Research Papers

November 2025

European Cloud Adoption for National Security

Joseph Jarnecki

RUSI

Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of the publication or any of the information contained in the publication by you or any third party. References to RUSI include its directors and employees.

RUSI Research Papers, November 2025

ISSN 2977-960X

Publications Team

Editorial

Director of Publications: Alice Trouncer

Managing Editor: Sarah Hudson

Assistant Editor: Sophie Boulter

Design

Graphic Designer: Lisa Westthorp

Research Editorial

Head of Research Governance and Editorial: Elias Forneris

Cover image: Artur Marciniec/Alamy

Get in touch

www.rusi.org

enquiries@rusi.org

+44 (0)207 747 2600

The Royal United Services Institute for Defence and Security

61 Whitehall, London

SW1A 2ET

United Kingdom

Follow us on

Contents

Acknowledgements

The author would like to acknowledge the incisive and purposeful critique offered by Sara Seppänen and Noah Sylvia in the development of this paper. The author is also grateful to the official peer reviewers for their comments on the paper as well as the many insights from colleagues and friends.

The project was supported by Amazon Web Services (AWS).

All research for this paper was conducted independently and all findings are the author's.

Executive Summary

Cloud computing has become a fundamental capability for European national security and defence. Governments increasingly depend on cloud services to strengthen national resilience, modernise legacy systems and provide advanced technological capabilities such as AI. Case studies of cloud deployments from the UK, Ukraine, Estonia and Finland demonstrate that cloud infrastructure enables governments to maintain continuity of operations, enhance readiness and sustain critical functions under conditions of cyber and kinetic stress.

In Ukraine, cloud-based hosting of government registries and battlefield systems has ensured digital continuity despite sustained cyber and physical attacks. Estonia's 'data embassy' model illustrates how delocalisation can safeguard sovereign data against occupation or disruption. Finland employs the cloud for advanced simulation and training, thereby strengthening operational readiness, while the UK leverages the cloud to support cyber defence and command-and-control programmes. These examples highlight that cloud technologies deliver tangible impacts to mission needs.

Yet, adoption is not without challenges. Governments' approaches are shaped by technical, legal and market-related barriers, including dependence on assured connectivity, restrictive regulatory frameworks and market concentration among a handful of non-European providers. Some perceived risks – such as exposure to the US Cloud Act or technical vendor lock-in – are often overstated. More substantive concerns include dependence, transparency and geopolitical exposure. The strategic question is therefore not whether governments should adopt cloud technologies, but how they should navigate trade-offs to maximise benefits for national security and defence.

To shape European governments' further adoption of cloud technologies, this paper advances recommendations across three areas:

- **Strategic preparation**. Governments must set out a clear strategic direction on cloud adoption for national security and defence. National legislation and regulations should be revised accordingly and the implications for international law and resourcing computing requirements should be considered.
- **Procurement**. Governments must publish and update explicit guidance for compute procurement that is based on an assessment of data and workload criticality.

Officials should be supported through centralised assurance functions, frameworks to assess strategic autonomy requirements and skills development programmes.

- **Deployment**. When deploying compute, governments should adopt mitigations to reduce the risk of dependency or adverse concentration – whether deploying self-hosted or on-premises, private, public or multicloud. Accepting that some dependence is inevitable, governments and providers should cooperate to build trust and practise transparency.

The cloud is now neither peripheral nor optional; it can enable national resilience and operational effectiveness. Governments that approach adoption with technical sophistication, strategic intent and forbearance will be positioned to harness its advantages while managing the associated risks.

Introduction

First developed as a tool for commercial efficiency, cloud computing has since become a backbone of modern digital infrastructure. At its simplest, the cloud delivers computing resources – processing, storage and networking – on demand and at a large scale. Its growth has transformed how organisations operate, with governments, militaries and critical national infrastructure (CNI) operators expanding their use. For national security users, cloud computing is not just about business transformation, but also how governments achieve resilience and resource critical mission requirements.

Recent crises have brought the impact of the cloud into the spotlight. During the Covid-19 pandemic, European businesses, governments and individuals relied on cloud services to enable remote working and scale the sustained delivery of digital services. Faced with a full-scale invasion by Russia, Ukraine rapidly migrated critical registries and government digital services to private and public clouds, ensuring the continuity of operations under relentless cyber and kinetic attack.

Cloud computing offers tangible advantages for national security and defence. It supports operational continuity under cyber and physical disruption, enables access to advanced technologies such as AI, and supports the rapid deployment of mission-critical systems. Drawing on case studies from the UK, Ukraine, Estonia and Finland, this paper illustrates how cloud adoption can deliver operational and strategic impacts and proposes four primary areas of contribution: achieving resilience; replacing legacy systems and rebalancing incentives; accessing advanced capabilities; and ensuring the visibility and coherence of the digital estate.

Governments' adoption of the cloud across national security and defence must be shaped by strategic considerations. Adoption involves managing trade-offs and mitigating between opportunity and risk. Governments must navigate obstacles to adoption, such as securing connectivity and aligning legal frameworks. Moreover, they must consider where risks are overstated, for example, the US Cloud Act or technical lock-in, and where they are consequential – notably, geopolitical exposure and dependency.[1] European governments therefore need clarity of purpose: understanding

1. Conceptboard, 'The US Cloud Act: Threatening European Data Protection', 22 September 2023, <https://conceptboard.com/blog/us-cloud-act-european-data-protection/>, accessed 6 August 2025.

what mission requirements the cloud can service, what risks are tolerable, and what mitigations are available.

European governments currently have diverse approaches to cloud adoption for national security and defence. National strategies differ in scope and ambition: the UK maintains a cloud-first policy that is being increasingly applied across national security priorities; Ukraine has rapidly revised its regulations to allow urgent cloud adoption during active conflict; and Estonia and Finland have experimented with innovative models and are exploring further legislative change to promote adoption. These countries are among the most proactive cloud adopters in Europe and effectively demonstrate national security use-cases. Nevertheless, there is no pan-European consensus on how the cloud should be adopted for national security and defence.

In this context, it is pressing to therefore ask:

- How do certain European governments use the cloud to strengthen national security and defence?
- What strategic considerations shape European governments' decisions to employ the cloud?
- How can European governments maximise benefits from the cloud for national security, while mitigating its risks?

To answer these questions, this paper offers an overview of how cloud technologies can be employed for national security and defence, and what strategic considerations shape their deployment by government. It notably builds on research conducted by the Carnegie Endowment for International Peace and the Atlantic Council, which informed US policymakers about cloud security.[2] However, this paper focuses on Europe, where research to date has primarily examined sovereignty, competition and law.[3] It benefits from literature on European software-defined defence and NATO digital modernisation.[4]

2. Tim Maurer and Garrett Hinck, 'Cloud Security: A Primer for Policymakers', Carnegie Endowment for International Peace, 31 August 2020, <https://carnegieendowment.org/research/2020/08/cloud-security-a-primer-for-policymakers?lang=en>, accessed 6 August 2025; Trey Herr, *Four Myths about the Cloud: the Geopolitics of Cloud Computing* (Washington, DC: Atlantic Council, 2020), accessed 6 August 2025.
3. Christopher Millard (ed.), *Cloud Computing Law*, Second Edition (Oxford: Oxford University Press, 2021); Maaike Okano-Heijmans and Alexandre Ferreira Gomes, 'Too Late to Act? Europe's Quest for Cloud Sovereignty', Clingendael, March 2024, <https://www.clingendael.org/publication/too-late-act-europes-quest-cloud-sovereignty>, accessed 6 August 2025; Max von Thun and Claire Lavin, 'Engineering the Cloud Commons: A Blueprint for Resilient, Secure and Open Digital Infrastructure', Open Markets Institute, 15 May 2025, <https://www.openmarketsinstitute.org/publications/engineering-the-cloud-commons-webinar>, accessed 6 August 2025.
4. See Simona R Soare, Pavneet Singh and Meia Nouwens, 'Software-Defined Defence: Algorithms at War', International Institute for Strategic Studies (IISS), 17 February 2023, <https://www.iiss.org/research-paper/2023/02/software-defined-defence/>, accessed 6 August 2025; Antonio Calcara, 'NATO's Digital Modernisation: The Case of Cloud Computing', Hague Centre for Strategic Studies, 14 May 2025, <https://hcss.nl/report/natos-digital-modernisation-the-case-of-cloud-computing/>, accessed 6 August 2025.

The paper argues that cloud technologies contribute positively to national security and defence objectives. Governments will suffer from inaction, but they should not adopt the cloud indiscriminately. Success depends on strategic preparation, disciplined procurement and mission-focused deployment.

The paper has three chapters. The first chapter provides illustrative case studies to demonstrate how cloud deployments support national security objectives. The second chapter examines the strategic considerations that shape governments' adoption of the cloud for national security and defence use and discusses how opportunities can be pursued while mitigating risks. The final chapter provides recommendations to shape governments' evolving approaches to cloud adoption for national security and defence across strategic preparation, procurement and deployment.

Methodology

The research for this paper addresses cases of cloud technology deployment for national security and defence and the strategic considerations that shape its use by governments. Its objective is to inform policymakers across European countries and NATO member states. The analysis focuses on cloud technologies and does not exhaustively compare these with alternative digital technologies.

The research focused on four countries: the UK, Ukraine, Estonia and Finland. These countries were selected because they are among the most proactive adopters of cloud technologies for use in national security and defence when compared with European counterparts. Moreover, Ukraine, Estonia and Finland face existential threats that have motivated the adoption of innovative security and defence technologies. Future research could consider other countries that have well-established debates on cloud deployment in the national security space – for example, France, Germany and the Netherlands.

Notwithstanding the advantages outlined above, the analysis is limited by challenges to accessing evidence, often restricted due to security and commercial sensitivity. Comprehensive, system-level analysis of cloud-related national security issues – such as workload requirements, cloud service provider (CSP) performance and outages – also remains scarce. Moreover, the research relied primarily on the Ukrainian case study due to the ongoing active conflict.

Data-gathering for this paper took place between October 2024 and April 2025. It consisted of the following qualitative methods: a systematic review of open source academic and grey literature on national security and cloud services; 51 semi-structured in-person and online interviews with stakeholders from public, private and civil society sectors; closed-door seminars hosted by CSPs, governments and academic institutions on topics including competition, regulation and classified cloud; and an

in-person roundtable hosted by RUSI on 19 February 2025 with 12 experts from government, academia and the private sector, to validate research findings. Interviews have been anonymised to encourage participants to speak openly.

Cloud Definition and Key Context

Cloud computing is a model of delivering computing resources – processing power, storage and networking – via remote infrastructure and according to user demands.[5] It depends on the ability to virtualise computation, and then on separate virtual machines to manage workloads across these systems.[6]

As compared with self-hosted computing, the cloud tends to be associated with increased availability, scalability, operational agility, elasticity and access to advanced technologies, including AI.[7] Cloud adoption is also assumed to impact resilience, confidentiality, cost and integrity.

There is not one singular technical approach to designing cloud systems. Accordingly, the business models of CSPs vary. The following discussion does not aim to exhaustively capture the scope and scale of every part of the cloud sector. Instead, it sets out to consider cloud technologies themselves. Nevertheless, the author acknowledges that the paper is concerned mostly with hyperscale CSPs, because of their dominant market share in Europe, their existing and growing role in national security and defence within the countries in scope, and the attention paid to them by interviewees engaged during the research.

Service and Deployment Models

Cloud service models relate to the type of computing resource purchased. The main types of cloud service models are detailed below:

- **Infrastructure-as-a-Service (IaaS)**. Raw computing resources, either physically or logically separated. Users can control operating systems.
- **Platform-as-a-Service (PaaS)**. Users develop and deploy applications, with no control over the underlying infrastructure.
- **Software-as-a-Service (SaaS)**. Complete applications accessed remotely (for example, Salesforce, CrowdStrike Falcon and Zoom).

5. W Kuan Hon, Christopher Millard and Jatinder Singh, 'Cloud Technologies and Services', in Millard (ed.), *Cloud Computing Law*, p. 4.
6. Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing', PeaSoup Cloud, September 2011, <https://peasoup.cloud/nist-definition-of-cloud-computing/>, accessed 10 August 2025.
7. Author interviews with government officials, London and online, 16 and 19 December 2024 and 24 April 2025; author interviews with representatives from private sector, London and online, 28 and 29 January 2025; author interviews with representatives from civil society, London and online, 20 November 2024, 10 January and 5 and 7 February 2025.

Service models impact how control and responsibility is distributed between users and providers. The shared responsibility model is used by CSPs to explain this division. Shared responsibility models differ between CSPs but, for example, providers are typically responsible for securing cloud infrastructure and server hardware, while customers are responsible for their application data and credential management.[8]

Cloud deployment models define how computing infrastructure is structured and accessed. Understandings of deployment models vary. Definitions for essential characteristics of each type are as follows:

- **Public cloud**. Customers rent computation from a commercial provider who owns and operates resources that are shared across the general public.
- **Private cloud**. Resources are provisioned for a single organisation.
- **Multicloud**. Organisations use cloud services from two or more providers, without necessarily integrating them.
- **Hybrid cloud**. Computing is integrated across public and private clouds, as well as with on-premises and self-hosted solutions.
- **Sovereign cloud**. Resources are provisioned to meet national or regional requirements, or to meet priorities set against diverse factors. There is no unified definition of sovereign cloud across either the EU or NATO.

In practice, cloud systems rarely involve a single service model or deployment type. One interviewee reflected that using a SaaS solution can, for example, expose users to the IaaS choice of the SaaS provider: 'you won't get to choose the infrastructure'.[9]

Market Conditions

Cloud markets are highly concentrated. As of 2024, AWS, Microsoft and Google – referred to as 'hyperscale' CSPs – control approximately two-thirds of global market share for cloud services and infrastructure.[10] In some countries this is higher. Ofcom – the relevant British regulator – found in 2022 that AWS and Microsoft Azure controlled 70–80% of the UK market for IaaS and PaaS.[11] The SaaS market is more fragmented because of the lower barriers to entry, therefore creating greater diversity of service offerings, although some digital products – such as productivity software – are concentrated.

8. SentinelOne, 'What is the Cloud Shared Responsibility Model?', 2 May 2025, <https://www.sentinelone.com/cybersecurity-101/cloud-security/what-is-cloud-shared-responsibility-model/>, accessed 10 October 2025.
9. Author interview with UK government official, online, 10 January 2025.
10. Hava, '2024 Cloud Market Share Analysis: Decoding Industry Leaders and Trends', 11 January 2024, <https://www.hava.io/blog/2024-cloud-market-share-analysis-decoding-industry-leaders-and-trends>, accessed 10 October 2025; Felix Richter, 'AWS Stays Ahead as Cloud Market Accelerates', Statista, 21 August 2025, <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>, accessed 15 October 2025.
11. Ofcom, 'Statement: Cloud Services Market Study (Final Report)', 5 October 2023, <https://www.ofcom.org.uk/internet-based-services/cloud-services/cloud-services-market-study>, accessed 10 October 2025.

