



Connect

# Sovereignty in the UK:

Aligning National Security, Compliance, and  
Enterprise Strategy

Martin Hosken

Technical Director, Defence & National Security | EMEA



# Martin Hosken

Technical Director, Defence & National Security | EMEA  
Red Hat



# U.S Cloud Dominance in Europe

## The FACTS:

€264BN

flows from Europe to the United States for cloud services each year

Estimated  
83%

of European large enterprise spending on cloud/software flows to US providers

80%

of the value added from these services sold to European companies is created in the United States.

1.95M

Million U.S. jobs supported

\$323BN

Generated in value added within the US economy

72%

of EU customer cloud spending is with AWS, Microsoft & Google

TECHNOLOGICAL DEPENDENCE ON  
AMERICAN SOFTWARE AND CLOUD  
SERVICES: AN ASSESSMENT OF THE  
ECONOMIC CONSEQUENCES  
IN EUROPE

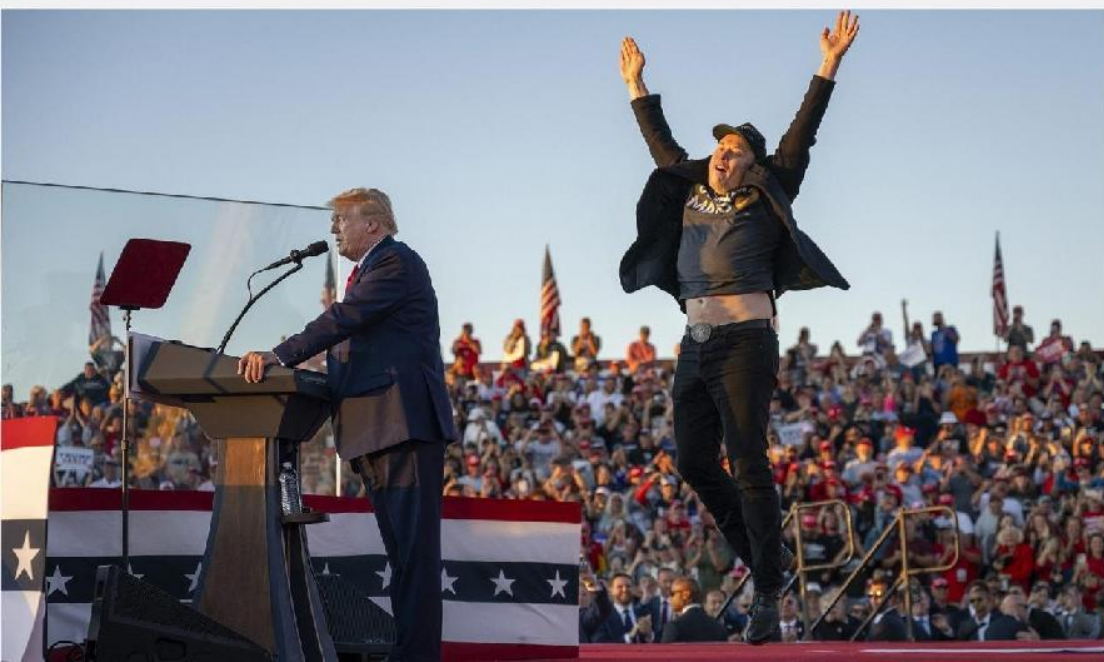
ASTERÈS

Economic Analysis Asterès

<https://www.cigref.fr/la-dependance-technologique-aux-softwares-cloud-services-americains-une-estimation-des-consequences-economiques-en-europe>

<https://www.cigref.fr/wp/wp-content/uploads/2025/05/TECHNOLOGICAL-DEPENDENCE-ON-AMERICAN-SOFTWARE-AND-CLOUD-SERVICES-AN-ASSESSMENT-OF-THE-ECONOMIC-CONSEQUENCES.pdf>



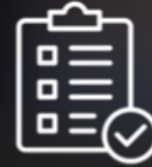


# What is digital sovereignty?



## **National Autonomy & Data Sovereignty**

Ensures that critical data and AI systems remain within national control, reducing risks of cyber espionage or external manipulation.



