V.A. Angelier BSCyS <vangelier@hotmail.com> Date: Apr 3, 2025

Digital Sovereignty in the Cloud

The Need for a Dutch Government Cloud in an Era of American Dominance and European Privacy Legislation

Introduction

Digital sovereignty is a critical concern in an era of globalisation and technological dependency. The Dutch government must address a pressing challenge: how to safeguard its digital infrastructure from foreign influence while delivering secure and transparent public services. Dependence on international cloud providers like Amazon Web Services and Microsoft Azure introduces not only technical but also legal and geopolitical risks. The US CLOUD Act, for example, enables American authorities to access data stored abroad, threatening the privacy and autonomy of Dutch citizens.

This essay argues that the Netherlands urgently needs a sovereign national government cloud. Such an initiative would enhance data control, align digital infrastructure with public values, and reduce legal exposure. It responds to growing concerns, as identified by Van der Wal (2024), about vendor lock-in and limited control over sensitive data. Recent geopolitical events including sanctions threats from the Trump administration and Elon Musk’s suggestion to disconnect nations from Starlink have further underscored these vulnerabilities.

In response, the Dutch government is exploring sovereign cloud options. This essay evaluates the rationale and feasibility of such an initiative, using the Ministry of the

Interior and DICTU as its core case. Structured around four themes: legal frameworks, risk analysis, strategic advantages, and implementation it applies models like SWOT, TOE, and NIST. The analysis draws from Dutch policy reports and international initiatives such as Gaia-X and Estonia's X-Road.

Background on Cloud Computing

Cloud computing enables on-demand access to shared computing resources, offering scalability and flexibility for modernising public services. However, reliance on foreign providers introduces vulnerabilities, including limited control over data location and exposure to foreign jurisdictions.

A national government cloud addresses these risks by ensuring critical data remains within Dutch legal frameworks. Built with technologies like containerisation and virtualisation, it would enhance efficiency and security. Open-source adoption reduces dependence on proprietary platforms while promoting transparency and innovation. Investing in sovereign cloud infrastructure strengthens digital resilience and ensures alignment with national public values.

Despite its benefits, public sector cloud use reveals systemic issues:

- **Extraterritorial legislation**: US providers fall under the CLOUD Act, enabling foreign data access even within Dutch borders (EDPLR, 2024).
- **Vendor lock-in**: Over-reliance on dominant providers limits negotiation leverage (Van der Wal, 2024).
- **Lack of transparency**: Commercial providers rarely disclose data handling practices.

- **Misalignment with public values**: Transparency and accountability are hard to guarantee on private platforms.

The proposed solution is a sovereign government cloud, where government data is exclusively stored and managed within Dutch or European jurisdictions. Key requirements include:

- Public ownership (e.g., DICTU or RDDI)
- Legal protection (GDPR compliance, no foreign legal reach)
- Security by design (NIST + Zero Trust)
- Technical sovereignty (open standards, modular architecture)

This approach aligns with European efforts like Gaia-X and Estonia’s X-Road, proving that efficient, trusted public cloud infrastructure is achievable without dependence on Big Tech.

Critical Analysis and Evaluation of the Proposed Solution

The Technology-Organization-Environment (TOE) framework shows that sovereign cloud adoption requires more than technology; it demands organisational readiness and regulatory alignment. DICTU already uses hybrid cloud models to enhance efficiency. For example, DigiD stores authentication data on-premises while scaling through public cloud infrastructure (CEPS, 2025). This hybrid setup automates identity checks, reduces manual handling, and improves coordination.

CEPS notes that such models are transitional and align with Europe’s digital autonomy goals. However, dependence on foreign platforms persists, making a sovereign solution essential to consolidate control and security.

A fully sovereign cloud would retain the benefits of current hybrid setups while eliminating associated vulnerabilities. This shift enables the Netherlands to meet evolving EU standards and regain full oversight over critical digital services like identity management.

Migrating to a sovereign cloud poses technical, financial, and organisational challenges. Legacy systems like DigiD may lack compatibility with modern cloud APIs, requiring middleware and extensive testing to avoid data loss (UK Government Digital Service, 2023). Staff shortages particularly in open-source expertise could delay progress. Resistance to unfamiliar systems like open-source platforms may also hinder adoption.