Numerous European governments use hyperscale CSP IaaS to run workloads and data storage at multiple levels of classification. British intelligence agencies and the UK Ministry of Defence have a contract with AWS to access diverse computation, including data storage and processing.[12] Ukraine migrated multiple government ministries to CSPs, including Azure, following Russia's invasion.[13] Finland's government IT centre (Valtori) has partnered with Nordcloud to support agencies in using Google Cloud and other CSPs.[14]

Worldwide spending on cloud services was estimated by Gartner at $595.7 billion in 2024, and the cloud market in the EU alone is expected to reach €300–€500 billion between 2027 and 2030.[15] Cloud services are increasingly central to business operations and critical infrastructure – including government – indicating their significance to national security as well as their centrality to distinct national security use.

12. Chris Mellor, 'Sovereignty? We've Heard of it. UK Government Gives Contract to Store MI5, MI6 and GCHQ's Data to AWS', *The Register*, 26 October 2021, <https://www.theregister.com/2021/10/26/uk_security_services_aws/>, accessed 8 October 2025.
13. Zach Marzouk, 'Microsoft Says It's Provided Over $100 Million in Tech Support to Ukrainian Government', *IT Pro*, 20 May 2022, <https://www.itpro.com/security/cyber-attacks/367752/microsoft-provides-over-100-million-in-support-to-ukraine-government>, accessed 12 October 2025.
14. Nordcloud, 'Nordcloud Wins Major Finnish Cloud Agreement', Blog, <https://nordcloud.com/blog/nordcloud-wins-major-finnish-cloud-agreement/>, accessed 1 October 2025.
15. Gartner, 'Gartner Forecasts Worldwide Public Cloud End-User Spending to Total $723 Billion in 2025', press release, 19 November 2024, <https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025>, accessed 2 October 2025; KPMG, 'Le Cloud européen' ['The European Cloud'], 4 May 2021, <https://kpmg.com/fr/fr/media/press-releases/2021/05/cloud-europeen-marche-enjeux-economiques.html>, accessed 6 August 2025.

Using the Cloud for National Security

This chapter assesses how cloud technology deployments contribute to national security and defence objectives by highlighting case studies in Ukraine, Finland, Estonia and the UK.

Achieving 'Resilience'

Cloud adoption presents opportunities to improve a state's ability to withstand, recover from and adapt to adverse conditions.

Withstand

Government data centres are viewed as legitimate military targets by adversaries of European states. Russian forces have notably seized and targeted Ukrainian data centres since 2022, using kinetic and cyber attacks, with the intention to disrupt or degrade the provision of Ukrainian digital services.[16] Anticipating these attacks, Ukraine's government and private sector organisations migrated data and services to cloud infrastructures – both inside and outside Ukraine.[17] Ukraine's then deputy prime minister and minister of digital transformation credited the emergency migration to the cloud with ensuring the continuity of government services.[18]

16. Cate Burgan, 'Ukraine Data Centers Became Physical Targets When Cyberattacks Failed', *MeriTalk*, 22 November 2022, <https://www.meritalk.com/articles/ukraine-data-centers-became-physical-targets-when-cyber-attacks-failed/>, accessed 10 October 2025; Grace B Mueller et al., 'Cyber Operations During the Russo-Ukrainian War', CSIS, July 2023, p. 9, <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war>, accessed 15 October 2025.
17. Nick Beecroft, 'Evaluating the International Support to Ukrainian Cyber Defense', Carnegie Endowment for International Peace, 3 November 2022, <https://carnegieendowment.org/research/2022/11/evaluating-the-international-support-to-ukrainian-cyber-defense?lang=en>, accessed 10 October 2025.
18. Frank Konkel, 'Ukraine Tech Chief: Cloud Migration "Saved Ukrainian Government and Economy"', NextGov, 1 December 2022, <https://www.nextgov.com/digital-government/2022/12/ukraine-tech-chief-cloud-migration-saved-ukrainian-government-and-economy/380328/>, accessed 10 October 2025.

Case Study 1: Ukraine's Diia App

Launched in 2020, Diia is an app that allows Ukrainian citizens to use e-identity documents to access over 130 digital government services, such as tax payment. Diia is built using an interoperable data exchange system with low construction and maintenance costs. The app has been adapted to wartime needs, introducing services including digital passports, the purchase of war bonds (raising around $54 million), financial support mechanisms and access to radio and TV broadcasts.[19]

As of December 2023, following 22 months of Russia's full-scale invasion, Diia usage had increased by 27% to 19.8 million users (63% of the Ukrainian population). [20]

A 2024 report by Brookings[21] directly links the 2022 decision of Ukraine's parliament allowing data storage in the cloud to ensuring the integrity and availability of Diia during wartime and guaranteeing the confidentiality of data on its systems. Diia data stored in the cloud outside Ukraine can still be targeted but is not vulnerable to kinetic attacks, can achieve greater scale, and can benefit from increased resilience against service interruption, for example, through multi-region hosting.

Recover

In 2007, Estonia experienced waves of cyberattacks that created significant disruptions lasting several months. Estonians were unable to access public web-based services or financial services or meet contractual requirements.[22] A report by NATO's STRATCOM Centre of Excellence concluded that Estonia was insufficiently prepared to swiftly remediate and recover from 'a relatively primate [sic] attack'.[23] While no formal

19. President of Ukraine, '"Diia" Will Become One of the Service Providers of the Reconstruction of Ukraine – President Volodymyr Zelenskyy's Speech at Diia Summit 2023', 19 December 2023, <https://www.president.gov.ua/en/news/diya-stane-odnim-iz-servisiv-provajderiv-vidbudovi-ukrayini-87837>, accessed 4 October 2025.
20. UNDP, '63% of Ukrainians Use State E-Services, User Numbers Grow for Third Year in Row – Survey', 25 January 2023, <https://www.undp.org/ukraine/press-releases/63-ukrainians-use-state-e-services-user-numbers-grow-third-year-row-survey>, accessed 4 August 2025.
21. George Ingram and Priya Vora, 'Ukraine: Digital Resilience in a Time of War', Working Paper No. 185, Brookings, January 2024, <https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war/>, accessed 6 August 2025.
22. James Pamment et al., 'Hybrid Threats: 2007 Cyber Attacks on Estonia', NATO Strategic Communications Centre of Excellence, 6 June 2019, p. 66, <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>, accessed 10 August 2025.
23. Pamment et al., 'Hybrid Threats', p. 69.

attribution was made, Russia is believed to have coordinated the attack, aiming to impose costs on Estonia following the decision to move a Soviet-era memorial.[24]

Interviews with Estonian stakeholders indicate that this incident – alongside Estonia's experience in restoring property rights following the end of the Soviet occupation – motivated Estonian officials to reassess approaches to government digital resilience, notably concerning data localisation.[25]

More recent national-scale ransomware incidents have exposed the importance of rapid recovery measures. Costa Rica and Indonesia experienced ransomware incidents in 2022 and 2024 respectively, primarily targeting legacy IT environments or private government clouds. A 2024 report from the World Bank links their use of legacy technology with the delays each experienced in recovery.[26] A senior cloud architect interviewed for this paper explained that cloud systems can more easily:

- Support simple and comprehensive data backups.
- Maintain backup programmes and remediate or rebuild systems rapidly.
- Provide 'hot swapping' (failover contingencies).[27]

Adapt

Essential characteristics of the cloud, as outlined by the US National Institute of Standards and Technology (NIST), include services automatically available on demand for users.[28] By contrast, traditional on-premises computing for large organisations can require users to navigate bureaucratic processes when, for example, provisioning additional servers for applications. The cloud's significant improvement in flexibility for users was credited by multiple interviewees as supporting mission objectives in several security contexts.[29] One notable example is the deployment of cloud-native cyber security SaaS applications such as endpoint detection and response (EDR) across Ukrainian government departments.[30]

24. Cyber Law Toolkit, 'Cyber Attacks Against Estonia (2007)', <https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007)>, accessed 20 October 2025.
25. Author interviews with Estonian officials, online, 16 December 2024, and 20 and 22 January 2025; Merje Feldman, 'Justice in Space? The Restitution of Property Rights in Tallinn, Estonia', *Ecumene* (Vol. 6, No. 2, 1999).
26. Ghislain de Salins, 'Unpacking Cloud Cybersecurity', Policy Report, World Bank Group, November 2024, p. 2, <https://documents1.worldbank.org/curated/en/099103124193527496/pdf/P177852-dda0bac6-71ce-408e-9fcb-f0d251cdb786.pdf>, accessed 20 October 2025.
27. Author interview with representative of hyperscale CSP, London and online, 29 January 2025.
28. Mell and Grance, 'The NIST Definition of Cloud Computing', p. 6.
29. Author interview with government officials, online, 17 December 2024 and 8 January 2025; Data-gathering workshop, London, 19 February 2025.
30. Author interview with former Ukrainian government official, online, 17 December 2024.

Case Study 2: Estonian Data Embassy

Under a 2016 bilateral agreement, Estonia created a 'data embassy' in Luxembourg to store critical government databases, registries and backups of essential services.[31] [32]

The data embassy intends to bolster Estonia's national digital resilience. Were the country to be invaded or occupied, stored data would be used by an Estonian government in exile. One interviewee involved in creating the data embassy explained that a government in exile could use digital ID cards and online voting to continue functioning for around five years, simply by utilising information backed up outside Estonia.[33]

Estonia's data embassy is a significant milestone in governments' use of cloud technology. It demonstrates how a country can pursue national resilience through reforming national legislation to permit the delocalisation of data. The data embassy, however, is closer to constituting an on-premises infrastructure than it is to the cloud. At the time of writing, the data embassy does not host live workloads, nor is it configured so that it automatically takes over key functions if the primary data centres running Estonian government workloads were disrupted.

Still, interviews with former and existing Estonian officials for this report illustrated the country's ambition – based on regulatory changes in 2024 – to expand the use of a delocalised public cloud to achieve greater availability and resilience.[34] As summarised by one interviewee: '99% of Estonian government digital services [are] under consideration for public cloud migration, adoption or expansion'.[35] Nonetheless, such a move will require further legal and cultural changes.

31. Ministry of Justice and Digital Affairs, 'Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the Hosting of Data and Information Systems', 20 June 2017, <https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf>, accessed 20 October 2025.
32. Riigi Teataja, 'Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel', ['Requirements for Network and Information System Security Measures and the Scope of Their Application When Using Cloud Services'], 3 January 2024, <https://www.riigiteataja.ee/akt/109012024025>, accessed 20 October 2025.
33. Author interviews with Estonian government officials, online, 16 December 2024 and 20 January 2025.
34. Author interview with former and existing Estonian government officials, online, 8 and 28 January 2025.
35. Author interview with former Estonian government official, online, 20 January 2025.

Replacing Obsolete Legacy Systems and Fixing Incentives

Self-hosted computing requires regular capital expenditure to replace outdated hardware systems. Under this model, organisations need to balance this requirement with other spending obligations. Current and former government officials from the UK, Estonia, Finland and Ukraine who engaged with this research shared the view that capital expenditure to replace legacy hardware is commonly deprioritised in favour of other spending.[36] One former government interviewee cited legacy technology as the primary driver for the UK adopting a cloud-first policy in 2011: 'the UK was in a fundamentally precarious position, [there were] more than 300 national data centres, none of which had a patch register – some of which were in a state of pretty much disrepair'.[37] This assessment was confirmed by two other former UK government officials.[38]

Cloud models provide a metered service and therefore require operational expenditure. The responsibility of ensuring that systems (both hardware and firmware systems) are replaced or updated falls on CSPs. Because CSPs' core business functions benefit from having up to date systems, they are incentivised to make the necessary capital expenditures.

Cost shifting from capital to operational expenditure, however, is not possible for all third-party software systems. Software licences are commonly considered as capital expenditure, and SaaS solutions will not always offer a metered option or may create cost incentives to encourage single upfront payments. SaaS that is operated by smaller providers often fits within these criteria; this notably includes SCADA (Supervisory Control and Data Acquisition) systems in CNI and real-time geographic information systems. In addition, organisations can struggle to access operational expenditure, which needs to be covered by year-to-date revenue, whereas capital expenditure can be funded through borrowing.

As for the public cloud, its scale and architecture – including the ability to 'load balance' (shift workloads across virtual computing resources as required) – allows updates to take place with minimal service interruption for customers. By contrast, private cloud or self-hosted solutions require updates to be more carefully managed by customers to minimise downtime.

36. Author interviews with existing and former government officials, London and online, 16 December 2024, 8 and 24 January and 12 February 2025; Data-gathering workshop, London, 19 February 2025.
37. Author interview with former UK government official, London and online, 29 January 2025.
38. Author interview with UK CSP, London and online, 24 January 2025; author interview with hyperscale CSP, online, 3 February 2025.

In national security and defence contexts, there are many advantages of having up-to-date systems with minimal operational downtime and which require small capital expenditure commitments, ensuring, in turn, a system's continuity and availability. By adopting cloud solutions, a state can therefore reduce reliance on legacy technology through diversified financial instruments and ensure its capabilities are 'evergreen … by default'.[39]

Case Study 3: UK Space Command and Control

The UK MoD announced in March 2025 that they would procure a software system ('Borealis') to 'monitor and protect satellites'.[40] Borealis, a space situational awareness solution, will collate and process information from multiple sources (up to top secret classification) and will support military decision-making.

While the availability of details remains limited, similar products (and interviews for this paper) indicate that Borealis will be SaaS: it will require cloud-hosted data storage and analytics to achieve the scale required for its mission functions.[41]

Access to Advanced Capabilities

The development and deployment of modern technologies relies on data and digital tools – especially advanced computing.[42] Some research tasks or workloads require bespoke skills or specific hardware that is finite, expensive or difficult to build and maintain, such as graphics processing unit (GPU) chips or quantum computers. Because of the cost and complexity, smaller countries struggle to develop domestic capacity across every innovative technology area, or even in the underlying data and digital tools. While the 'digital divide' is associated with the Global South, smaller

39. Andres Raieste et al., 'Government Resilience in the Digital Age', 2024, p. 28, <https://www.oii.ox.ac.uk/news-events/reports/government-resilience-in-the-digital-age/>, accessed 20 October 2025; Ministry of Defence, 'Cloud Strategic Roadmap for Defence', Policy paper, 2 February 2023, <https://www.gov.uk/government/publications/cloud-strategic-roadmap-for-defence/cloud-strategic-roadmap-for-defence>, accessed 20 October 2025; Scottish Government, 'Benefits of Cloud', 9 June 2020, <https://www.gov.scot/publications/benefits-of-cloud/pages/evergreen-it/>, accessed 20 October 2025.
40. Ministry of Defence, 'New UK-Made Space System To Help Protect Military Satellites', 7 March 2025, <https://www.gov.uk/government/news/new-uk-made-space-system-to-help-protect-military-satellites>, accessed 20 October 2025.
41. Steven J Johnston et al., 'Clouds in Space: Scientific Computing using Windows Azure', *Journal of Cloud Computing: Advances, Systems and Applications* (Vol. 2, 2013); Mark Say, 'MoD Awards Borealis Space Software Contract to CGI', UK Authority, 28 February 2025, <https://www.ukauthority.com/articles/mod-awards-borealis-space-software-contract-to-cgi/ >, accessed 20 October 2025.
42. Alexander Szalay and Jim Gray, 'Science in an Exponential World', *Nature* (Vol. 440, 2006), pp. 413–14.

