Vast majority of European countries exposed to US 'kill switch', via national defence systems

- More than three quarters (23/28) European countries rely on US cloud providers for national defence systems, thus with a medium to high risk exposure to a US 'kill switch'
- 16 out of 28 European countries are classed as high risk to a potential US 'kill switch', including Germany, Poland, the UK and Denmark
- Only one country - Austria - appears to use fully sovereign cloud solutions for defence and security systems, while The Netherlands only last week announced intentions to follow suit yet continues to rely US cloud providers
- Results come from a first of its kind analysis of EU 27 + UK countries' defence cloud contracting
- New polling released at the same time shows that nearly two-thirds (62%) of respondents in France, Germany, Italy, Spain, and Poland see storing national government data on US tech companies as a threat to European security.

[Brussels, 17th April 2026] - Europe's defence and security systems are dangerously dependent on US cloud infrastructure, leaving critical security capabilities exposed to the threat of sanctions and a US 'kill switch' according to a new report by FOTI (Future of Technology Institute).

The analysis is the first comprehensive review of European countries' defence and security contracting that examines US cloud dependencies. The Trump administration's recent sanctioning of six judges and three prosecutors at the International Criminal Court (ICC) for authorizing arrest warrants for Israeli Prime Minister Benjamin Netanyahu has highlighted the increasing threat of US tech dependencies and the power of refusal of service. Caught in the midst of geopolitical tensions, the vast majority of European countries hold defence and security contracts with US cloud providers that are identified as a lethal vulnerability.

> *"Europe's defence leaders no longer have the luxury to ignore the risk of a cloud kill switch. The Trump administration and its Big Tech backers have weaponised our tech dependencies - and this only looks set to get worse. Not only is Europe's military cloud architecture a critical choke point, it is also an investment opportunity that can be directed to European challengers. On-shoring Europe's critical cloud is no longer an option - it's a must",* said **Cori Crider, Executive Director, FOTI**

The report finds 16 European countries facing a high risk of exposure to a potential US 'kill switch', while seven countries are at medium risk, facing indirect exposure to US cloud services. Only one country - Austria - is classified as lower risk cases as they appear to have built fully sovereign solutions (see Table 1 in Notes to Editors). US tech giants Microsoft, Google and Oracle are the main beneficiaries of European defence and security partnerships (Table 2).

Calls for 'European Tech Sovereignty' have increased significantly. In February, the European Defence Agency (EDA) presented plans to establish a fully operational military-grade data-sharing platform free from US dependencies by 2030. American hyperscalers have responded by offering so-called "sovereign cloud" solutions. Amazon Web Services opened a Germany based data centre under such branding last year, describing it as "physically and logically separate cloud infrastructure, with all components located entirely within the EU". Promises of insulation from US overreach stand in stark contrast to statements made by Microsoft executives in a hearing before the French Senate of Parliament last summer. Prompted whether EU data would be secure from US government reach, Microsoft's Chief Legal Officer declined to provide such a guarantee.

It's not just defence and security agencies that are concerned about this over-reliance on US cloud technology, European citizens are feeling it too. A new poll commissioned by FOTI shows that a majority of respondents in France (63%), Germany (67%), Italy (64%), Spain (61%) and Poland (53%) see storing national government data with US tech companies as a threat to European security. The poll, conducted by YouGov, collected responses from over 1,000 respondents in each country.

FOTI's analysis shows the complexity of modern day defence and security cloud contracting, with many countries relying on a variety of contractors and subcontractors. Even nominally 'sovereign' cloud solutions were still found to be exposed to US tech via hidden dependencies.

> "*Cloud infrastructure must be treated as a core pillar of Europe's defence strategy. As governments increase military spending, decisions about the digital backbone of European defence and security will shape Europe's strategic autonomy for decades. Strengthening sovereign cloud capacity, auditing high-risk dependencies, and redirecting public investment toward European-controlled solutions would not only improve resilience but boost the European economy and develop European technology solutions*" said **Tobias B. Bacherle, Germany Senior Lead, FOTI**.

— ENDS —

Notes to Editors:

Media contact:
For questions or interview requests please contact:
tobias.bacherle@futureinstitute.tech

About FOTI:
FOTI is a think tank dedicated to building a prosperous and fair European future that harnesses the power of technology.

FOTI's goal is simple: tech that truly serves the public. We help democracies shape a digital future that is open, fair, and accountable. We design market reforms, advocate for enforcement, and back credible challengers.

We're not your typical think tank. Working across Europe, we turn ideas into action, building technical proofs of concept, convening unconventional debates, and offering practical solutions for leaders, innovators, and citizens alike.

Today, we're advancing ways to open social media, reduce dependencies on tech monopolies, and democratise tech debate. We actively partner with builders, businesses, citizens, and democrats from across the political spectrum.
https://futureinstitute.tech/

Additional information:

Table 1

Exposure level (per open data)	European country
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 appear to be fully sovereign solutions)	Austria
Unknown	Bulgaria, Cyprus, Malta, Sweden

Table 2

Cloud provider	European country
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

Methodology:

FOTI 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." They also searched local media for the name of the defence ministry in each country's native language alongside these key terms. They used Google Translate to translate pages not written in English. They also reviewed recent literature on European defence cloud systems.

They cross-referenced 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. They 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, they searched for contracts mentioning those providers as well. Because the UK does not publish procurement data on TED, they used the UK Contracts Finder as an alternative.

They 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 of such technology attached. They also identified missing data, where government sources suggested that a cloud system was in use but no corresponding contract could be found. They supplemented missing contract data with information from government procurement websites, official budgets, and press releases.

Where possible, they 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, they 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.

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