## **Regulatory Compliance**

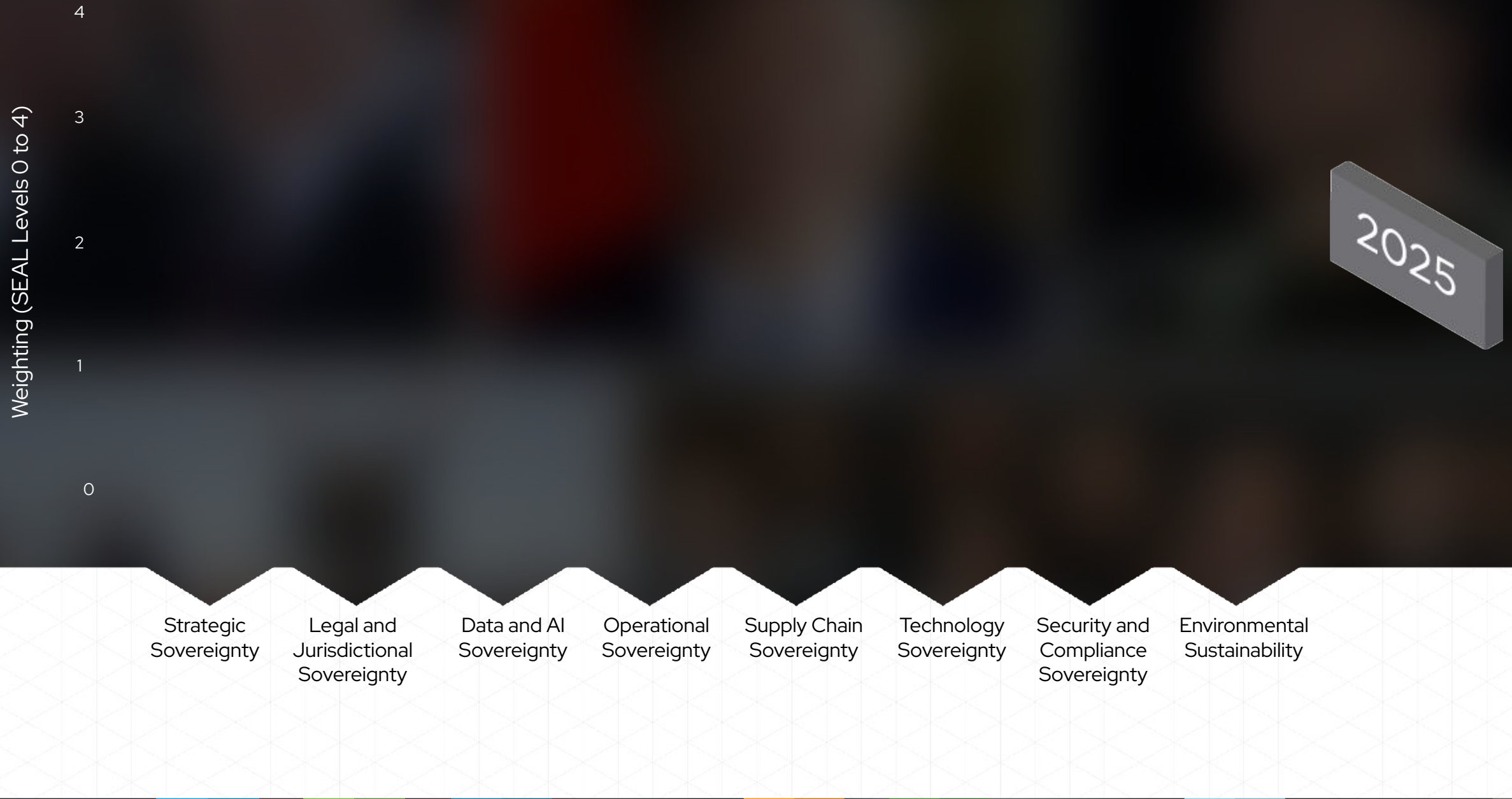
Must be tailored to align with national laws and policies, including privacy regulations and ethical guidelines.



## **Economic Growth & Innovation**

Encourages local AI research and development, cultivating domestic expertise and technological capabilities. Fosters the creation of high-value industries and jobs, enhancing global competitiveness.