European countries can also struggle to access the latest technologies that are available to their larger peers. In 2024, the Ada Lovelace Institute proposed that the UK should invest more that £900 million in public computation for AI alone. This scale of investment, amid conflicting spending priorities, will be hard to justify for smaller countries.[43]

Case Study 4: UK Active Cyber Defence

The UK National Cyber Security Centre's (NCSC) Active Cyber Defence (ACD) programme consists of several interventions and services designed to tackle high-volume commodity cyberattacks.

One ACD service is the Protective Domain Name Service (PDNS), a SaaS that prevents access to domains known to be malicious by not fulfilling user access requests.[44] It is a free service which the UK Cabinet Office has mandated that all government departments adopt, and is also available to other parts of the public sector, including the NHS. At the time of writing, the PDNS is implemented by Cloudflare[45] and Accenture.

The PDNS uses cloud technologies to achieve scale, service integrity, latency and cost-efficiency. It also benefits from the seamless integration of multiple cyber threat intelligence streams, enabled by cloud architectures.

Alternatively, technology hosted on the public cloud or provided as part of broader private cloud procurements offers access to the latest technologies for smaller governments, without incurring the significant sunk costs associated with government-funded domestic capacity development. The most prominent example of this is AI. As demonstrated by partnerships between leading AI companies and hyperscale CSPs – AWS and Anthropic, Azure and OpenAI, Google and Gemini – AI development and deployment presently requires massive data-storage and data-processing capabilities.[46] AI is also critical to the management and effective leveraging of increasingly large

43. Eleanor Shearer, Matt Davies and Mathew Lawrence, 'The Role of Public Compute: How Can We Realise the Societal Benefits of AI With a Market-Shaping Approach?', Ada Lovelace Institute, 24 April 2024, <https://www.adalovelaceinstitute.org/blog/the-role-of-public-compute/>, accessed 20 October 2025.
44. National Cyber Security Centre, 'Protective Domain Name Service (PDNS)', 17 September 2024, <https://www.ncsc.gov.uk/information/pdns>, accessed 20 October 2025.
45. Cloudflare, 'Protective DNS for Governments', Cloudflare Docs, <https://developers.cloudflare.com/reference-architecture/diagrams/sase/gateway-for-protective-dns/>, accessed 20 October 2025.
46. McKinsey & Company, 'The Cost of Compute: A $7 Trillion Race to Scale Data Centers', 28 April 2025, <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-cost-of-compute-a-7-trillion-dollar-race-to-scale-data-centers>, accessed 20 October 2025.

datasets. Companies assume the development cost and provide these services directly to users and consumers or integrate the technology in other products.

Kenneth Payne recently outlined how diverse AI technologies '[are]rapidly altering the landscape of national security'.[47] He highlighted AI's overlap with other technologies – quantum computing, satellite coordination, hypersonic weapons – and identified tactical use-cases, including AI integration into autonomous weapons systems, targeting and situational awareness.[48] Models are not always hosted on remote public or private cloud servers: they can, for example, be run on edge devices. However, most model training does require large-scale computation that is provisioned through a remote, centralised cloud.

Ukraine's defence against Russia and Israel's war in Gaza have incidentally led to technological innovation, and numerous companies have trialled their products in this context. For example, it has been reported that the Israeli Defence Forces (IDF) have used commercial cloud-hosted AI capabilities during the war in Gaza, storing over 13.6 petabytes between 7 October 2023 and July 2024 with a single CSP.[49] While this information is unconfirmed by other sources, the report states that the IDF has used cloud-hosted AI capabilities to 'transcribe, translate and process [open source] intelligence', which is then cross-referenced with classified sources.[50] The IDF's use of commercial and effectively dual-use cloud and AI capabilities demonstrates how armed forces can scale computation rapidly, but also raises questions about associated risks (see next chapter).

Interviews with cloud procurement experts also indicated that access to advanced computing capabilities, which are packaged and integrated as a single all-in-one service, are more compelling to governments than the procurement of individual systems and in-house integration.[51] Two government interviewees offered this as an explanation for why their government had procured a single hyperscale CSP for multiple functions, using data at a high classification level.[52] A 2025 report from the UK Competition and Markets Authority finds that similar service bundling by CSPs – primarily through software licensing practices – can create anti-competitive or negative outcomes for customers.[53]

47. Kenneth Payne, 'AI Technologies and National Security', RUSI Explainer, 17 April 2025, <https://www.rusi.org/news-and-comment/explainers/ai-technologies-and-national-security>, accessed 20 October 2025.
48. *Ibid.*, pp. 5–9.
49. Michael Biesecker, Sam Mednick and Garance Burke, 'As Israel Uses US-Made AI Models in War, Concerns Arise About Tech's Role in Who Lives and Who Dies', *Associated Press*, 18 February 2025.
50. Michael Biesecker, Garance Burke and Sam Mednick, 'Microsoft Says It Provided AI to Israeli Military for War But Denies Use to Harm People in Gaza', *Associated Press*, 17 May 2025.
51. Author interview with representative of civil society organisation, online, 8 January 2025; author interview with representative of hyperscale CSP, online and London, 30 January 2025.
52. Author interviews with government officials, online, 19 December 2024.
53. Competition and Markets Authority, 'Cloud Services Market Investigation: Summary of Provisional Decision', 28 January 2025, para. 29, <https://assets.publishing.service.gov.uk/media/67989251419bdbc8514fdee4/summary_of_provisional_decision.pdf>, accessed 20 October 2025.

Case Study 5: Ukraine's Delta Platform

Delta is a cloud-native situational awareness and battlefield management platform deployed by Ukraine on localised public cloud servers immediately after the 2022 invasion by Russia.[54] Interviews for this paper confirm that Delta's battlefield impact has increased the sense of urgency within NATO to develop an Alliance-wide interoperable equivalent.[55]

As outlined by Stefan Soesanto, Delta provides five services: (1) 'Monitor', live battlespace mapping updated via diverse data inputs including military sensors and civilian reports; (2) 'Element', securing inter-unit messaging; (3) 'Vezha', streaming video from deployed devices and analysing feeds for automatic battlefield mapping; (4) 'Mission Control', synchronisation tools for mission planning and execution; and (5) 'NextCloud', cloud storage, similar to commercial business-to-consumer SaaS offering such as Google Drive or Microsoft OneDrive.[56]

Primary data-gathering revealed that additional modules compose Delta: (6) 'Target Hub', tasking and tracking destructive targeting of identified enemies; (7) 'Orbit', management of information about enemy units; (8) 'Monitor Mobile', offline versions of Delta tooling; and (9) 'BattleSpace Management', planning and awareness tool for units.

Hosting Delta in the public cloud renders the service highly portable and provides the scale to receive extensive data inputs. It also mitigates the risk that a kinetic attack would cause significant service disruption: indeed, if Delta were run in private data centres, it would be more easily targeted than as a dynamic workload distributed across the public cloud. Ukraine has also proposed that Delta could be hosted on data centres outside the country. It is not clear from public reporting whether this has happened so far, although the author believes it is likely. Were a third country to host military workloads, it remains to be

54. Vadim Kushnikov, 'Ukraine Unveiled Its Own Delta Situational Awareness System', *Militarnyi*, 27 October 2022, <https://militarnyi.com/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system/>, accessed 20 October 2025.
55. Author interview with government official, online and London, 18 December 2024; author interview with former government official, online, 17 December 2024; Private multistakeholder seminar, online, 31 January 2025.
56. Stefan Soesanto, 'The Ukrainian Way of Digital Warfighting', ETH Zurich Center for Security Studies, 29 July 2024, <https://css.ethz.ch/en/center/CSS-news/2024/07/the-ukrainian-way-of-digital-warfighting-volunteers-applications-and-intelligence-sharing-platforms.html>, accessed 20 October 2025.

confirmed whether the host country would be a legitimate military target under international law.

Case Study 6: Finland's Cloud-Based Live-Virtual-Constructive Training

Since 2018, Finland's Air Force has used a Live-Virtual-Constructive (LVC) training architecture integrating live aircraft, mixed reality simulators and virtual scenarios.[57] This system allows pilots to use simulators that allow real-time training alongside aircraft in flight. The architecture leverages cloud computing to develop simulations and analyse performance analytics through live transmission of training data to the cloud.[58]

Virtual training capabilities help improve and maintain the preparedness of individual pilots and the whole force – especially since the expense and complexity of running air platforms constrains the rolling stock available for exercising.[59] There is some evidence that the higher the quality of LVC training, the more value pilots assign to it.

Visibility and Coherence of the Digital Estate

When designed effectively, the cloud can improve the visibility of a digital estate across systems and enable greater coherence.

A former Ukrainian government official explained that cloud migration equipped government cyber defenders with centralised management and automated cloud-native monitoring tools.[60] In contrast, self-hosted or on-premises systems often require more manual security assessments and monitoring. As a result, cyber defenders with proficiency in cloud systems can more easily generate and manage asset inventories. They can identify misconfigurations and vulnerabilities and mitigate risks. Moreover,

57. Varjo, 'Case Finnish Air Force: Future of Pilot Training with LVC & Mixed Reality', <https://varjo.com/blog/case-finnish-air-force-the-future-of-pilot-training-with-a-live-virtual-constructive-solution-in-mixed-reality/>, accessed 20 October 2025.
58. Author interviews with Finnish government officials, online, 24 April 2025.
59. Rogier Woltjer et al., 'The Future of Fighter Pilot Training? Live Virtual Constructive in Large Force Exercises: Perceived and Expected Training Value', *International Journal of Aerospace Psychology* (Vol. 34, No. 1, 2024), pp. 2–41.
60. Author interview with former Ukrainian government official, online, 17 December 2024.

on the public cloud, the system awareness and logging capabilities can improve the gathering of cyber threat intelligence (CTI).[61] One interviewee, a former official in a national technical body, further explained the order of magnitude difference in recording logs between on-premises or private cloud, and the public cloud. Hyperscale CSPs, they stressed, will in some instances retain logs for 10 years or more. Although the expectation is typically that larger systems are harder to protect, 'the scale of services actually gives you a defensive advantage, which is really counterintuitive'.[62] To directly access the gathered CTI, users have to pay – although, one can assume this is leveraged by the CSP to improve security, creating an indirect benefit for users.

Ukraine's cloud migration enabled international partners to provide cyber capability support. For example, under the UK–Ukraine Cyber Programme (UCP), cloud-native cyber-security tooling was provided to Ukraine's government, including malware analysis capabilities, virtual firewalls and EDR.[63] The UCP has since provided a model for the Tallinn Mechanism, a multicountry initiative supplying civilian cyber assistance, particularly through cloud-native tooling.[64]

Visibility afforded by cloud integration also provides the opportunity for greater coherence across digital estates. Traditional networks rely on individual asset owners or centralised manual processes which implement cross-network changes. As a result, mission-critical or urgent updates depend on human response times and bureaucratic processes. Cloud architectures can more effectively roll out updates across systems automatically and simultaneously. Although a centralised facility to roll out updates can improve system integrity, it can also create a single point of failure that can distribute faulty updates and cause systemic errors (see discussion of Crowdstrike in the section Impact of Concentration and Dependency). Dynamic updates in technology are increasingly important as software and hardware converge in multiple capabilities. For example, in 2017, during Hurricane Irma, Tesla pushed a software update to its Model S and X vehicles in Florida. The update unlocked full battery capacity, giving a lifeline to users who could now access an extra 30–40 miles of range.[65] Increased range was an improvement for users within the context; however, it was an augmentation to better adapt the vehicle to the mission, rather than a net enhancement. Allowing a battery to run down fully can present other issues to the vehicle, and in some cases,

61. Author interview with hyperscale CSP, London and online, 28 November 2024.
62. Author interview with former UK government official, online, 3 February 2025.
63. Foreign, Commonwealth & Development Office, 'UK Boosts Ukraine's Cyber Defences with £6 Million Support Package', 1 November 2022, <https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package>, accessed 20 October 2025.
64. Joseph Jarnecki, 'Innovations in International Cyber Support: Comparing Approaches and Mechanisms for Cyber Capability Support', in C Kwan et al. (eds), *2024: 16th International Conference on Cyber Conflict: Over the Horizon* (Tallinn: CCDOE Publications, 2024); Ministry of Foreign Affairs, Republic of Estonia, 'Tallinn Mechanism', <https://vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/tallinn-mechanism>, accessed 20 October 2025.
65. Simon Usborne, 'How Did Tesla Make Some of Its Cars Travel Further During Hurricane Irma', *The Guardian*, 11 September 2017.

reduce its lifespan. Extending this logic to the battlefield, opportunities become apparent. For example, capabilities could be remotely adapted to dynamic situations or deployed early, reducing the deployment cycle, and then systems could be iteratively improved during service. These examples depend on the underlying design of the capability and are not necessarily cloud-native. However, it can be assumed that the cloud plays a role when these instances are considered part of networked warfare. NATO's Supreme Allied Commander Transformation, Pierre Vandier, uses the Telsa example to demonstrate the tactical adaptability that could be achieved through similar design principles that permit dynamic updates.[66]

The possibility to integrate diverse systems was presented as an advantage offered by cloud technologies in several interviews with representatives from defence companies.[67] The conflict in Ukraine has demonstrated that in wartime, multiple commercial systems can be rapidly proliferated and procured to be used by combat or intelligence units, such as UAVs.[68] Integrating these systems – especially where devices have not been designed for interoperability – is critical to translating tactical capabilities into operational advantage (see Case Study 7). Nevertheless, other interviewees challenged this perspective, arguing that cloud migration can obscure more simple systems improvement, such as adopting modern architectures – for example, US Joint All-Domain Command and Control – that are not cloud-dependent.[69] Moreover, legacy defence products are more likely to run on old technology stacks that are less well suited to integration. Cloud adoption therefore can be correlated, but not necessarily causally linked, with improvements in systems integration.

66. *War on the Rocks*, 'Transforming NATO for the Future Fight', podcast, 12 February 2025.
67. Author interview with representative from the private sector, online, 29 November and 16 December 2024.
68. Kateryna Bondar, 'Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare', CSIS, 6 March 2025, <https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare>, accessed 20 October 2025.
69. Author interview with representative from private sector, London and online, 29 November 2024 and 24 January 2025.

Case Study 7: Avengers Platform

Avengers Platform is an AI system developed by Ukraine's Centre for Innovation and Development of Defence Technologies to automate the detection of enemy military assets.[70] The system comprises video and image processing, deep learning models, cloud-based infrastructure, user feedback loops and integration functions for compatibility with Delta (see Case Study 5).

Initially built by volunteer engineers, Avengers reportedly used public cloud services to rapidly prototype and train models on large datasets, enabling fast iteration without self-hosted hardware.[71] As the platform scaled, hybrid cloud infrastructure supported both experimentation and operational deployments.

Avengers processes video feeds from drones and stationary cameras, extracting frames, detecting objects and relaying data into Delta. Outputs are transmitted to Delta modules, including Vezha for decryption, or to Monitor to display on maps. Continuous frontline feedback enables real-time refinement of models and workflows.

The platform allows operators to do the following: detect thousands of targets per week; reduce duplicated tasks for analysts and better track workloads; tune detection sensitivity; support autonomous UAV and ISR development; and enable secure dataset sharing for AI development. Cloud computing ensures scalable, high-speed processing of its mission-critical workloads.