A phased plan mitigates these risks (example):

- Phase 1 (6 months): Migrate non-critical municipal archives to test compatibility.
- Phase 2 (9 months): Transfer core systems like DigiD, with parallel testing.
- Phase 3 (3 months): Optimise performance and deliver staff training.

Key milestones include pilot completion (month 6), system transition (month 15), and operational readiness (month 18). Structured checkpoints ensure continuity and minimise disruption.

DICTU should address skills gaps by hiring legacy integration specialists and leveraging the National Cyber Security Centre (NCSC) for support (NCSC, 2025). A change management programme using workshops, incentives, and communication could foster staff engagement and reduce resistance.

These measures create a stable transition path. While complex, the shift is feasible with strong planning, capacity-building, and policy alignment ensuring operational continuity and reinforcing sovereignty goals.

Cost-Benefit Analysis of a Sovereign Government Cloud

The Netherlands Court of Audit (2025) highlights inefficiencies and risks in current cloud use. Two-thirds of material public cloud services lack risk assessments, increasing exposure to data breaches and service disruptions. A sovereign cloud could resolve these issues through centralisation and stronger governance.

Although the report lacks a full cost-benefit analysis, it stresses the need for unified oversight. Potential savings could arise from consolidating infrastructure and reducing fragmented procurement.

While precise figures remain uncertain, the financial impact of data breaches, legal costs, fines, and reputational harm is substantial (Fortinet, 2025). Enhanced security and legal certainty offered by a sovereign cloud could mitigate such risks and justify investment.

Social Impact

A sovereign government cloud can enhance inclusivity, transparency, and public trust. It enables equitable access to digital services for vulnerable groups, including the elderly, people with disabilities, and rural populations. Public ownership ensures accessibility remains a design priority.

Greater transparency follows from increased control over data handling. Citizens gain clearer insight into how their data is used, strengthening institutional trust. The cloud also facilitates open data platforms that empower municipalities and citizens to co-create solutions in areas like urban planning and healthcare.

According to CEPS (2025), the Dutch government offers APIs for services such as DigiD, BRP, and DUO. A sovereign cloud supports seamless service integration, ensuring digital transformation aligns with societal values.

Legal and Ethical Dimensions

A sovereign cloud must follow principles such as privacy by design and data minimisation. This aligns with the EU Artificial Intelligence Act, which mandates that AI systems use relevant and limited data (Art. 10), maintain transparency (Art. 13), and ensure human oversight (Art. 14).

Compliance with the EU NIS2 Directive also requires robust technical and organisational safeguards for critical infrastructure. A sovereign cloud, built on European security principles, is better positioned to meet these obligations.

AI-based threat detection raises ethical concerns, especially regarding bias and transparency. Algorithms trained on skewed datasets risk perpetuating inequality (ACM, 2025; Future of Life Institute, 2025). Ethical governance is essential: regular bias audits, explainability standards, and diverse stakeholder oversight are recommended.

DICTU could establish an ethics committee to conduct audits and publish explainability reports. Citizen panels may advise on AI policies to enhance fairness and accountability.

This approach is inspired by Estonia’s X-Road, where citizen input informs e-governance. Similarly, the Netherlands’ ‘Values-Driven Digitalisation’ agenda reinforces this alignment with public trust and democratic control (CEPS, 2025).

SWOT analysis

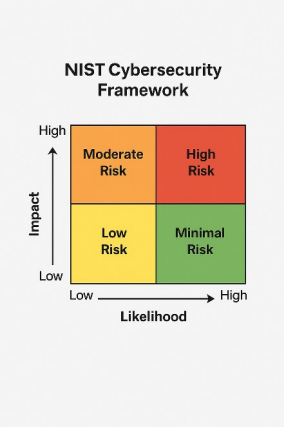
A SWOT analysis clarifies DICTU's strategic position in sovereign cloud adoption:

- **Strengths**: GDPR compliance and public governance support legal and ethical goals.
- **Weaknesses**: High start-up costs and limited internal expertise.
- **Opportunities**: EU collaboration (e.g., Gaia-X) enhances interoperability, while a sovereign cloud improves services like DigiD.
- **Threats**: Lobbying by Big Tech and cyber risks during transition.

CEPS (2025) notes the Netherlands relies partly on proprietary systems, unlike Estonia's open digital model. Expanding open-source adoption would strengthen sovereignty and reduce vendor dependency.