# What is digital sovereignty?



# UK Sovereignty Drivers



## Political

- Brexit
- Geo-political
- Economic
- National Security
- Legislative / Regulatory Independence



## Technical Control

- Supply Chain Independence
- Multi Cloud Complexity
- Data Residency
- Service Interdependence
- Security and Transit
- Platform Resiliency
- AI Sovereignty / LLM Ownership



## Compliance

- Regulatory – NCSC cloud security principles, DPA part 3
- Regulation Maturity
- Data Sensitivity
- G-Cloud
- AI Regulation



*If the UK relies on foreign companies for cloud, semiconductors, software and telecommunications, how much control does it actually have over its digital future?*

Main drivers:

- **National security:** dependence on external technology providers can create strategic vulnerabilities.
- **Economic security:** digital infrastructure underpins almost every major sector.
- **Data:** where data is stored, processed and governed matters for privacy and state access.
- **Critical infrastructure:** telecommunications, cloud computing, energy systems and government IT increasingly depend on digital systems.
- **AI:** access to advanced computing, models, chips and data is becoming strategically important.
- **Geopolitics:** US–China competition, supply-chain disruption and changing international technology rules.



# Emergence of Data Privacy Risks



## CLOUD Act (The Clarifying Lawful Overseas Use of Data Act) 2018

is a law that grants the government the authority to access electronic data held by US-based technology companies, even if that data is stored on servers located outside of the United States

## FISA Section 702 (Foreign Intelligence Surveillance Act) 2008

It's primarily focused on collecting information about non-U.S. persons located outside the U.S. The government can compel U.S. companies to help in this collection.

## Chinese NIL (National Intelligence Law 2014

All organisations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of.



# CLOUD Act Agreements



The U.S. has entered into **CLOUD Act agreements** with the United Kingdom (2022) and **Australia (2024)** to facilitate law enforcement access to digital evidence across borders.

The **Five Eyes Alliance**, an intelligence and security partnership between Australia, Canada, New Zealand, the United Kingdom, and the United States. The alliance was founded on the UK/USA Agreement of 1941 and involves cooperation on security and intelligence matters across its member countries.

One of the Five Eyes' core principles is that members **do not spy on other governments in the alliance**. US Director of National Intelligence Admiral Dennis C. Blair said in 2013, "We do not spy on each other. We just ask."



*If the UK relies on foreign companies for cloud, semiconductors, software and telecommunications, how much control does it actually have over its digital future?*

### **Key questions for the UK:**

Who controls and can legally access UK data?

How dependent are public services on overseas cloud providers?

Who builds and operates critical networks?

Can the UK access critical chips and components reliably?

How dependent are organisations on foreign platforms and operating systems?

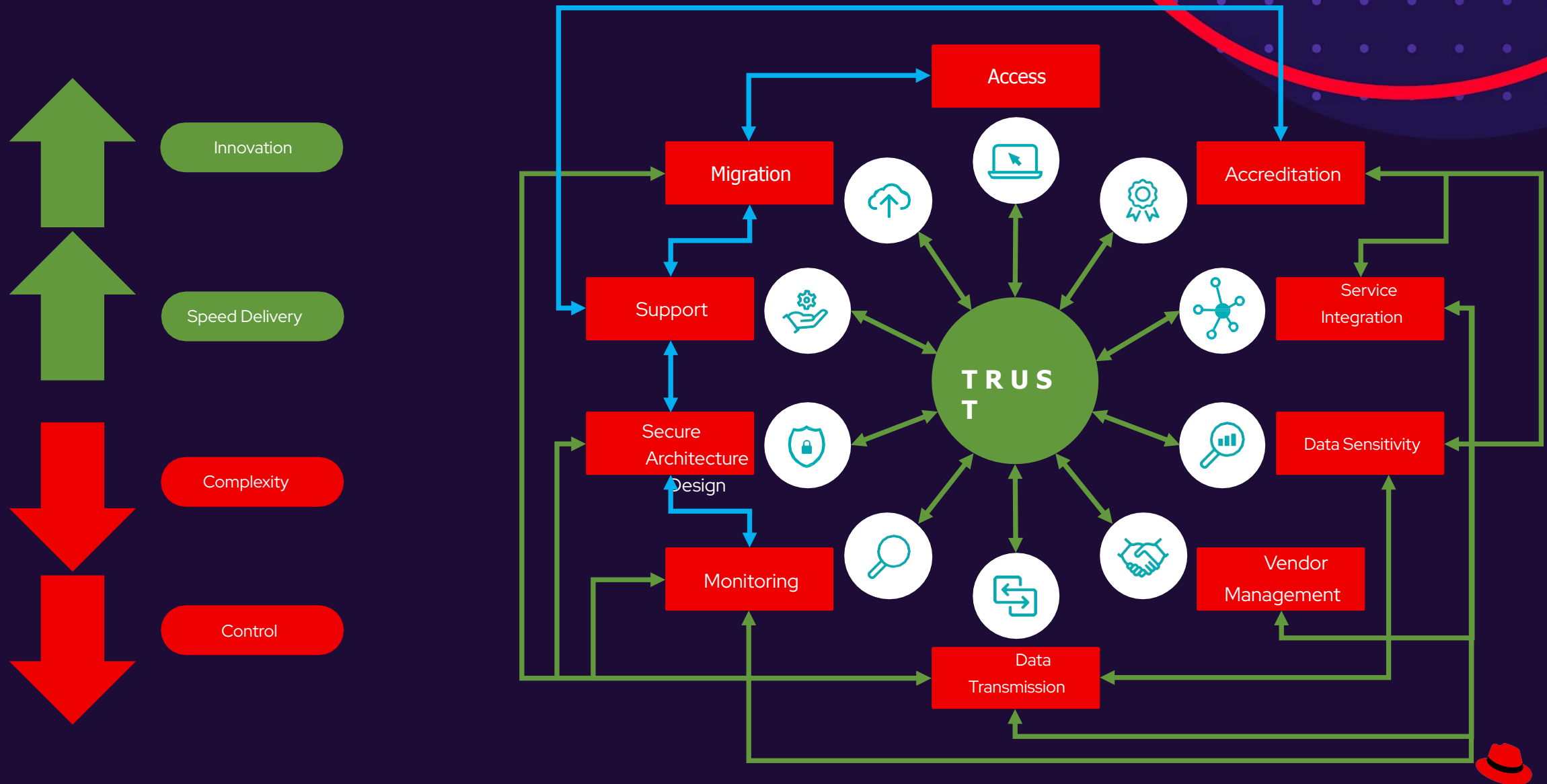
Does the UK control enough compute, models and expertise?