70. Ukraine Ministry of Defence, 'Kateryna Chernohorenko: 12 000 Enemy Targets are Detected by the Ukrainian Military Weekly with the Help of Artificial Intelligence', 23 September 2024, <https://mod.gov.ua/en/news/12-000-enemy-targets-are-detected-by-the-ukrainian-military-weekly>, accessed 20 October 2025.
71. Alga, 'Платформа Avengers: хто і як створював AI-платформу, що допомагає Силам Оборони України' ['Avengers Platform: Who Created and How an AI Platform that Helps the Defense Forces of Ukraine'], DOU, 10 December 2024, <https://dou.ua/forums/topic/51563/>, accessed 20 October 2025.

Strategic Considerations of Cloud Adoption for National Security

This chapter examines the practical obstacles and strategic considerations that shape governments' adoption of cloud capabilities for use in national security and defence.

Obstacles to Deploying Cloud Capabilities

Tactical Environment

Leveraging tactical use of the cloud for national security requires connectivity. Devices require links to servers that store and process data. Ukraine's Delta system (see Case Study 5) has demonstrated the value of accessing tactical-level, easily deployable and hardened high-bandwidth connectivity, in this case provided by Starlink.[72] Delta has succeeded in leveraging both large-scale remote public cloud and private cloud capabilities which are closer to the battlefield. Ukraine's effective deployment of Delta has motivated NATO to place more emphasis on refining its Allied Software for Cloud and Edge initiative[73] and its Digital Backbone.[74]

Nevertheless, in the modern battlefield, connectivity is contested and units often operate in degraded connectivity environments that limit access to remote computing.[75]

72. Stefan Soesanto, 'The Ukrainian Way of Digital Warfighting: Volunteers, Applications, and Intelligence Sharing Platforms', ETH Zurich Center for Security Studies, 29 July 2024, p. 43, <https://css.ethz.ch/en/center/CSS-news/2024/07/the-ukrainian-way-of-digital-warfighting-volunteers-applications-and-intelligence-sharing-platforms.html>, accessed 20 October 2025.
73. NATO, 'NATO Cloud Conference Advances Innovation and IT Security Across the Alliance', 21 January 2025, <https://www.nato.int/cps/en/natohq/news_232539.htm?selectedLocale=en>, accessed 20 October 2025.
74. NATO, 'NATO's Digital Transformation Implementation Strategy', 17 October 2024, <https://www.nato.int/cps/en/natohq/official_texts_229801.htm>, accessed 20 October 2025.
75. See, for example, Jack Watling and Noah Sylvia, 'Competitive Electronic Warfare in Modern Land Operations', *RUSI Occasional Papers* (January 2025), <https://www.rusi.org/explore-our-research/

To assure the availability of computing functions, armed forces leverage 'edge computing', a distributed model that places processing and storage closer to data sources.[76] Edge computing architectures, however, pose data security risks where systems are deployed on capturable devices. For example, the Ukrainian Armed Forces have captured Russian UAVs and other edge devices, including servers, that host AI models. Ukrainian engineers were then able to extract and analyse these models, helping to develop countermeasures.[77]

Recognising the need for tactical- and theatre-level edge computing, NATO commissioned Thales in 2021 to build Firefly.[78] This has been characterised as a deployable cloud capability; yet, it does not meet several of the NIST's guidelines: for example, it is neither scalable nor elastic.[79] While Firefly does demonstrate some characteristics of cloud computing (resource pooling, on-demand self-service, measured service), it illustrates the persistent propensity to label any networked system as the cloud.

On a national scale, connectivity is also an issue. Consider a country using cloud systems to improve resilience through data storage and the operation of digital services in foreign data centres. Disruption to the country's international connectivity would degrade its access to these capabilities. For countries bordering partners, this concern is primarily technical. However, if countries border adversaries, or rely heavily on subsea cables, there is an increased risk of disruption fuelled by geopolitical tensions. Damage to subsea cables in the Baltic Sea as a result of activities linked to Russia, and in the South China Sea linked to the activities of China, illustrate this point.[80]

Another tactical consideration concerns how cloud use-cases technically interoperate.[81] Where multiple digital solutions – cloud-native or not – are deployed, there is a risk that

publications/occasional-papers/competitive-electronic-warfare-modern-land-operations>, accessed 20 October 2025.

76. Frank T Johnsen, 'Towards Big Data in the Tactical Domain', NATO Science & Technology Organization (STO), 2019, <https://www.sto.nato.int/document/towards-big-data-in-the-tactical-domain/>, accessed 20 October 2025; NATO STO, 'NATO Science and Technology Organization (STO)', <https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-178/MP-IST-178-11.pdf>, accessed 20 October 2025.
77. Author interview with Ukrainian government official, online, 18 December 2024; Roman Kohanets, 'Ukrainian Intelligence Reveals Specifications of Russia's AI-Powered V2U Strike Drone', *United24 Media*, 9 June 2025, <https://united24media.com/latest-news/ukrainian-intelligence-reveals-specifications-of-russias-ai-powered-v2u-strike-drone-8994>, accessed 20 October 2025.
78. Thales, 'NATO Selects Thales to Supply Its First Defence Cloud for the Armed Forces', 25 January 2021, <https://www.thalesgroup.com/en/group/journalist/press-release/nato-selects-thales-supply-its-first-defence-cloud-armed-forces>, accessed 20 October 2025.
79. Mell and Grance, 'The NIST Definition of Cloud Computing', p. 6.
80. Aleksander Cwalina, 'Concerns Grow Over Possible Russian Sabotage of Undersea Cables', Atlantic Council, 12 September 2024, <https://www.atlanticcouncil.org/blogs/ukrainealert/concerns-grow-over-possible-russian-sabotage-of-undersea-cables/>, accessed 20 October 2025; Erin L Murphy and Matt Pearl, 'China's Underwater Power Play: The PRC's New Subsea Cable-Cutting Ship Spooks International Security Experts', CSIS, 4 April 2025, <https://www.csis.org/analysis/chinas-underwater-power-play-prcs-new-subsea-cable-cutting-ship-spooks-international>, accessed 20 October 2025.
81. See, for example, Calcara, 'NATO's Digital Modernisation', p. 5.

they will not function together, resulting in some capabilities being degraded or unavailable. For example, a 2023 report found that the F-22A and F-35 fighter jets have incompatible data protocols, impacting their ability to share information.[82] The same report provides other similar examples, and clearly demonstrates the particular difficulty in integrating older systems with newer platforms designed around digital- and software-first hyperconnectivity.[83] There will be an opportunity for cloud systems to provide a service which better connects diverse existing systems, while not adding additional challenges for users. NATO's Digital Backbone initiative and Digital Interoperability Framework support this effort.[84] Similarly, governments should encourage and require interoperability by design wherever possible through measures such as common commercial standards and protocols.[85]

At the enterprise level, technical interoperability is equally important. For example, a 2025 report recommended improving government services by leveraging aggregated data held in registries across multiple government departments.[86] Where government departments rely on commercial cloud storage solutions, it is critical that CSPs account for their customers' need to interoperate with their competitors' systems.[87] Efforts to ensure technical interoperability are being pursued by various stakeholders, for example, CSPs, competition authorities, customers, legislators and civil society. FINOS' Common Cloud Controls is one initiative that develops common controls for CSP services in the financial sector, and there is an ongoing NATO Industrial Advisory Group process addressing cloud interoperability.[88] Where multicloud systems are adopted, interoperable and secure identity access management protocols and services are critical. Partly because of cloud adoption, identity is becoming the new security perimeter; its effective management is therefore paramount to ensuring tactical effectiveness. Further research exploring its implementation where users are experiencing attempted disruption by adversaries would be beneficial.

In addition to connectivity and interoperability, the integrity of separation and encryption are fundamental to assuring tactical deployment of cloud solutions. Separation within (public) cloud infrastructures guarantees that customers can only

82. Soare, Singh and Nouwens, 'Software-Defined Defence', p. 7.
83. Soare, Singh and Nouwens, 'Software-Defined Defence'.
84. NATO, 'NATO's Digital Transformation Implementation Strategy', 20 February 2017, <https://www.nato.int/cps/en/natohq/official_texts_229801.htm>, accessed 20 October 2025.
85. Maia Hamin and Alphaeus Hanson, 'User in the Middle: An Interoperability and Security Guide for Policymakers', Atlantic Council, 24 June 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/user-in-the-middle-an-interoperability-and-security-guide-for-policymakers/#paths>, accessed 20 October 2025.
86. Henry Li et al., 'Governing in the Age of AI: Building Britain's National Data Library', Tony Blair Institute for Global Change, 25 February 2025, <https://institute.global/insights/tech-and-digitalisation/governing-in-the-age-of-ai-building-britains-national-data-library >, accessed 20 October 2025.
87. Author interviews with government officials, London and online, 13 and 19 December 2024 and 10 and 20 January 2025.
88. FINOS, 'FINOS CCC – Resources', <https://www.finos.org/common-cloud-controls-project>, accessed 20 October 2025; author interviews with government officials, London and online, 24 April 2025.

use and access the resources allocated to them. Where separation is ineffective, customers can breach cloud servers, or compute instances, belonging to different customers. In practice, interviews with representatives from national technical authorities reveal this is highly unusual; instead, breaches of cloud environments more often result from identity access management failures or from misconfigurations.[89] Secure encryption of cloud services is critical to customer trust, in the same way that it is crucial to technologies such as messaging services. Encryption is itself complex: considerations must include where encryption happens, who manages the 'keys', and what type of encryption is used. Commercial cloud providers are incentivised to ensure the robust encryption of customer data.[90] Primary interviews revealed that CSPs view data confidentiality as a competitive advantage and cite robust encryption as a partial guard against requests to disclose customer data to a foreign country.[91]

Legal Environment

Deploying cloud uses for national security and defence depends on their legality under international law. An interview with an expert on international law highlighted two possible problematic areas:

1. Does hosting defence or security workloads on commercial public cloud result in data centres becoming legitimate military targets during armed conflict? Ruben Stewart, an Advisor on Technology in Warfare to the International Committee of the Red Cross, explains that: 'If the line between civilians and the military becomes blurred, the principle of distinction, the obligations to differentiate between military objectives and civilian persons and objects, becomes harder to implement'.[92] In such a scenario, a public cloud targeted by a military force would create risk for other users.
2. If country A uses a capability based in a data centre in country B to attack country C, what responsibility does country B have under international law – if any? Is it legitimate for country C to identify the capability based in country B as a target? Does country B inadvertently become involved in the conflict? This question is made more complex since the hosting data centre will likely be privately owned, and not necessarily by a company based in country B. Moreover, the CSP operating the data

89. Author interviews with representatives from national technical bodies, online and London, 13 and 16 December 2024 and 10 January 2025; Google Cloud, 'Threat Horizons', H1 2024 Threat Horizons Report, <https://services.google.com/fh/files/misc/threat_horizons_report_h12024.pdf>, accessed 20 October 2025, p. 4.
90. There are some exceptions, including traffic inspection or where data travels unencrypted within a CSPs infrastructure. In each instance, encryption would present obstacles to CSPs.
91. Author interviews with representatives from hyperscale CSPs, London and online, 24, 29 and 30 January and 3 February 2025.
92. Ruben Stewart, 'The Shifting Battlefield: Technology, Tactics, and the Risk of Blurring Lines in Warfare', ICRC Humanitarian Law & Policy Blog, 22 May 2025, <https://blogs.icrc.org/law-and-policy/2025/05/22/the-shifting-battlefield-technology-tactics-and-the-risk-of-blurring-lines-of-warfare/>, accessed 20 October 2025.

centre is unlikely to know the precise activities of its customers.[93] This set of questions was also considered in the development of Estonia's data embassy.[94]

Each of these areas require further expert analysis, as it is beyond the remit of this paper to take a definitive position.

National legislation also presents obstacles to deploying cloud capabilities for national security and defence use. Localisation requirements – of data (processing, transit and storage), personnel or infrastructure – were cited extensively by interviewees as obstacles to public and, in some cases, private cloud adoption and can vary significantly by jurisdiction. For example, under the EU's GDPR regime, data subjects are protected even when their data is held outside their home jurisdiction. And, in the US, cloud facilities servicing some Department of Defense (DoD) uses must be operated by personnel who hold a specific clearance.[95] These restrictions have multiple impacts on deploying cloud capabilities. For example, in May 2025, an article highlighted that UK soldiers were prevented from practising electronic warfare techniques, including counter-drone jamming, because of restrictions under UK GDPR.[96]

Another factor that shapes governments' adoption of the cloud for national security and defence use is the physical security of data centres and access to them. These include minimum redundancy in energy supply, personnel vetting and facility hardening against environmental threats. Many CSPs will impose additional security or resilience measures, such as minimum distances between data centres to mitigate the impact of localised events and minimum numbers of data centres constituting a hyperscale region.[97] Regulatory and commercial requirements have an impact on governments' adoption of cloud capabilities and CSPs willingness to act as a supplier.

Interviews with former and existing government officials also indicated a misalignment between intuitive understandings of cloud computing risk and official positions.[98] Interviewees indicated that some government officials self-restrict – they

93. See, for example, AWS, 'Data Privacy Center', <https://aws.amazon.com/compliance/data-privacy/>, accessed 20 October 2025; Google Cloud, 'Google Cloud Privacy Notice', <https://cloud.google.com/terms/cloud-privacy-notice>, accessed 20 October 2025; Microsoft, 'Azure Customer Data Protection', <https://docs.azure.cn/en-us/security/fundamentals/protection-customer-data>, accessed 20 October 2025.
94. Author interview with representative from civil society, online, 7 October 2024; author interview with former Estonian government official, online, 28 January 2025.
95. Council of the European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)', Official Journal of the European Union Regulation (L 119/1, 4 May 2016), <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>, accessed 20 October 2025; Ron Rice, 'Clod Computing Security Requirements Guide', Defense Information Systems Agency, May 2018, <https://disa.mil/-/media/Files/DISA/News/Events/Symposium/Cloud-Computing-Security-Requirements-Guide.ashx>, accessed 20 October 2025.
96. Charles Clover, 'UK Military Prevented from Flying Drones Over Soldiers' Heads', *Financial Times*, 2 May 2025.
97. For a discussion of hyperscale regions, see, for example, AWS, 'Regions and Availability Zones', <https://aws.amazon.com/about-aws/global-infrastructure/regions_az/>, accessed 2 September 2025.
98. Author interviews with former and existing government officials, London and online, 13 and 19 December 2024 and 8, 20 and 29 January 2025.

