give the US in adversarial situations.

A path towards European strategic independence for its military digital backbone is now urgently required. European defence and security agencies and leaders should:

- Prioritise digital resilience and sovereignty in cloud infrastructure as a core element of Europe's military modernisation and integrate this into the EU Commission's Future of European Defence plans.
- Audit current cloud dependencies in all defence and national security sectors to identify the highest-risk systems.
- Mandate local control: sensitive government and defence computing should operate exclusively on infrastructure housed and *controlled* within Europe.
- Develop phased migration plans to transition the most critical systems to sovereign European cloud solutions by 2030.
- Reform public procurement rules to favour sovereign, European-controlled providers and ensure full data sovereignty.
- Exclude hyperscaler platforms that claim sovereignty but remain exposed to foreign jurisdiction or geostrategic leverage.
- Increase public investment in sovereign, open-source software to help builders tailor solutions to defence and security requirements.
- Impose strict limits on foreign direct investment in domestic digital infrastructure providers to prevent indirect control.
- Facilitate cross-national sharing of best practices among early-adopter agencies, defence and otherwise, that have completed migrations.

- Pool procurement across member states where possible to scale demand for secure, European-developed digital solutions.

Just as Europe has learned to plan for the unthinkable on its physical borders, it must now apply that same unsentimental realism to its digital ones. Failure to act is itself a choice — one that leaves Europe's digital flank dangerously exposed.

About FOTI

FOTI is a pan-European think and do tank who work to build a future of European tech that is more secure, prosperous, and fair. We offer research and insights to European leaders in the service of opening market chokepoints and building sovereign alternatives. We are non-partisan and accept no corporate funding.

Appendix 1
– US cloud usage according to open databases

Country	Defence or security agency	Defence agency uses US cloud services	Defence agency partners with a US company for cloud services (may be contracted through a third party)	Defence agency holds licenses for software made by US cloud provider but unclear if services are on-prem or in the cloud	Defence agency contracts with a European cloud provider that does or seem to depend on US-based technology	Defence agency uses US tech but claims its cloud is "sovereign"	Defence agency appears to operate a cloud independently of US tech	Could not identify any information about defence cloud	Defence cloud provider(s)
Austria	Bundesministerium für Landesverteidigung/ BMLV/ Federal Ministry of Defence						x		'Private Clouds', LibreOffice for productivity
Belgium	Belgische Defensie/La Défense belge/Belgische Streitkräfte	x		x					Microsoft
Bulgaria	Министерство на отбраната, Ministerstvo na otbranata							x	
Croatia	Ministarstvo obrane Republike Hrvatske	x		x					Microsoft
Cyprus	Κυβερνητική Πύλη							x	
Czech Republic	Armáda České republiky		x						Microsoft
Denmark	Forsvarsministeriet	x	x		x				SitaWare BattleCloud, Microsoft
Estonia	Eesti Vabariigi Kaitseministeerium,	x		x					Microsoft

Country	Defence or security agency	Defence agency uses US cloud services	Defence agency partners with a US company for cloud services (may be contracted through a third party)	Defence agency holds licenses for software made by US cloud provider but unclear if services are on-prem or in the cloud	Defence agency contracts with a European cloud provider that does or seem to depend on US-based technology	Defence agency uses US tech but claims its cloud is "sovereign"	Defence agency appears to operate a cloud independently of US tech	Could not identify any information about defence cloud	Defence cloud provider(s)
	Eesti Kaitsevägi								
Finland	puolustusministeriö	x	x		x				SitaWare, Mattermost, Microsoft
France	Ministère des Armées	x			x				, Thales originally developed on Microsoft
Germany	Bundesministerium für Verteidigung, Bundeswehr	x	x			x			Google Cloud & VMware (through BWI), Microsoft
Greece	Υπουργείο Εθνικής Άμυνας, Ελληνικές Ένοπλες Δυνάμεις	x			x				Microsoft
Hungary	Magyar Honvédség	x		x					Microsoft
Ireland	Department of Defence	x		x					Oracle, Microsoft
Italy	Ministero della Difesa, Forze Armate Italiane	x			x	x			Polo Strategico Nazionale (on Google Cloud and Oracle tech)

Country	Defence or security agency	Defence agency uses US cloud services	Defence agency partners with a US company for cloud services (may be contracted through a third party)	Defence agency holds licenses for software made by US cloud provider but unclear if services are on-prem or in the cloud	Defence agency contracts with a European cloud provider that does or seem to depend on US-based technology	Defence agency uses US tech but claims its cloud is "sovereign"	Defence agency appears to operate a cloud independently of US tech	Could not identify any information about defence cloud	Defence cloud provider(s)
Latvia	Aizsardzības ministrija, Latvijas Nacionālie bruņotie spēki	x		x					Microsoft
Lithuania	Lietuvos Respublikos krašto apsaugos ministerija, Lietuvos ginkluotosios pajėgos	x		x					Microsoft
Luxembourg	Directorate of Defence	x			x	x			Clarence (on Google Cloud tech)
Malta	Forzi Armati ta' Malta							x	
Netherlands	Ministerie van Defensie		x						Microsoft, Amazon
Poland	Ministerstwo Obrony Narodowej	x			x				Microsoft, Oracle
Portugal	Ministério da Defesa Nacional	x		x					Microsoft
Romania	Ministerul Apărării Naționale	x	x						Microsoft
Slovakia	Ministerstvo obrany Slovenskej republiky			x					Microsoft

Country	Defence or security agency	Defence agency uses US cloud services	Defence agency partners with a US company for cloud services (may be contracted through a third party)	Defence agency holds licenses for software made by US cloud provider but unclear if services are on-prem or in the cloud	Defence agency contracts with a European cloud provider that does or seem to depend on US-based technology	Defence agency uses US tech but claims its cloud is "sovereign"	Defence agency appears to operate a cloud independently of US tech	Could not identify any information about defence cloud	Defence cloud provider(s)
Slovenia	Ministrstvo za Obrambo Republike Slovenije	x		x	x				SitaWare BattleCloud, Microsoft
Spain	Ministerio de Defensa	x			x	x			Telefonica (backed by Oracle technology)
Sweden	Försvarsdepartementet, Högkvarteret							x	
UK	Ministry of Defence	x	x			x			Google Cloud, Oracle, Amazon Web Services, Microsoft
For all Information and further explanations see Appendix 2.									

Thank you for reading.

www.futureinstitute.tech

FOTI