Does it have the people needed to maintain strategic capability?

Can the UK protect critical digital infrastructure?



# The Cloud Conundrum



# Sovereignty vs. Dependence

*UK digital sovereignty is not simply about bringing technology “back home”; it also involves trusted international partnerships and diversified supply chains*

## **Argument for greater sovereignty:**

- Reduces exposure to foreign governments and geopolitical shocks.
- Improves resilience.
- Gives government greater strategic freedom.
- Can support domestic innovation and industrial capability.

## **Arguments for collaboration:**

- Building everything domestically would be extremely expensive.
- The UK is deeply integrated into global technology markets.
- Protectionism can reduce competition and innovation.
- International partnerships can themselves increase resilience.
- Some technologies may simply be uneconomic for the UK to develop independently.



# Understanding Authority over Data



Andy Burnham



Donald Trump



Satya Nadella



Alan Sugar



## Sensitive UK police data vulnerable to 'compromise' by US government and foreign actors

Exclusive: Official UK security assessment found Microsoft cloud platform storing files was at potential risk from hostile hackers



Illustration: Guardian Design/Getty

Vast troves of highly sensitive police data are lying on **Microsoft** cloud platforms which an official UK security assessment deemed to be vulnerable to "compromise" by foreign actors and the US government, a Guardian investigation can reveal.

<https://www.theguardian.com/uk-news/2026/sep/18/sensitive-uk-police-data-vulnerable-to-compromise-by-us-government-and-foreign-actors>

NEWS

## Microsoft admits no guarantee of sovereignty for UK policing data

Documents show Microsoft's lawyers admitted to Scottish policing bodies that the company cannot guarantee sensitive law enforcement data will remain in the UK, despite long-standing public claims to the contrary



By Sebastian Klovig Skelton, Data & ethics editor

Published: 19 Jun 2024 8:30

The Register

Off-Prem ▶ PaaS + IaaS

## Microsoft attempts to woo governments with Cloud for Sovereignty preview

Sovereignty = you'll run on Azure and you'll be told when our engineers access your resources