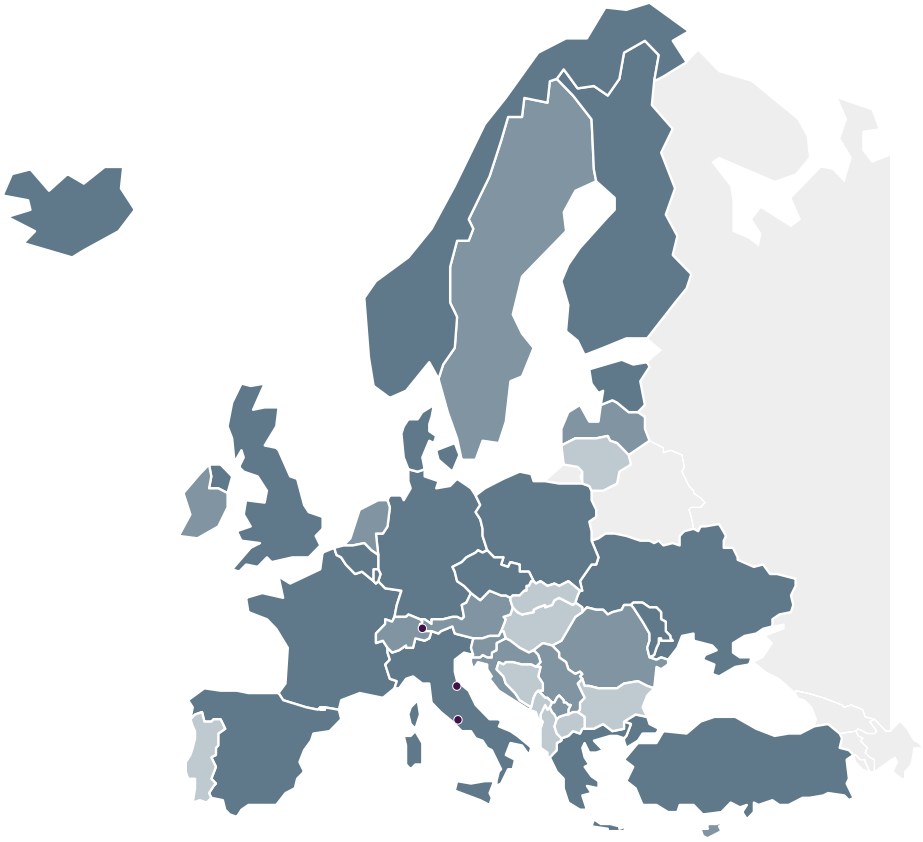
assume that government policy on the use of the cloud will be more restrictive than it is in practice. As such, the UK's Government Digital Service issued guidance in February 2025 that multi-region cloud and SaaS based outside the UK were permitted up to OFFICIAL classification 'to provide resilience, capacity and access to innovation'.[99] As the guidance indicates, this was not a change of policy: the UK has a long-standing strategic commitment to cloud-first across the government digital estate and at multiple classifications.[100] The need to issue this guidance indicates either a reluctance among officials to procure cloud capacity, or a gap in the understanding of existing legislation.[101] Releasing guidance intends to reassure and encourage government officials; as one interviewee with experience of the Estonian and Ukrainian governments explained, 'officials are compliance driven, [hence] explicit guidelines can mitigate concerns – lowering risk perception'.[102]

National approaches to cloud adoption differ between European countries. Figure 1 draws on open source data to illustrate measures that European governments have adopted to date (for example, specific cloud policies or adopting a cloud strategy). It is a reductive and high-level illustration intended to highlight the widespread attention afforded to cloud issues in Europe, not a scorecard of countries' performance on cloud. Many countries do not have specific legislation on the cloud; Ukraine is a notable exception (among others). Nevertheless, interviews with government officials indicate that this does not necessarily prevent governments from adopting the public or private cloud, instead it acts as an obstacle or a delaying factor.[103]

Where national legislation on cloud use for defence and national security differs, additional obstacles to binational and multinational cooperation appear, and joint capabilities are put at risk. For example, Sweden joined NATO in 2024 and has limited specific legislation on cloud use, although there are related regulations, including on information and service security, produced by the Civil Contingencies Agency.[104] A report by the law firm Cirio confirms accounts by interviewees, which indicated that Sweden has been reticent in cloud procurement for government in the absence of specific regulations, and will probably bring forward new legislation.[105]

99. Government Digital Service, 'Multi-Region Cloud and Software-as-a-Service (HTML)', Guidance, 5 February 2025, <https://www.gov.uk/government/publications/multi-region-cloud-and-software-as-a-service/multi-region-cloud-and-software-as-a-service-html>, accessed 20 October 2025.
100. *Ibid*.
101. Author interviews with government officials, online, 19 December 2024.
102. Author interview with government official, online, 8 January 2025.
103. Author interviews with government officials, London and online, 17 December 2024, 22 January and 24 April 2025.
104. Dahae Roland and Peter Nordbeck, 'Q&A: Cloud Computing Law in Sweden', Lexology Panoramic, 18 September 2023, <https://www.lexology.com/library/detail.aspx?g=05ec99f7-fdb4-47f0-bae9-063678182e75>, accessed 20 October 2025.
105. Author interview with representative from private sector, online, 29 November 2024; David Frydlinger and Caroline Olstedt Carlström, 'Cloud Services, Publicity, and Confidentiality in the Public Sector', Cirio, 12 May 2020, <https://cirio.se/en/news/cirio-slapper-sin-rapport-om-molntjanster-offentlighet-och-sekretess-i-offentlig-sektor>, accessed 20 October 2025.

Figure 1: European Approaches to Cloud Adoption



Score 0 - No evidence of national cloud policy or strategy. Cloud technologies are likely used by government entities in isolation.

Score 1 - Cloud mentioned in a national digital, ICT or e-government strategy.

Score 2 - Some cloud policies (Memorandums of Understanding with CSPs, pilots, initial frameworks) but no published government strategy on the cloud.

Score 3 - Published national cloud strategy and/or government cloud marketplace or other centralised procurement and assurance framework.

Source: Author generated using open source material.

Source: Note: To identify relevant information about each country, targeted and systematic online searches were conducted. Search phrases consisted of '[country name] government cloud'; '[country name] cloud strategy'; '[country name] government cloud strategy'; '[country name] cloud migration' and '[country name] government cloud computing'; '[country name] cloud adoption'. The author accepts this information may be incomplete or partial.

One interviewee who was familiar with NATO's cloud ambitions highlighted the risk that such legislation would create national restrictions, preventing Sweden's use of cloud capabilities alongside those presently developed across the Alliance.[106] The risk

106. Author interviews with former and existing government officials, online, 29 November 2024 and 24 April 2025.

that countries' legislation prevents access to cloud use is also illustrated by the Global Combat Air Programme, a joint initiative between the UK, Italy and Japan to develop a sixth-generation fighter. At one stage of the programme, the partners were not able to run a shared digital platform because of perceived ambiguity and misalignment in domestic legislation on classifications and encryption controls for digital systems.[107]

Concentration and Dependence

This paper finds that questions of concentration and dependence synthesise most strategic concerns of decision-makers in government and industry regarding the role of the cloud in national security and defence. European national competition authorities, including in the UK and the Netherlands, have released reports outlining concerns about cloud market concentration,[108] with one NGO having reiterated these concerns with specific reference to national security.[109] Interviews with European government officials for this paper echo these points.[110]

Definition: Concentration

Using a small number of providers for most of the volume of use (for example, workloads and data storage). This can include situations where alternative options are available.

Definition: Dependence

Using a service where there are limited or no alternatives, and/or where the cost of change is prohibitive.

Neither concentration nor dependence are unique to cloud markets in the context of national security. Self-hosted solutions can also be concentrated and dependent, as can the critical components or supporting infrastructure of cloud computing. For example, in Q1 2025, the Taiwanese multinational semiconductor manufacturing and design

107. Joseph Jarnecki, Philip Shetler-Jones and Pia Hüsch, 'What Next for the UK–Japan Cyber Partnership?', *RUSI Occasional Papers* (September 2024), p. 31, <https://www.rusi.org/explore-our-research/publications/occasional-papers/what-next-uk-japan-cyber-partnership>, accessed 20 October 2025.
108. Netherlands Authority for Consumers and Markets, 'Market Study into Cloud Services', ACM/INT/440323, 5 September 2022, p. 4, <https://www.acm.nl/en/publications/market-study-cloud-services>, accessed 20 October 2025; Competition and Markets Authority, 'Cloud Services Market Investigation'.
109. Max von Thun and Claire Lavin, 'Engineering the Cloud Commons: Tackling Monopoly Control of Critical Digital Infrastructure', Open Markets Institute, May 2025, p. 20, <https://www.openmarketsinstitute.org/publications/report-rethink-regulatory-approach-to-essential-cloud>, accessed 20 October 2025.
110. Author interviews with European government officials, online and London, 16 and 19 December 2024, 10 and 22 January and 24 April 2025.

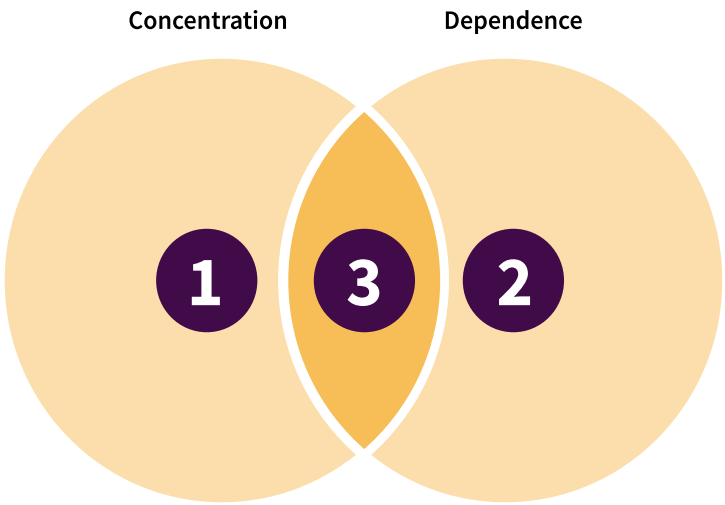
company TSMC held 67.6% of the global wafer foundry market.[111] In the same quarter, the US technology company NVIDIA had around 92% of the global GPU market.[112] Most undersea cables are built by four companies – Alcatel, SubCom, NEC Corporation and Huawei Marine Networks.[113] These inputs and enablers of cloud computing merit acknowledgement. Several interviewees for this paper have argued, however, that CSPs themselves are most salient because they can present significant cascading risks, as they have control over the live provision of extensive computing functions.[114] While this argument is easy to grasp, it is also the case that other modern national security and defence platforms allow for software updates by providers, potentially creating a similar, but more isolated, risk.[115] Additionally, many non-connected and non-digitised systems or products purchased by national security or defence organisations rely on supply chains where the original equipment manufacturer can degrade or disable the capability by withdrawing its involvement, for instance by not providing repair parts – albeit there is a longer delay before impact (as compared with CSPs).

All CSPs that were interviewed for this paper contested the premise that their services would be switched off – especially for government national security use.[116] Research participants from hyperscale CSPs referenced their sovereign cloud solutions and other guarantees of service continuity.[117] Open source data-gathering did not identify instances where cloud services for national security were unilaterally suspended. Nevertheless, as detailed below, companies can be required to limit access by government mandates, illustrated by restrictions on high-performance technology exports to China, and have previously withdrawn commercial provision in moments of

111. A wafer is a thin slice of semiconductor. See Chen Cheng-hui, 'TSMC Still Top Foundry, with 67.6% Market Share', Taipei Times, 10 June 2025, <https://www.taipeitimes.com/News/biz/archives/2025/06/10/2003838326>, accessed 21 October 2025
112. Faizan Farooque, 'Nvidia Secures 92% GPU Market Share in Q1 2025,' yahoo! finance, <https://finance.yahoo.com/news/nvidia-secures-92-gpu-market-150444612.html>, accessed 21 October 2025.
113. Bradley Martin et al., *Supply Chain Interdependence and Geopolitical Vulnerability: The Case of Taiwan and High-End Semiconductors* (Santa Monica, CA: RAND Corporation, 2023); Daniel F Runde, Erin L Murphy and Thomas Bryja, 'Safeguarding Subsea Cables: Protecting Cyber Infrastructure Amid Great Power Competition', CSIS, 16 August 2024, <https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition>, accessed 20 October 2025; Hassan Mujtaba, 'NVIDIA Dominates AIB GPU Market With 92% Share in Q1 2025, AMD Drops to 8% & Intel to 0%', WCCF Tech, 5 June 2025, <https://wccftech.com/nvidia-dominates-aib-gpu-market-share-in-q1-2025-amd-intel-drop/>, accessed 20 October 2025.
114. Author interview with representative from civil society, online, 28 November 2024; author interviews with academics, London and online, 17 December 2024, 9 January and 7 February 2025.
115. Soare, Singh and Nouwens, 'Software-Defined Defence', pp. 5–6.
116. Author interview with representatives from CSPs, online and London, 29 October 2024, 29 and 30 January and 3 February 2025.
117. Author interview with representatives from CSPs, online and London, 28 November 2024, 29 and 30 January and 3 February 2025. For the specific service guarantees cited by CSPs, see, for example, AWS, 'More Choice for Your Data', <https://aws.amazon.com/compliance/europe-digital-sovereignty/>, accessed 20 October 2025; Google Cloud, 'Sovereign Cloud', https://cloud.google.com/sovereign-cloud>, accessed 20 October 2025; Brad Smith, 'Microsoft Announces New European Digital Commitments', Microsoft blog, 30 April 2025, <https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/>, accessed 20 October 2025.

political tension, as with the departure by many companies from the Russian market following the invasion of Ukraine. Furthermore, concentration and dependence are not mutually exclusive (Figure 2).

Figure 2: Concentration, Dependence and Choice



Source: The author.

Using Figure 2 as a framework, three generic scenarios for cloud adoption emerge:

1. **Concentrated but not dependent**. In this scenario, users select one or a few providers – when other options are available – for most of their computing needs, such as data storage and processing. There are valid reasons for users to choose concentration, for instance, to access advanced capabilities and for the purpose of scale or simplicity (see Chapter one).
2. **Dependent and not concentrated**. In this scenario, services which do not make up most of the use by volume but are critical for operations and have few or no alternatives, can create cascading impacts in the event of failure. Moreover, customers are locked into these services, for instance because of prohibitive costs to changing providers (see 'Lock-In' section).
3. **Concentrated and dependent**. In this scenario, users store most of their workloads and data with a single provider or a few providers. There are no alternatives or only limited ones, and/or there are prohibitive costs to changing providers.

Whereas the question of concentration primarily concerns technical challenges, the question of dependence is shaped by political perceptions. How providers are categorised has an impact on whether users understand themselves to be in a position of dependence. For example, CSPs can have different products and security track records, yet can be grouped together because they have a common country of origin. In line with this framing, several European officials who engaged in the research for this

paper indicated a dependence on 'American CSPs', designating them as one single entity rather than distinguishing between individual US CSPs.[118]

Impact of Concentration and Dependence

The following section outlines the role of concentration and dependence in shaping governments' decision-making on cloud adoption for national security, primarily with relation to the hyperscale cloud. In most cases, impacts are assessed here using examples observed after events. However, some impacts have not yet been observed but are anticipated or assessed to be likely based on evidence that is not yet public. The author therefore acknowledges that the following examples have variable analytical value.

Outages

Outages suspend or degrade access to services or data. Data-gathering for this paper does not categorically indicate whether cloud systems or self-hosted and on-premises systems experience more outages. Interviews with national security stakeholders suggest that systems experience less downtime on the public cloud, benefitting from fault tolerance and automated recovery – features that are also available in a diluted format in private cloud models.[119] Nevertheless, cloud outages have a wider impact where CSPs host multiple organisations' workloads and data. Table 1 outlines examples of CSP outages. These examples are illustrative and are not a representative sample.