Risk Assessment Using the NIST Cloud Security Framework

A sovereign cloud must address risks such as misconfigurations, unauthorised access, and data breaches. For instance, 67% of Dutch public cloud services lack required risk assessments, increasing vulnerability (Court of Audit, 2025).



The NIST Cybersecurity Framework offers a structured approach, aligning with the AI Act (Art. 9). Key risk levels include:

- **High-priority risks**: Misconfigurations and lack of assessments.
- **Medium-priority risks**: Insider threats and account hijacking, mitigated via IAM policies and staff training.
- **Low-priority risks**: DoS attacks, which disrupt but rarely compromise data.

Mitigation involves proactive monitoring, multi-factor authentication, encryption, and regular audits (NCSC, 2025). NIST's five domains guide cloud governance:

- **Identify**: Classification of data and assets based on sensitivity.
- **Protect**: Implementation of encryption, access control, and segmentation.
- **Detect**: Real-time monitoring using AI-driven anomaly detection.
- **Respond**: Clearly defined incident response protocols.
- **Recover**: Reliable backup and recovery systems in isolated environments.

Using this model, Dutch policymakers can develop and certify resilient sovereign cloud systems while addressing evolving threats effectively.

Critical Reflection

While a sovereign cloud offers autonomy and security, critics cite high costs and complexity, especially given budget constraints. Foreign provider reliance may persist during the transition (IEEE, 2025). Yet, a phased rollout beginning with non-critical systems reduces disruption and cost.

At the EU level, Gaia-X offers strategic alignment. The Netherlands can help shape shared standards, data governance, and interoperability across member states. This builds trust, distributes investment, and reduces dependency on non-European platforms.

Gaia-X's standardised APIs would also ease DICTU's integration with EU systems (Gaia-X, 2024). Shared encryption protocols and threat intelligence networks enhance resilience. Countries like Germany and Switzerland show how joint EU

infrastructure can support digital sovereignty. Though savings remain unclear, shared development reduces long-term costs.

To ensure success, DICTU must invest in open-source technology, internal expertise, and transparent governance. Public-private academies could train staff, while open-source initiatives reduce vendor lock-in (Van der Wal, 2024).

Ultimately, governance not just infrastructure is key. Democratic oversight, transparency, and citizen participation must guide sovereign cloud operations. These principles ensure digital autonomy serves public interest and strengthens trust.

Threats, Security Challenges and Recommendations

Transitioning to a national cloud introduces risks:

- Supply chain attacks: External vendors are frequent targets.
- Human error: Misconfigurations remain a leading breach cause.
- Insufficient segmentation: Poor isolation enables data leaks.
- Political influence: Big Tech lobbying can distort procurement.

To counter these, the following strategies are recommended:

- Zero Trust Architecture: Enforce continuous authentication and micro-segmentation (IEEE, 2025).
- Encryption & key management: Store keys under Dutch control.
- AI-based monitoring: Detect anomalies in real time (ACM, 2025).
- Audits & red teaming: Test defences regularly via external experts.
- Accountable governance: Oversight by a public body with parliamentary scrutiny.

- Shift-left principle: Integrate security early in development.

The Netherlands already has strong cybersecurity infrastructure via NCSC and DICTU. Aligning these with EU frameworks like Gaia-X reinforces sovereignty. Risks include policy inertia, industry pressure, and skills gaps.

To overcome these, the government must invest in knowledge infrastructure, open technologies, and staff development. The solution is not only technical but also institutional, grounded in transparency, public ownership, and long-term vision.

Conclusion

Digital infrastructure in 2025 is no longer a technical issue it underpins sovereignty, public services, and societal resilience. The Netherlands must align innovation with autonomy, security, and democratic control.

This essay has shown that a sovereign government cloud is essential. Continued reliance on foreign providers poses legal, technical, and political risks. Public values such as transparency and equal access are difficult to safeguard under profit-driven platforms.

A sovereign cloud built on European standards and managed by public institutions like DICTU offers a viable alternative. It strengthens resilience and supports EU goals for digital sovereignty.

Ultimately, digital sovereignty enables citizen trust, responsible governance, and democratic continuity in the digital age.