Richard Speed  
Wed 4 Oct 2023 // 13:45 UTC

5

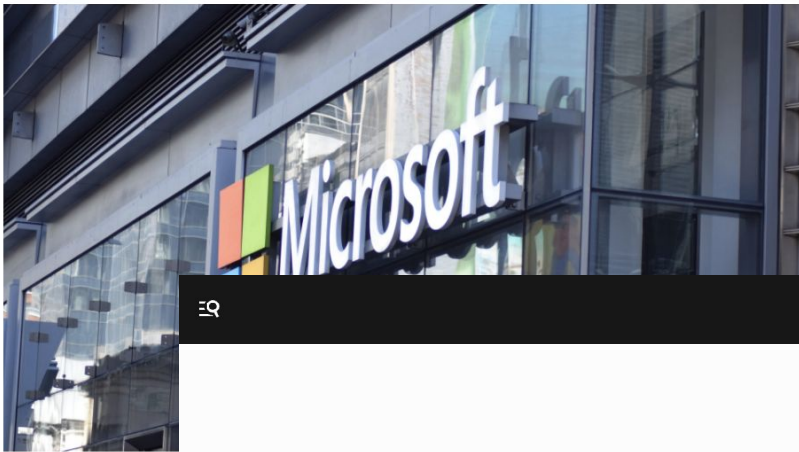
[https://www.theregister.com.cdn.ampproject.org/c/s/www.theregister.com/AMP/2023/10/04/microsoft\\_cloud\\_for\\_sovereignty/](https://www.theregister.com.cdn.ampproject.org/c/s/www.theregister.com/AMP/2023/10/04/microsoft_cloud_for_sovereignty/)

<https://www.computerweekly.com/news/366589152/Microsoft-admits-no-guarantee-of-sovereignty-for-UK-policing-data>

Legal Director confirmed

# Microsoft: EU data not protected from US access

21. July, 2025 11:35



## S Hyperscaler Headw

rench

“No, I cannot guarantee that.”

Forbes

wire Product Solutions Resources Pricing

Data Privacy

### Big Tech is Making Data Sovereignty Promises it Can't Keep

US surveillance laws override EU privacy rules, why Microsoft and other tech giants can't keep their promises on data sovereignty, and what the EU must do next.

Facebook

WhatsApp

This article

Explosive te  
Microsoft ca  
is safe from US authorities de

Microsoft cannot protect Euro  
access by US authorities – eve  
data centers. This was admitt  
legal director of Microsoft Fra  
a [hearing before the French S](#)

INNOVATION > CYBERSECURITY

## Microsoft Can't Keep EU Data Safe From US Authorities

By **Emma Woollacott**, Senior Contributor. © Emma Woollacott is a freelance jo... Follow Author