Any protracted or widespread outage affecting multiple or critical sectors have a bearing on national security. In 2024, CrowdStrike pushed a defective content update to its Falcon EDR SaaS – impacting around 8.5 million Microsoft Windows hosts on the Azure platform and creating costs for businesses, including service disruption and remediation, estimated at $10 billion.[120] Disrupted sectors included water, aviation, banking and transport. This incident illustrates the potential widespread consequences of outages when technologies are pervasive and have privileged access to customer networks. Several interviewees used the CrowdStrike incident to justify their concerns about outages of concentrated CSP services that would result in a similar scale of impact.[121]

118. Author interviews with officials, London and online, 10 January and 24 April 2025.
119. Author interviews with private sector, Lonon and online, 25 and 29 November and 16 December 2024.
120. David Weston, 'Helping Our Customers Through the Crowdstrike Outage', Microsoft, 20 July 2024, <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>, accessed 20 October 2025; Financial Conduct Authority, 'CrowdStrike Outage: Lessons For Operational Resilience', 31 October 2024, <https://www.fca.org.uk/firms/operational-resilience/crowdstrike-outage-lessons-operational-resilience>, accessed 20 October 2025; Lian Kit Wee, 'Here Comes the Wave of Insurance Claims for the Crowdstrike Outage', *Business Insider*, 22 July 2024, <https://www.businessinsider.com/businesses-claiming-losses-crowdstrike-outage-insurance-billions-losses-cyber-policies-2024-7>, accessed 20 October 2025.
121. Data-gathering workshop, London, 19 February 2025; author interviews with government officials, online, 13 and 19 December 2024.

Table 1: Cloud Outages

CSP	Date	Impact	Cause
GCP (Google Cloud Platform)	2019[122]	Multiple service regions unavailable	Misconfigured network capacity update
AWS	2020[123]	Regional outage of Kinesis (US-East-1), impacting multiple services	Capacity addition to Kinesis above operating system limit
OVH	2021[124]	Facility fire destroys one data centre and damages others, creating widespread outages and catastrophic data loss	Unknown. The fire began in the battery and power supply premises, no automatic extinguishing system was present
AWS	2021[125]	Regional disruption or latency on SaaS (Netflix, Alexa, Slack) and AWS services (for example, EC2 and Lambda)	Internal network congestion and overload
GCP	2021[126]	Global Google services impacted. GCP customers faced errors, latency or disruption	Bug in the system that manages customer configuration rules
Azure	2023[127]	Multiple regions and services including Microsoft 365. Impact on government services where they rely on public cloud	Faulty wide area network update
Azure	2023[128]	Regional (South East Asia) outage of workloads and data	Cooling failure at Azure availability zone (data centres)
Oracle	2025[129]	Outage of Oracle's identity platform in Germany's central region	Unconfirmed

Source: The author.

Some national security workloads or data have a near-zero tolerance for fault or disruption. For mission-critical systems, maximising confidentiality, integrity and availability takes precedence over cost or user experience. Where this is the case, the

122. Google Cloud, 'Google Cloud Networking Incident #19009', 5 June 2020, <https://status.cloud.google.com/incident/cloud-networking/19009>, accessed 20 October 2025.
123. AWS, 'Summary of the Amazon Kinesis Event in the Northern Virginia (US-EAST-1) Region', 25 November 2020, <https://aws.amazon.com/message/11201/>, accessed 20 October 2025.
124. Peter Judge, 'The OVHcloud Fire Still Smolders', DCD, 28 March 2024, <https://www.datacenterdynamics.com/en/analysis/ovhcloud-fire-france-data-center/>, accessed 20 October 2025.
125. AWS, 'Summary of the AWS Service Event in the Northern Virginia (US-EAST-1)-Region', 10 December 2021, <https://aws.amazon.com/message/12721/>, accessed 20 October 2025.
126. Google Cloud, 'Global: Experiencing Issue with Cloud Networking', 16 November 2021, <https://status.cloud.google.com/incidents/6PM5mNd43NbMqjCZ5REh>, accessed 20 October 2025.
127. Microsoft Azure, 'Azure Status History', Post Incident Review (PIR) – Azure Networking – Global WAN Issues, Tracking ID: VSG1-B90, <https://azure.status.microsoft/en-us/status/history/>, accessed 23 July 2025; Microsoft Reactor, 'Azure Incident Retrospective: WAN Issues, January 2023 (Tracking ID: VSG1-B90)', YouTube, 26 June 2024, <https://www.youtube.com/watch?v=J4knDk1vfPo>, accessed 20 October 2025.
128. Microsoft Reactor, 'Azure Incident Retrospective: Datacenter Cooling in Southeast Asia, Feb 2023 (Tracking ID: VN11-JD8)', YouTube, 26 June 2024, <https://aka.ms/AIR/VN11-JD8>, accessed 20 October 2025.
129. Lindsay Clark, 'European Customers Report Oracle Cloud Identity Outage, Big Red is Silent', The Register, 19 May 2025, <https://www.theregister.com/2025/05/19/oci_outage_europe/>, accessed 20 October 2025.

consensus among interviewees was that governments should pursue a hybrid multicloud strategy with redundancy or failover in on-premises systems. Multicloud and hybrid models, however, are more expensive and complex than using a single provider, for example, because there are more data-exchange points that require trust and identity management. Nevertheless, when properly leveraged they are highly impactful for resilience. According to normal accident theory, major accidents are inevitable within complex systems. Small failures – which cannot be designed out – overlap with other systems and cascade, creating further failures.[130] Conditions that increase the likelihood of this scenario are system complexity, tight coupling and catastrophic potential – in other words, conditions found in the cloud. As a result, some CSPs have made efforts to adopt chaos theory by artificially generating random failures in live environments to test system resilience.[131] The author strongly advocates for more widespread adoption of such precautionary practices.

Leverage

In situations of dependency, CSPs have leverage over customers. The impacts of this leverage discussed below are financial and geopolitical.

Financial

Where companies provide services that enjoy inelastic demand – in other words, price increases hardly impact consumption – companies are incentivised to increase prices. Because contracts are often negotiated individually – sometimes at a government departmental level – it is difficult to ascertain systematically whether the cost of cloud services for national security use has increased or decreased in recent years. In May 2025, several Danish cities and a German state government chose to move away from software in the Microsoft productivity suite, citing rising costs and concerns about digital sovereignty.[132] National competition authorities have found that CSPs have also used their market power to condition the decision-making of user organisations; for example, Ofcom found that AWS delayed providing WarnerMedia with a platform for its streaming service on the Amazon Fire TV device until it agreed to extend its cloud hosting contract.[133] However, the author has not found open source evidence of similar activities against national governments.

130. Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton, NJ: Princeton University Press, 1999).
131. Ben Pollins, 'Bringing Order to Chaos: A Practical Guide to Chaos Testing in the Cloud', capacitas, 13 June 2025, <https://www.capacitas.co.uk/insights/bringing-order-to-chaos-a-practical-guide-to-chaos-testing-in-the-cloud>, accessed 20 October 2025.
132. *Economic Times*, 'After Danish Cities, Germany's Schleswig-Holstein State Government to Ban Microsoft Programs at Work', 13 June 2025, <https://economictimes.indiatimes.com/news/international/us/after-danish-cities-germanys-schleswig-holstein-state-government-to-ban-microsoft-programs-at-work/articleshow/121833653.cms?from=mdr >, accessed 20 October 2025.
133. Ofcom, 'Cloud Services Market Study', para 6.96.

One interviewee warned that the spending power of hyperscale CSPs empower them relative to smaller European countries: expenditures of the largest CSPs on compute build-out (building computing power) or R&D far exceed those of most European countries.[134] Spending power, however, is not an exact measure of power or influence. Further research is required to ascertain the experience of smaller countries when procuring from the largest multinational CSPs; other factors, such as information symmetry, may be more significant. Currently, CSPs offer limited detailed systems documentation, which can create challenges for customers that want a thorough overview of their security posture or want to move to another provider. The normalisation of this opacity across the market provides individual CSPs with leverage when negotiating with customers. Nevertheless, there are well-grounded concerns by CSPs that excessive openness could pose a security risk. The author suggests that in some national security uses, a perfect balance has yet to be achieved. A detailed study on the structural power of hyperscale CSPs would therefore be beneficial.[135]

Political

Dependence on a concentrated service, such as on a single CSP or a limited group of CSPs, can create risks to availability and data confidentiality.

Service Availability

National security uses of the cloud require reliable availability. Where services are concentrated, relevant providers have significant responsibility. Because of the nature of the market, hyperscale IaaS providers play a critical role and invest significantly to achieve service integrity and continuity (see Chapter one). Nonetheless, the fact that they control concentrated services means that their choices have meaningful downstream impacts: one interviewee presented this as a 'single point of failure' risk.[136] As outlined above, this also has relevance to the critical components and supporting infrastructure of the cloud – illustrated by the US export controls on advanced computing components to China.[137]

In 2018 it was revealed that Google had a contract – 'Project Maven' – with the US DoD to deliver a capability to analyse drone footage using AI to help identify potential

134. Author interview with representative from civil society, online, 5 February 2025; see also Matthias Bauer, Fredrik Erixon and Dyuti Pandya, 'The EU's Trillion Dollar Gap in ICT and Cloud Computing Capacities: The Case for a New Approach to Cloud Policy', European Centre for International Political Economy, May 2024, <https://ecipe.org/publications/eu-gap-ict-and-cloud-computing/>, accessed 20 October 2025.
135. For a discussion of structural power, see Srijan Shukla, 'Revisiting Structural Power in the Global Economy: It's Multinationals, Not States', *Journal of International Affairs* (Vol. 75, No. 1, 2022).
136. Author interview with representative from civil society, online, 26 November 2024.
137. US Department of Commerce, Bureau of Industry and Security, 'Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)', 7 October 2022.

targets and provide real-time battlefield intelligence.[138] Thousands of Google employees protested about the company's involvement and eventually the contract was not renewed.[139] The largest CSPs are not primarily defence companies: their products are dual-use and civilian uses make up the majority of their revenue. The decision to not continue Project Maven reflects a concern expressed by several interviewees about CSP mission commitment when faced with commercial trade-offs.[140]

In 2021, following the storming of the US Capitol, Parler – a conservative social network – was deplatformed by several technology companies. Apple and Google removed it from their app stores and AWS suspended its account, removing access to cloud hosting.[141]

In May 2025, the Microsoft exchange email of the International Criminal Court (ICC) Chief Prosecutor Karim Khan was blocked, following the US sanctions justified by the ICC's 'illegitimate and baseless actions targeting America and our close ally Israel'.[142] Multiple media outlets have reported that Microsoft was responsible for the action and blocked the account to comply with sanctions.[143] The company has denied involvement in 'the cessation of services', but at the time of writing, neither Microsoft nor the ICC had provided an explanation.[144] While the reason for the block remains unclear, this example adds weight to arguments by interviewees that the imposition of sanctions by the US to restrict access to cloud services is a valid risk.[145]

Anxieties in Europe about cloud service availability primarily result from a breakdown of trust in the current US administration. European stakeholders interviewed for this

138. Irja Malmio, 'Ethics as an Enabler and a Constraint – Narratives on Technology Development and Artificial Intelligence in Military Affairs Through the Case of Project Maven', *Technology in Society* (Vol. 72, February 2023).
139. *BBC News*, 'Google "to End" Pentagon Artificial Intelligence Project', 2 June 2018.
140. Author interviews with representatives from civil society, online, 26 November 2024 and 8 January 2025.
141. Jordan Novet, 'Parler's De-Platforming Shows the Exceptional Power of Cloud Providers Like Amazon', CNBC, 16 January 2021, <https://www.cnbc.com/2021/01/16/how-parler-deplatforming-shows-power-of-cloud-providers.html>, accessed 20 October 2025; Caroline Donnelly, 'Parler Sues AWS for Anti-Trust and Breach of Contract After Amazon Public Cloud Ban Takes it Offline', 12 January 2021, <https://www.computerweekly.com/news/252494666/Parler-sues-AWS-for-anti-trust-and-breach-of-contract-after-Amazon-public-cloud-ban-takes-it-offline>, accessed 20 October 2025.
142. The White House, 'Imposing Sanctions on the International Criminal Court', 6 February 2025, <https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/>, accessed 20 October 2025.
143. Owen Sayers, 'Microsoft's ICC Email Block Reignites European Data Sovereignty Concerns', *ComputerWeekly.com*, 23 May 2025, <https://www.computerweekly.com/opinion/Microsofts-ICC-email-block-reignites-European-data-sovereignty-concerns>, accessed 20 October 2025; DigWatch, 'Microsoft Allegedly Blocked the Email of the Chief Prosecutor of the International Criminal Court', 25 May 2025, <https://dig.watch/updates/microsoft-allegedly-blocked-the-email-of-the-chief-prosecutor-of-the-international-criminal-court>, accessed 24 May 2025.
144. Sam Clark, 'Microsoft Didn't Cut Services to International Criminal Court, Its President Says', *Politico*, 4 June 2025, <https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/>, accessed 20 October 2025.
145. Author interviews with representatives from civil society, London and online, 29 October, 26 and 28 November and 8 and 28 January 2025; author interviews with government officials, London and online, 13 and 18 December 2024 and 10 January, 3 February and 24 April 2025; author interviews with academics, London and online, 18 December 2024 and 9 January and 7 February 2025.

paper have indicated that Europe's renewed digital and data sovereignty priorities are a product of this environment; statements by European policymakers also resonate with this finding.[146] To counteract this sentiment, US companies have made commitments to protect European users and outlined new product offerings.[147] This paper asks whether this is a Sisyphean task, and if trust can become resilient to political change. Meanwhile, other compelling reasons drive continued procurement of US CSPs in Europe, such as advanced capabilities, scale and lack of substantial alternatives. Other critical industries, notably financial services, illustrate how foreign companies operating services that impact national security can secure the trust of governments outside their country of origin. Cloud computing will increasingly be viewed as a critical industry, utility or public good and CSPs should therefore look to leverage the experience of other companies becoming trusted partners of foreign governments. One approach is to consider institutional trust theory, which provides a framework to improve confidence based on sensitivity to factors including experience, performance, social context, institutional design, transparency and relationship type.[148] CSPs aiming to improve and preserve customer relations would benefit from structuring behaviours and interactions with reference to this theory.