References

ACM. (2025). 'AI-Driven Threat Detection in Multi-Cloud Government Systems'. ACM Transactions on Cloud Security. [Online] Available on: https://www.researchgate.net/publication/383032327_AI-POWERED_THREAT_DETECTION_IN_CLOUD_ENVIRONMENTS [Accessed on: April 2, 2025]

CEPS. (2025, March).GRID DPI-1: Digital public infrastructure in Europe (IDA-2025-03). Centre for European Policy Studies. Available at: https://cdn.ceps.eu/wp-content/uploads/2025/03/IDA-2025-03_GRID_DPI-1.pdf [Accessed on: April 3, 2025]

European Data Protection Law Review. (2024). 'The CLOUD Act Dilemma: Legal Implications for European Government Clouds'. *European Data Protection Law Review*. [Online] Available on: https://www.edpl.eu/issues/2024/4 [Accessed on: April 1, 2025]

European Commissie. (2024). 'EU Digital Sovereignty Report 2024'. Brussel: Europese Commissie. [Online] Available on: https://digital-strategy.ec.europa.eu/en/library/report-state-digital-decade-2024 [Accessed on: April 1, 2025]

European Commission. (2024). Artificial Intelligence Act (Regulation laying down harmonised rules on artificial intelligence). Brussels: European Commission. Available at: https://artificialintelligenceact.eu/ai-act-explorer [Accessed on: April 2, 2025]

EU Cloud Code of Conduct. (2025). 'Compliance Framework for GDPR-Conform Cloud Environments'. [Online] Available on: https://eucoc.cloud [Accessed on: April 1, 2025]

e-Estonia, [n.d.]. Facts and figures. Tallinn: e-Estonia. Available at: https://e-estonia.com/facts-and-figures [Accessed on: April 2, 2025]

Fortinet. (2025). 'Cloud Security Report: Compliance and Operational Risk'. Sunnyvale: Fortinet. [Online] Available on: https://www.fortinet.com/resources/reports/cloud-security-2025 [Accessed on: April 1, 2025].

Future of Life Institute, 2025. The AI Act Explorer. [Online] Available at: https://artificialintelligenceact.eu/ai-act-explorer [Accessed on: April 2, 2025]

Gaia-X. (2024). The Gaia-X Initiative: European Infrastructure for Trusted Cloud Services. [Online] Available at: https://www.gaia-x.eu [Accessed April 1, 2025].

GovTech, [n.d.]. Papers. [n.p.]: GovTech. Available at: https://papers.govtech.com [Accessed on: April 1, 2025].

Government Digital Service, 2023. 'Guidance on the legacy IT risk assessment framework'. London: GOV.UK. Available at: https://www.gov.uk/government/publications/guidance-on-the-legacy-it-risk-assessment-framework/guidance-on-the-legacy-it-risk-assessment-framework [Accessed on: March 27, 2025].

IEEE. (2025). 'Zero Trust in Public Sector Clouds: Mitigating Supply Chain Attacks'. *IEEE Transactions on Cloud Computing*, 15(2), pp. 123-135. [Online] Available at: https://www.computer.org/csdl/journal/cc/2025/01/10758678/221BoZVwUvK [Accessed on: March 24, 2025].

Kalvet, T., (2024) 'E-Government as a Development Strategy: The Case of Estonia'. Tallinn: ResearchGate. Available at: https://www.researchgate.net/publication/378274450_E-Government_as_a_Development_Strategy_The_Case_of_Estonia [Accessed on: April 2, 2025]

National Cyber Security Centre (NCSC). (2025). 'Cloud Security Principles'. [Online] Available on: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles [Accessed on: March 28, 2025]

Netherlands Court of Audit. (2025) 'Dutch central government in the cloud.' The Hague: Netherlands Court of Audit. Available at: https://english.rekenkamer.nl/publications/reports/2025/01/15/dutch-central-government-in-the-cloud [Accessed on: April 1, 2025].

Van der Wal, M. (2024) On the sovereignty of Dutch government data: How the national cloud policy falls short of protecting government data against risks from third countries' jurisdiction and why this matters. Available at: https://scripties.uba.uva.nl/search?id=c11345955 [Accessed on: April 2, 2025]

Thales Group. (2024). 'Trends in Public Sector Cloud Security'. *Thales Cloud Security Study*. [Online] Available on:

https://www.thalesgroup.com/en/markets/digital-identity-and-security/cloud-security/public-sector-trends-2024 [Accessed on: March 28, 2025]