Published Jul 22, 2025, 07:56am EDT

Share Save

fudzilla.com HOME NEWS REVIEWS ABOUT

RealTyme Product Solutions Pricing Community Resources Company

## Microsoft Admits: It Can't Protect EU Data from U.S. Snooping

July 30, 2025

RealTyme

Microsoft Admits: It Can't Protect EU Data from U.S. Snooping

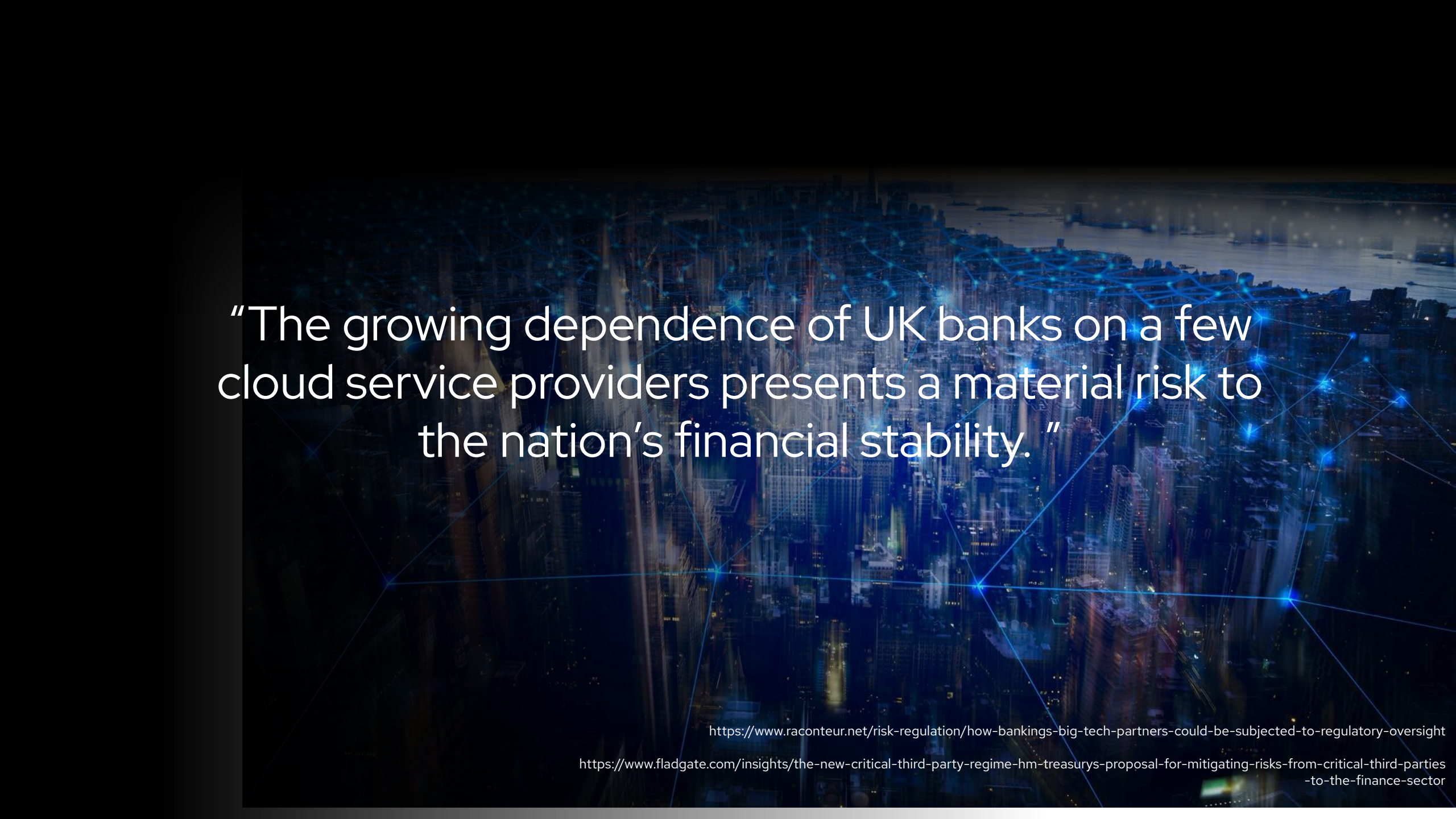
READ MORE!

CLOUD

## Microsoft can't keep EU data out of US paws

by **NICK FARRELL** on 22 JULY 2025 Post Like Be the first of your friends to like this.

FONT SIZE PRINT EMAIL

An aerial night view of a city, likely New York City, with a prominent blue digital network overlay. The network consists of glowing blue nodes connected by thin lines, creating a complex web across the city's skyline. The city lights are visible in the background, and the overall tone is dark and futuristic.

“The growing dependence of UK banks on a few cloud service providers presents a material risk to the nation’s financial stability.”

<https://www.raconteur.net/risk-regulation/how-bankings-big-tech-partners-could-be-subjected-to-regulatory-oversight>

<https://www.fladgate.com/insights/the-new-critical-third-party-regime-hm-treasurys-proposal-for-mitigating-risks-from-critical-third-parties-to-the-finance-sector>

# The strategic impact of sovereign AI

# What Does "Sovereign" Mean in the AI Context?

## Data Sovereignty

Manageability

Governance

Security

Controls

Data

Infrastructure

Operations

Large Language Models (LLMs) can be set up securely in a private cloud, and context data for AI can be provided securely.

Ready-made AI apps can be used, customer projects can be developed securely, and business processes can be compliantly automated end-to-end.

Use AI and still retain control over your data.