Data Confidentiality

Use of cloud services is predicated on data confidentiality. Where data is subject to legal controls – namely, personally identifiable information and classified material – confidentiality is a greater priority. The primary consideration that European interviewees raised about data confidentiality was jurisdictional risk, specifically that international customer data would be compromised based on US legal orders.[149]

146. Author interviews with government officials, London and online, 8 and 22 January and 24 April 2025; author interviews with academics, London and online, 9 January and 7 February 2025; data-gathering workshop, London, 19 February 2025. See also Mark Ballard, 'EU Promotes Plan to Usurp US Big Tech With Digital Markets', *ComputerWeekly.com*, 22 November 2024, <https://www.computerweekly.com/news/366616313/EU-promotes-plan-to-usurp-US-Big-Tech-with-digital-market>, accessed 20 October 2025; European Parliament, 'Strategic Dependence: Brussels Losing Its Soul in American Clouds (Cloud Services of Microsoft, AWS/Amazon, Google)', 8 May 2025, <https://www.europarl.europa.eu/doceo/document/E-10-2025-001866_EN.html>, accessed 20 October 2025.
147. See, for example, AWS, 'AWS Digital Sovereignty: More Choice for Your Data', <https://aws.amazon.com/compliance/europe-digital-sovereignty/>, accessed 20 October 2025; Judson Althoff, 'Announcing Comprehensive Sovereign Solutions Empowering European Organizations', Microsoft blogs, 16 June 2025, <https://blogs.microsoft.com/blog/2025/06/16/announcing-comprehensive-sovereign-solutions-empowering-european-organizations/>, accessed 20 October 2025; Google Cloud, 'Sovereign Cloud'.
148. See, for example, Roderick M Kramer and Tom R Tyler, *Trust in Organizations: Frontiers of Theory and Research* (Thousand Oaks, CA: Sage Publications, 1996); Henry Farrell, 'A Theory of Institutions and Trust', in *The Political Economy of Trust: Institutions, Interests, and Inter-Firm Cooperation in Italy and Germany* (Cambridge: Cambridge University Press, 2009), pp. 23–62.
149. Author interviews with academics, online,18 December 2024 and 9 and 10 January and 7 February 2025; author interviews with government officials, London and online, 16 and 19 December 2025; data-gathering workshop, London, 19 February 2025.

The limited public reporting on the subject stresses that the US Cloud Act is a far-reaching 'threat' to European data sovereignty.[150] This claim is exaggerated. The Cloud Act permits law enforcement (rather than national security entities) to access digital content from service providers when it relates to an individual connected with a criminal case, and when a warrant has been issued for specific data.[151] It does not allow mass surveillance or an expansion of national security powers, and providers are able to challenge warrants where they conflict with national (non-US) legislation.[152]

More relevant to national security, the Foreign Intelligence Surveillance Act (FISA) authorises electronic surveillance on 'foreign powers' based on national security priorities. Under section 702, FISA allows authorities to issue production orders to CSPs for customer data.[153] According to researcher Johan David Michels, CSPs are not able to disclose when they have been compelled under section 702.[154] This, he argues, means that CSPs' commitments to be transparent about production orders under US legislation are less meaningful.[155] Nevertheless, while FISA is a legitimate concern, the threshold for its invocation is high and orders to provide customer information can still meet with resistance from CSPs. Other practical obstacles include customers employing robust encryption for their data, which offers additional protections.

Ultimately, the Cloud Act, FISA and other legislation are less important than trust built through shared experience, the geopolitical context and sentiment. Numerous European stakeholders interviewed for this paper were sceptical about US reassurances concerning data confidentiality, raising the example of the surveillance of the mobile device of then-German chancellor, Angela Merkel, as well as the revelations of mass surveillance under the Prism program.[156]

150. See, for example, Conceptboard, 'The US Cloud Act: Threatening European Data Protection', 22 September 2023, <https://conceptboard.com/blog/us-cloud-act-european-data-protection/>, accessed 20 October 2025; Anna Desmarais, 'Is Overreliance on US Big Tech a Threat to Europe? The Netherlands May Soon Find Out', *euronews*, 26 February 2025, <https://www.euronews.com/next/2025/02/27/is-overreliance-on-us-big-tech-a-threat-to-europe-the-netherlands-may-soon-find-out>, accessed 20 October 2025.
151. Clarifying Lawful Overseas Use of Data Act or the CLOUD Act', introduced at 115th Congress, 2017–2018, <https://www.congress.gov/bill/115th-congress/house-bill/4943>, accessed 20 October 2025.
152. BSA and Software Alliance, 'The CLOUD Act and the European Union: Myths vs. Facts', February 2019, <https://www.bsa.org/files/policy-filings/02282019CLOUDACTEUMythvsFact.pdf>, accessed 20 October 2025.
153. US Congress, 'FISA Amendments Act of 2008', <https://www.congress.gov/bill/110th-congress/house-bill/6304>, accessed 20 October 2025.
154. Johan David Michels, 'Sovereign Cloud for Europe', Broadcom, Queen Mary University of London, February 2025, https://www.vmware.com/docs/sovereign-cloud-report; see also Amazon, 'Law Enforcement Information Requests', <https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF>, accessed 20 October 2025; Google, 'Global Requests for User Information', < https://transparencyreport.google.com/user-data/overview?hl=en_GB>, accessed 20 October 2025; Microsoft, 'Government Requests for Customer Data Report', <https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data>, accessed 20 October 2025.
155. Michels, 'Sovereign Cloud for Europe', p. 10.
156. Author interviews with government officials, London and online, 13 and 18 December 2024 and 24 April 2025; author interview with academics, online, 17 December 2024 and 10 January 2025; private multistakeholder seminar, online, 31 January 2025; Glenn Greenwald and Ewen MacAskill, 'NSA Prism

Lock-In

When customers experience prohibitive barriers to changing cloud services – financial or otherwise – this can be described as lock-in. National competition authorities in the UK, France and other countries have found that 'customers face both commercial and technical barriers' to the use of the multicloud or to switching providers.[157] Academic research has reinforced these findings,[158] and officials interviewed for this paper indicated that they were highly concerned with the lock-in for national security use-cases.[159] Their concerns related more to data and service availability than to the risk of price increases, although these were also mentioned.[160] There are multiple forms of lock-in:

- **Technical**. Where data or workloads cannot be (easily) migrated from one CSP network to another due to technical barriers, such as the extensive use of proprietary systems with no clear substitute.
- **Commercial**. Where customers face contractual or financial barriers to reducing or cancelling a cloud service (for example, egress fees), or where procurement rules erroneously limit access to providers.
- **Organisational**. Where cultural habits and institutional structures incentivise officials to remain with the same provider.
- **Personnel and skills**. Where employees of organisations that purchase cloud computing are skilled in one CSP's products, and, in some instances, these skills are not transferrable.

None of these forms of lock-in necessarily prevents migration from or between clouds, but they certainly create friction. Additionally, these lock-ins are not all a function of the CSP models; most can result from customer decision-making. One notable example is how Ukraine deliberately designed Delta (see Case Study 5) as a 'cloud agnostic' service, where there are little to no proprietary systems involved and Delta engineers are confident they could move to any IaaS provider with minimal lead time.[161] Delta was also designed to be cloud-agnostic because the provision in Ukraine's 2022 Law on Cloud Services that allows government data to be delocalised will lapse six months

Program Taps in to User Data of Apple, Google and Others', *The Guardian*, 7 June 2013; *Reuters*, 'U.S. Spy Agency Tapped German Chancellery for Decades: WikiLeaks', 9 July 2025.

157. Autorité de la concurrence, 'Cloud Computing: the Autorité de la Concurrence Issues Its Market Study on Competition in the Cloud Sector', 29 June 2023, <https://www.autoritedelaconcurrence.fr/en/press-release/cloud-computing-autorite-de-la-concurrence-issues-its-market-study-competition-cloud>, accessed 20 October 2025; Competition and Markets Authority, 'Cloud Services Market Investigation', para. 17.
158. See, for example, Hedaia-t-Allah Nabil Abd Al Ghaffar, 'Government Cloud Computing and National Security', *Review of Economics and Political Science* (Vol. 9, No. 2, 2024), pp. 116–33; Ferreira Gome and Okano-Heijmans, 'Too Late to Act?'; Calcara, 'NATO's Digital Modernisation'.
159. Author interviews with government officials, London and online, 13, 16, 17, 18 and 19 December 2024 and 10 January 2025; private multistakeholder seminar, online, 31 January 2025.
160. Author interviews with government officials, online, 13 and 16 December 2024.
161. Author participation in closed-door discussions.

after martial law ends.[162] This cloud-agnostic design, however, can limit access to transformative capabilities, creating a question of trade-offs and prioritisation.

Lock-in is not necessarily a drawback. Competitive dynamics can produce concentrated markets where large providers leverage economies of scale to minimise cost and invest in security and advanced capabilities (see Chapter one). Lock-in is disadvantageous where it leads to other outcomes, including more catastrophic outages or coercion by companies and other actors.

Misuse

Confidentiality of customer data in the cloud can be a double-edged sword for national security. On the one hand, legitimate customer data is protected, but on the other, CSPs also have limited visibility of their product's misuse. In a 2025 paper for NATO's Cycon conference, cyber security expert Volodymyr Styran found that Russian warfighting applications exploit the West's open technology ecosystem.[163] Using data gathered by Ukraine's State Service of Special Communications and Information Protection, Styran highlighted how these Russian applications 'extensively utilize Western cloud services for data storage, media streaming, and access management, alongside … protect[ion] against cyberattacks'.[164] Russian users can do so because Western CSPs have insufficient customer verification processes and Western countries have minimal controls in place: export controls on cloud services are understood and applied inconsistently.[165]

Furthermore, according to Styran, Russian users leverage publicly accessible Western cloud technologies because they offer the best convenience, data availability and maturity of developer ecosystems.[166] For example, Russia lacks high-fidelity geospatial and meteorological data, or the supercomputing necessary for weather forecasting, which are critical functions for targeting fires. Essentially, Russian armed forces use Western cloud services because they are better than the alternatives. This phenomenon was confirmed in several interviews with experts with military operational backgrounds.[167]

162. Vadym Koverznev, Sergiy Ponomarov and Andrii Ivanov, 'Legal Regulation of the Cloud Services Market of Ukraine', *European Journal of Sustainable Development* (Vol. 13, No. 1, 2024), p. 84.
163. Volodymyr Styran, 'Military Mobile Applications Exploit Western Tech in the War Against Ukraine', in C Kwan et al. (eds), *17th International Conference on Cyber Conflict: The Next Step* (NATO Cooperative Cyber Defence Centre of Excellence, 2025), pp. 143–70.
164. Styran, 'Military Mobile Applications Exploit Western Tech in the War Against Ukraine', p. 143.
165. Kolja Brockmann and Lauriane Héau, 'Spyware as a Service: Challenges in Applying Export Controls to Cloud-Based Cyber-Surveillance Software', Stockholm International Peace Research Institute, 17 February 2025, <https://www.sipri.org/commentary/topical-backgrounder/2025/spyware-service-challenges-applying-export-controls-cloud-based-cyber-surveillance-software>, accessed 20 October 2025; author interview with representative of civil society, online, 29 November 2024.
166. Styran, 'Military Mobile Applications Exploit Western Tech in the War Against Ukraine', p. 167.
167. Author interview with representatives of private sector, online, 20 and 29 November 2024.

Recommendations

This chapter sets out recommendations on strategic preparation, procurement and deployment for European governments adopting the cloud in defence and national security. Recognising that adoption is already underway in many countries, these recommendations aim to guide and shape ongoing efforts.

Strategic Preparation

European states enjoyed a post–Cold War peace dividend, but that era of relative security has ended. Reacting to geopolitical pressures, NATO's European members are hardening their security postures by committing to spending 5% of GDP on core defence requirements and related expenditures and creating ReArm Europe.[168] Alongside these strategic measures, NATO's European members must ensure their approach to national security and defence is equipped for modern challenges. Understanding and deploying cloud capabilities for national security and defence is critical to Europe's security.

Countries exposed to existential threats in recent years have demonstrated the value of cloud capabilities. Facing a bellicose neighbour and kinetic threats, Ukraine, Finland and Estonia have proactively adopted cloud capabilities to support national security and defence objectives, including the resilience of critical systems and data, and battlefield and enterprise management. In contrast, countries that are insulated from existential threats have been more hesitant to adopt cloud technologies, citing obstacles outlined in Chapter two: connectivity, interoperability, legality, service continuity, leverage, lock-in and access.

168. NATO, 'Defence Expenditures and NATO's 5% Commitment', 27 June 2025, <https://www.nato.int/cps/en/natohq/topics_49198.htm>, accessed 20 October 2025; See, for example, European External Action Service, 'White Paper for European Defence – Readiness 2030', 21 March 2025, <https://www.eeas.europa.eu/eeas/white-paper-for-european-defence-readiness-2030_en>, accessed 20 October 2025; Sebastian Clapp et al., 'ReArm Europe Plan/Readiness 2023', European Parliamentary Research Service briefing, 3 April 2025, <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)769566>, accessed 20 October 2025.

The following recommendations advocate for a pragmatic approach to cloud adoption, identifying how governments can safely and securely access capability advantages that align with their national interests.

Recommendation 1. Issue and implement a strategic direction for cloud adoption tailored to national security and defence

Governments should state, develop and implement a coherent position on cloud adoption for national security and defence, responding to the strategic and operational benefits of modern compute and systems architecture. This could involve issuing a distinct strategy, a strategic statement as part of a wider document, a policy or a set of guidance – examples include France's strategy for cloud computing and data sharing, and the UK government's Cloud-First policy.[169] Such a step sends a signal internally and externally regarding a government's commitment and ambition for cloud adoption.

Setting a strategic direction does not imply uniform alignment with a single model of cloud adoption. Instead, it emphasises the need to be purposeful in adoption and to create a top-down, principles-based approach: the most appropriate cloud modality – public, private, hybrid or classified – should be selected based on mission needs.

Furthermore, governments should not be myopic with the cloud. It may be that a different strategic direction for national security and defence uses is needed compared with wider society. National security creates more onerous constraints on, for example, data classification, operational security, sovereignty, legal duties and interoperability with allies.

Recommendation 2. Revise legal frameworks to enable cloud adoption for national security and defence use

European countries should identify and address legal or regulatory barriers that limit the adoption of cloud technologies critical to national security and defence.

Ukraine's swift legal reforms following Russia's 2022 invasion enabled rapid migration to private and public cloud infrastructure, a move essential to maintaining digital continuity under kinetic threat. In response to a shifting threat landscape, Finland and Estonia are similarly reassessing their legislative frameworks to enhance their digital resilience.

States facing less immediate threats should not wait for a crisis to expose their regulatory inflexibility. Considering the increased frequency and unpredictability of geopolitical shocks, governments must ensure that their legal environments allow

169. Gouvernement Français, 'French Strategy for Cloud Computing & Data-Sharing', 15 March 2023, <https://gaia-x.eu/wp-content/uploads/2023/03/03.15-10.30-Adrien-Laroche-French-strategy-cloud-and-data-1.pdf>, accessed 20 October 2025; HM Government, 'Government Cloud First Policy', updated 19 June 2023, <https://www.gov.uk/guidance/government-cloud-first-policy>, accessed 20 October 2025.

timely access to cloud capabilities to support secure, scalable and resilient digital operations in both peacetime and conflict.

For governments that remain reluctant to adopt commercially provided delocalised cloud solutions – whether public or private – NATO should explore creating a data-storage function for critical information, such as state registries, that can be leveraged in crises. The mechanism would ensure that data is transmitted, stored and processed exclusively in the territory of NATO Allies. Requisite computing capabilities to provide a minimum viable functionality for this mechanism are neither prohibitively costly nor complex.