## Full Jurisdictional Control of Data



# How to strike the right balance?

INNOVATION

SCALABILITY

COOPERATION



AUTONOMY

SOVEREIGNTY

SECURITY

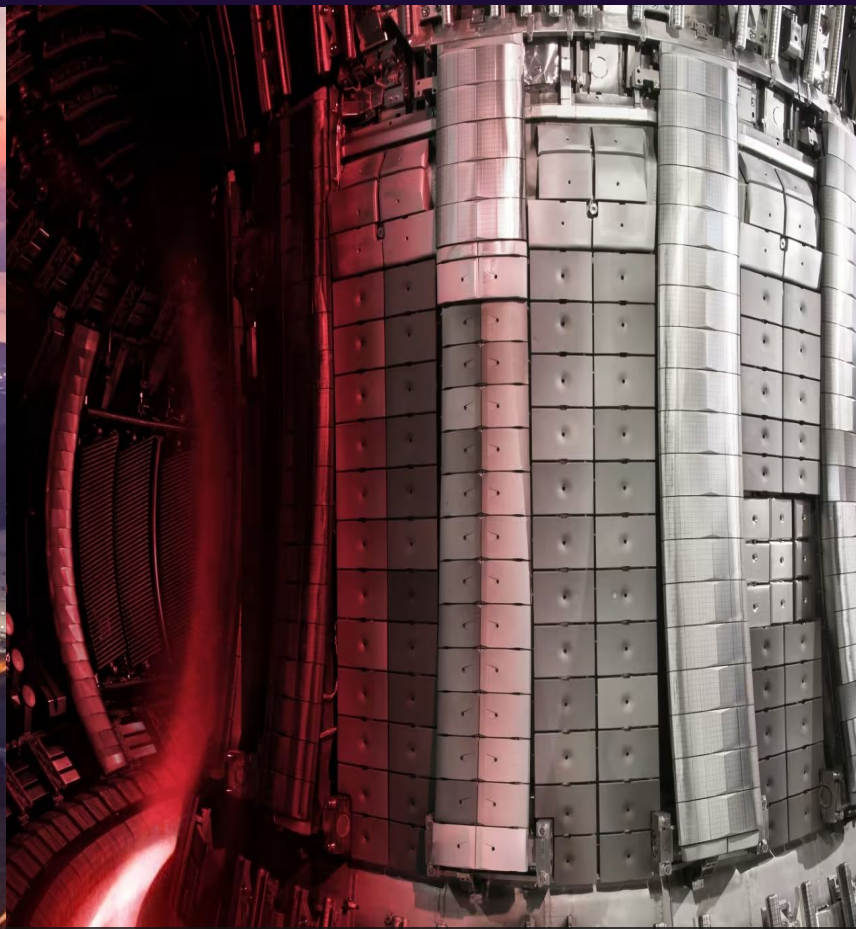
Sovereignty & Autonomy: Innovation & Global  
Cooperation



# Where Data and AI Sovereignty Matters



Critical National Infrastructure

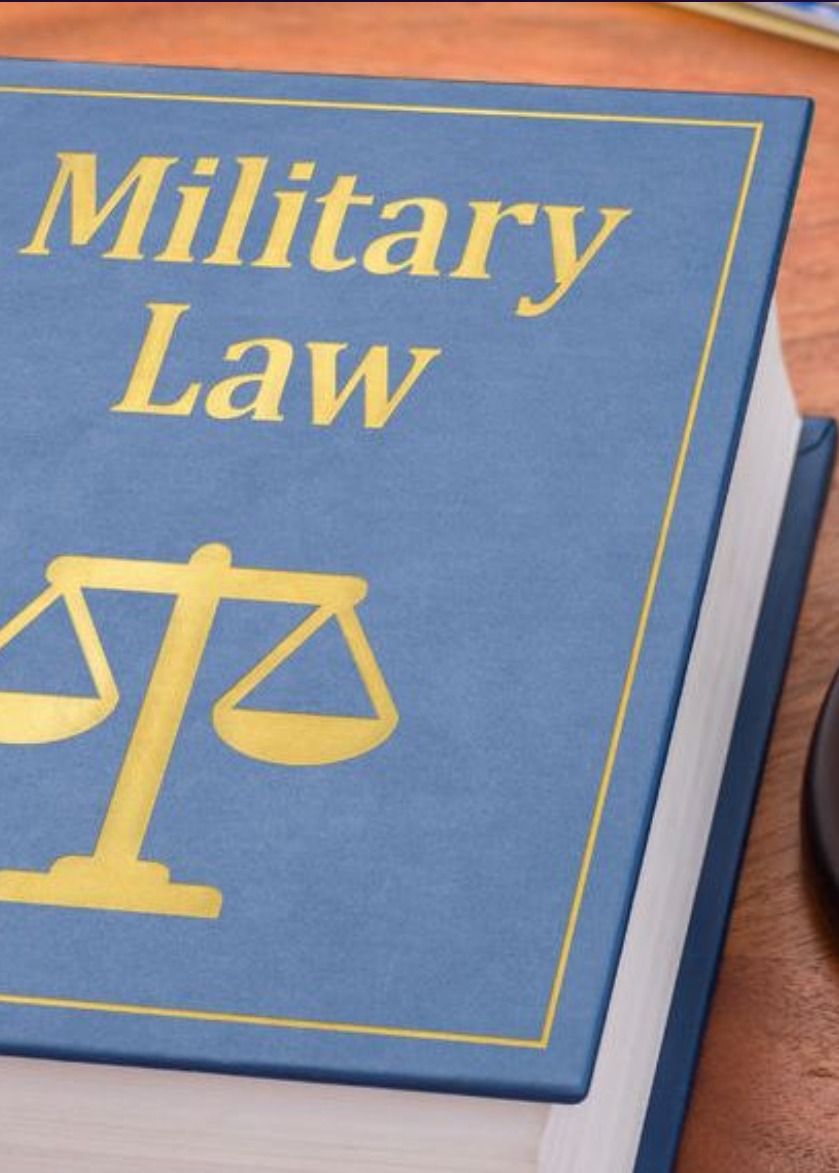


Top Secret Research

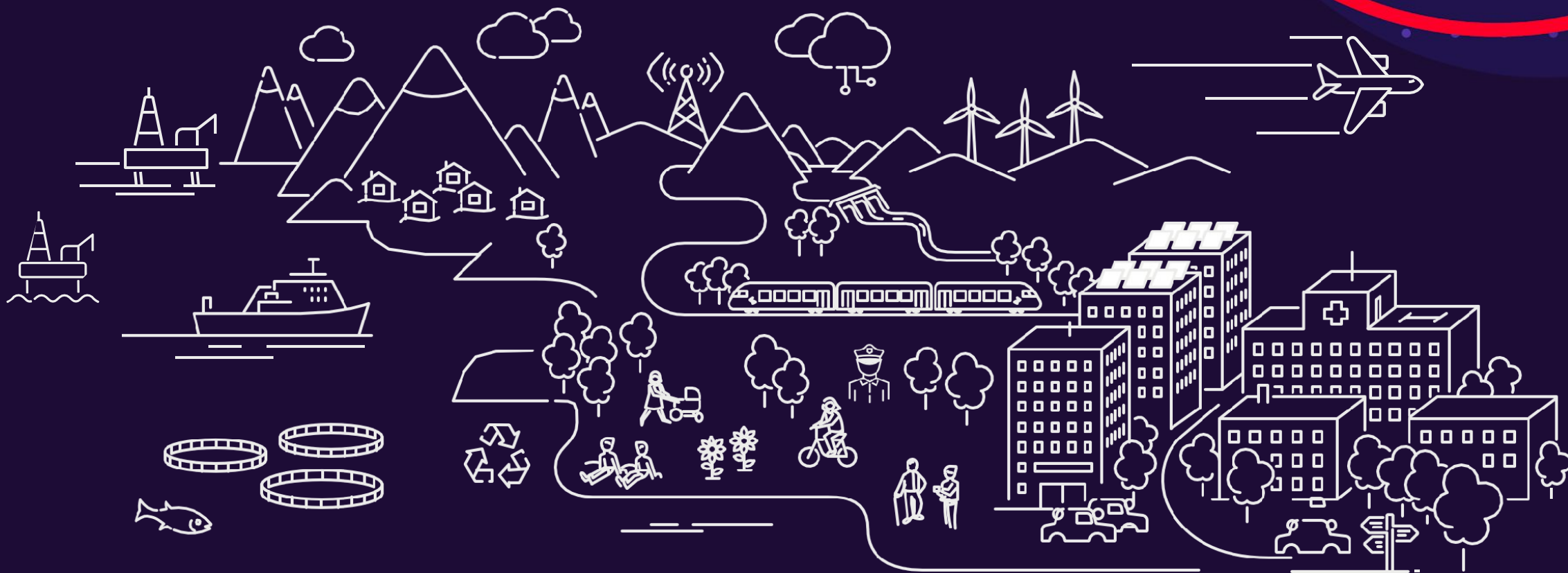


Sensitive Personal Data

## & Defence and National Security



# The world is how we shape it



**Martin Hosken**

Technical Director, Defence & National Security | EMEA



<https://www.linkedin.com/in/martin-hosken-471aa410/>





Connect

# Thank you



[linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)



[facebook.com/redhatinc](https://facebook.com/redhatinc)



[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)



[x.com/RedHat](https://x.com/RedHat)