Recommendation 3. Plan future compute requirements through scenario-based modelling

The digitalisation of national security and defence – including the adoption of AI and data-driven systems – is driving a significant increase in compute demands. At present, many governments lack a clear understanding of their present and future compute requirements.

Ukraine's experience, particularly with its system, Delta, highlights the scale of compute needed during high-intensity conflict, which exceeds the capacity of national data centres and relies on delocalisation to augment resilience against kinetic threats. Even outside wartime, reliance on highly secure, private or on-premises facilities may constrain access to sufficient compute power.

Governments should initiate structured assessments of current and projected compute needs across a range of scenarios, from peacetime operations to large-scale conflict. This modelling will enable defence and security stakeholders to identify capacity shortfalls, evaluate the resilience of existing infrastructure and plan for scalable provisioning.

Recommendation 4. Assess the implications of cloud adoption for national security and defence with respect to international law

Public clouds are an increasingly fundamental digital backbone to society. They are critical to diverse civilian functions and are becoming more essential to CNI and defence sectors. Are data centres that support the public cloud objects that can be legitimately targeted under international law during wartime?

Governments must clarify their positions on this question and structure their cloud procurement and deployment accordingly. Resources, including the Tallinn Manual 2.0 on International Law Applicable to Cyber Operations and the Handbook on Developing

a National Position on International Law and Cyber Activities, should be considered in developing a national position.[170]

Procurement

Cloud systems represent a departure from self-hosted models, both in their technical capabilities and their business processes. Effective procurement of cloud solutions requires strategic intent informed by practical understanding. Governments who are capable customers of the cloud stand to benefit.

Currently, there are inconsistent approaches to cloud procurement across European countries. Interviewees revealed that there is often insufficient guidance and an over-emphasis on new risks associated with adoption, compared with risks associated with the status quo. Governments must establish and maintain strategic conditions that enable officials to make evidence-based decisions on digitalisation. These decisions should account for the complexity of resourcing computing requirements to deliver the most suitable technologies for specific mission needs. Mainstreaming this approach across government requires centralising key functions, including purchasing, procurement, security assurance and live monitoring.

Recommendation 5. Publish and regularly update guidance for government compute procurement based on a set strategic direction

There is ambiguity about cloud adoption across many European governments. As detailed in Recommendation 1, governments must set out strategic positions on this problem. Their approaches must also provide answers to pressing political questions such as dependence, sovereignty and trusted third parties. Based on these strategic positions, governments must then publish and regularly update guidance for officials on procurement, deployment and other functions.

Without clear guidance informed by firm strategic decision-making on political issues, officials are left unsupported and are expected to make highly complex and politically charged decisions. In this situation, they are incentivised to preference the status quo as they can avoid owning new risk.

170. Michael N Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second Edition, (Cambridge: Cambridge University Press, 2017); Kubo Mačák, Talita Dias and Ágnes Kasper, *Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States* (Exeter and Tallinn: University of Exeter and NATO Cooperative Cyber Defence Centre of Excellence, 2025).

Recommendation 6. Adopt a risk-based approach to cloud procurement anchored in the criticality of data and services

Effective cloud adoption begins with the classification of data and services according to their criticality and sensitivity. This step is essential to design digital systems that are both secure and fit for purpose.

Once data and services are categorised, governments can adopt a risk-based approach to digital systems. Guidance is available on principles for a risk-based approach to cloud adoption – notably from the European Central Bank and the World Bank.[171] This approach typically involves the following measures: establishing a strategic cloud posture; creating an internal marketplace for cloud services; categorising data and workloads; conducting risk assessments to assure cloud services; issuing procurement guidance; recruiting and retaining relevant skilled personnel; and monitoring implementation to iterate subsequent policies.

Governments differ in their perception of risk, but, as Ukraine's experience shows, the need for resilient and accessible capabilities takes precedence under existential threat. Risk must also be assessed in relation to the status quo: existing, alternative digital solutions have their own limitations, and inaction carries strategic and operational costs.

Trade-offs and normative questions raised in this paper should inform governments' understanding of risk. This includes questions of sovereignty and digital resilience as well as ethical uses of technology for defence.

Recommendation 7. Centralise procurement and assurance functions for cloud services

Governments should centralise procurement and assurance functions for cloud services to improve efficiency, security and leverage in commercial negotiations. Core cloud services – particularly IaaS – are relatively standardised and can support a wide range of government users. Acting as a single customer, a government can secure preferential pricing and negotiate stronger contractual terms with CSPs.

Centralising procurement should not eliminate user choice. A centrally assured catalogue of approved cloud services can offer government departments and agencies a menu of vetted options, thus maintaining product competition while ensuring compliance, interoperability and oversight.

171. European Central Bank, 'ECB Guide on Outsourcing Cloud Services to Cloud Service Providers', 2024, <https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon240603_draftguide.en.pdf>, accessed 20 October 2025; Ghislain de Salins, 'Unpacking Cloud Cybersecurity: A Guide for Policy Makers in Developing Countries', World Bank Group, November 2024, <https://documents1.worldbank.org/curated/en/099103124193527496/pdf/P177852-dda0bac6-71ce-408e-9fcb-f0d251cdb786.pdf>, accessed 20 October 2025.

Such a model offers government officials confidence that the cloud services they select meet government standards, which reduces duplicated assurance work, and strengthens overall visibility and control across the digital estate.

Recommendation 8. Create a framework to assess when sovereignty and strategic autonomy are necessary, then implement across existing computing uses

Sovereignty is becoming a focal issue for European states, driven by sputtering economic growth, rising geopolitical tension and expanding military spending. Foundational digital technologies, including (cloud) computing, are part of this trend. Multinational CSPs argue that secure access to the best computational capabilities should be the priority, and that their solutions are not incompatible with sovereignty. Opponents disagree and argue that these companies are a black box.

This paper does not offer a judgement on this debate. Instead, it recommends that governments more proactively engage with relevant questions to understand how they resource specific mission needs.

Governments should create and maintain a framework to assess whether computing functions need to be sovereign or strategically autonomous. First, this requires governments to define what these terms mean for them and outline how they should be implemented. A central entity – such as a prime minister's secretariat – should develop a framework in consultation with relevant ministries. It should then be deployed by those officials that have responsibility for compute functions covering national security and defence.

Recommendation 9. Equip personnel with skills to identify, adopt and procure cloud solutions

Cloud systems are complex and can be unintuitive even for those with expertise in traditional computing. Efforts to train personnel who use cloud technologies – soldiers, technicians and systems engineers – are commendable. Skills development, however, should also be extended to functions that would benefit from stronger understanding of the cloud: procurement, legal affairs, systems integration, contracting and related functions.

Governments should ensure targeted training is available and integrated into existing professional development programmes to build this cross-functional cloud literacy. Enhancing such capabilities will improve decision-making, reduce risks and accelerate effective cloud adoption across national security and defence sectors.

Where possible, training should be cloud-agnostic. Many CSPs, irrespective of size, are committed to upskilling their users and therefore provide free training or qualifications to government officials. These efforts demonstrate a commitment to improving outcomes for users and customers. However, governments should be wary

about over-specialising their officials in closed technology environments. Cloud-agnostic training mitigates this risk.

Deployment

The UK, Finland, Estonia and Ukraine demonstrate how cloud technologies can generate advantage across national security and defence. Cloud adoption enables governments to access advanced capabilities, provision and scale workloads on demand, ensure system continuity and integrity, and resource mission-critical resilience. These factors, among others, are motivating European governments to reassess their approaches to the cloud.

Nevertheless, strategic considerations continue to shape, and in some cases limit, the take-up of cloud technologies, especially where these are public and delocalised. Governments face tactical, practical obstacles, including technical barriers and national and international law, as well as thorny political questions.

Despite compelling evidence from Ukraine's experience of deploying cloud technologies, deteriorating Euro-Atlantic tensions have brought concerns about illicit data-gathering back to the fore. Many European politicians are concerned that concentration and dependence on foreign providers will undermine national resilience by putting confidentiality and availability at risk.[172] Simultaneously, efforts to create European solutions that are insulated from any international dependencies are not moving at the same speed as security and defence needs.

Governments must understand and account for these challenges and trade-offs. Delaying take-up of cloud technologies will place governments further behind the curve. But reckless adoption presents risk. Governments must therefore proactively adopt the cloud computing capabilities that are best suited to their needs in a way that mitigates against the risk of dependence and harmful concentration. They should collaboratively identify and pursue opportunities to build trust with suppliers, following historical precedents in national security and defence sectors.

172. See, for example, Mark Ballard, 'EU Promotes Plan to Usurp US Big Tech with Digital Market', *ComputerWeekly.com*, 22 November 2024, <https://www.computerweekly.com/news/366616313/EU-promotes-plan-to-usurp-US-Big-Tech-with-digital-market>, accessed 10 October 2025; European Parliament, 'Strategic Dependence: Brussels Losing its Soul in American Clouds (Cloud Services of Microsoft, AWS/Amazon, Google)', 8 May 2025, E-001866/2025, <https://www.europarl.europa.eu/doceo/document/E-10-2025-001866_EN.html>, accessed 10 October 2025.

Recommendation 10. Adopt mitigations to reduce the risk of dependence or adverse concentration

The cloud presents unique risks and security concerns. Governments should adapt their security controls to the cloud's risk environment, account for challenges including dependence and concentration, and consider the following measures:

- **Client-side encryption**. Data encrypted by the user before it is transmitted to the cloud. This can include application layer encryption.[173]
    - **CSP encryption**. Data is encrypted by the CSP once it is transmitted to the cloud. Certain national laws regulating data management are ambiguous on the use of encryption keys.
- **Data and systems portability**. The ability to move data and applications between cloud providers, or back on-premises.
- **Interoperability**. Regulatory or contractual requirements that CSPs design in interoperability, for example, by ensuring that management systems, data formatting and protocols are mutually intelligible.
- **Self-hosted or on-premises systems**. Maintaining systems that meet minimum threshold requirements to provide a failover option, or that can run highly sensitive workloads.
- **Hybrid and multicloud**. The use of multiple computing environments – public and private cloud or on-premises – to distribute risk, enhance resilience and align workloads with appropriate security, legal or operational requirements.
- **Classification hygiene**. Consistent and accurate labelling of data, applications and users according to sensitivity, enabling the user to implement proper controls.
- **Software escrow**. A legal agreement to ensure user access to source code or critical software assets if the provider fails to meet contractual obligations. Where software escrow is used, it is paramount that the confidentiality of assets is protected, otherwise new vulnerability is created. If it is not, legal risk is traded for system integrity risk.
- **Cost modelling**. Functions to assess cost differences between cloud services and self-hosted options, accounting for factors including access to operational and capital expenditure.

Several other key measures are often used and yield benefits for national security, but also have their own limitations, which tend to be underestimated:

- **Data localisation**. The requirement for data to be stored and processed within specific geographic or jurisdictional boundaries. This does not account for critical

173. IBM, 'Enhance Your Data Security Posture With a No-Code Approach to Application-Level Encryption', 23 May 2024, <https://www.ibm.com/think/insights/enhance-your-data-security-posture-with-a-no-code-approach-to-application-level-encryption>, accessed 20 October 2025.

functions that sometimes cannot operate in this manner for certain cloud services, for example, software updates.

- **Subsidiaries**. Operating through local companies that are subsidiaries of CSPs or franchised to use CSP technologies. The effectiveness of this measure depends on the control functions that exist between the companies.
- **Contractual protections**. Legal commitments by CSPs to, for example, challenge orders by foreign governments to provide customer data. Some orders prohibit CSPs from sharing data when compelled.

Recommendation 11. Pursue opportunities to build trust and practise transparency

Trust between governments and CSPs is impacted by the actions of a CSP's home government. This challenge is not unique to the cloud, nor is it insurmountable. Trust-building can sustain normal working relations even during periods of political tension.

Trust-building measures can consist in CSPs inviting national technical authorities to participate in exercises testing the security of their digital estates. Governments, in turn, can include CSPs – alongside CNI providers – in national resilience exercises. Transparency is equally important and should build on detailed shared responsibility models to cover operational practices (for example, the location and management of security functions); technology architectures; service development and availability roadmaps; supply chain dependencies; and ongoing threats and breaches – appreciating that not all this information can also be shared publicly.

Trust can also be institutionalised through state-to-state deals and contractual mechanisms, which for security and commercial reasons often remain private or classified. Other sectors such as defence, energy and finance benefit from independent regulatory oversight – which improves trust – because they are designated as critical infrastructure. Governments should assess whether to extend a similar designation to the cloud sector, although what this would mean in practice is not simple. Nonetheless, enhanced transparency and structured trust-building are essential.

Trust can also be reinforced at regional and international levels. Mechanisms such as mutually recognised service assurance processes, notably in groupings such as NATO, not only strengthen cooperation but also reduce duplication of effort across jurisdictions.

Conclusion

Cloud computing is reshaping the strategic and operational foundations of national security. As this paper argues, cloud technologies are enabling governments to meet mission requirements with greater speed, scale and resilience. Whether supporting battlefield awareness, cyber defence or the continuity of government services, cloud capabilities are increasingly central to digital infrastructure that meets modern national security requirements.

Furthermore, this paper has argued that the strategic considerations surrounding cloud adoption, such as market structure and geopolitical tension, need to be weighed against the need for cloud capabilities to answer urgent operational requirements and deliver value. Rather than viewing strategic considerations as impassable barriers, this paper advocates that governments treat them as design constraints to be managed and mitigated through policy, procurement and technical architecture. The priority must remain on ensuring that national security and defence users have access to the capabilities they need, when they need them.

For NATO and European allies, cloud adoption is not only a matter of digital modernisation; it is also a question of strategic readiness. The ability to deploy interoperable, scalable and secure digital capabilities will shape the Alliance's capacity to deter and respond to emerging threats. Ukraine's experience has underscored the operational impact of cloud-enabled systems, while also highlighting the importance of legal clarity, international cooperation and resilience planning.

European governments must therefore act with strategic intent. This means defining and investing in sovereign capabilities where necessary but also recognising the value of global partnerships and commercially driven innovation. This paper recommends expanding trust-building with providers, strengthening governments' capacity to manage the cloud and ensuring that cloud adoption is guided by national interest rather than inertia, fear or lack of information.

Ultimately, the cloud is not a silver bullet, but rather a strategic enabler. Its integration into national security must be deliberate, layered and informed by both mission needs and strategic foresight. As Europe navigates an increasingly contested and digital security environment, the cloud will be central to the ability to project power, protect sovereignty and maintain technological advantage.

About the Author

Joseph Jarnecki is a Research Fellow in RUSI's Cyber and Tech research group. His research focuses on the integration of cloud computing in European security and national approaches to sovereign cloud. He leads projects on UK cyber cooperation and engagement in East Asia and the cyber security of mobile devices and climate transition technologies. Joseph will be publishing a paper on the upcoming refresh of the UK National Cyber Strategy.

His previous work has explored topics such as the UK–Japan cyber partnership, crisis response mechanisms established following Russia's invasion of Ukraine and transnational cybercrime networks. From 2024 to 2025, he was a European Cybersecurity Fellow at Virtual Routes. He holds a MA from the Department of War Studies at King's College London.

194 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 194 years.

RUSI is registered as a charity in England and Wales

Charity number: 210639

VAT number: GB752275038