Clouds Over the Netherlands: Preserving Public Interest Internet Governance in the Era of Hyperscaler Clouds

Corinne Cath

critical Infrastructure lab

Clouds Over the Netherlands

Preserving Public Interest Internet Governance in the Era of Hyperscaler Clouds

Published by the critical infrastructure lab, Amsterdam, April 2025.

The report “Clouds Over the Netherlands: Preserving Public Interest Internet Governance in the Era of Hyperscaler Clouds” is marked with CC0 1.0 Universal.

Set in Source Sans, Source Serif, and Source Code.

Made with free software from plain text:
https://github.com/criticalinfralab/criticalinfralab/tree/main/print-automation

critical infrastructure lab document series
CIL#010

DOI 10.5281/zenodo.15230914

Acknowledgments

I would like to thank Fieke Jansen, Niels Ten Oever, maxigas, Andreas Baur, Tijmen de Vries, Bert Hubert, Simon Besteman, Seda Gürses, the PIP peeps, Wouter Tepee, Elisabeth IJmker, Mallory Knodel, Suzanne van Geuns, Erin Simpson, Ot van Daalen, Isa Stasi, Mark Dempsey, Justin Hendrix, Kate Sim, Matt Mahmoudi, Vidushi Marda, Agustin Ferrari-Braun, Marijn Speth, ARTICLE 19, especially Global Team Digital, the Oxford Internet Institute's DIESL group, especially Vili Lehdonvirta, Philipp Riederle, and Anniki Mikelsaar, for their comments and feedback. This report is dedicated to little 'cloud-striker' Aloys, born on 19 July 2024–taking down the global internet in the process. Lastly, it would be remiss not to thank SIDN for inadvertently bringing the topic of cloud-related harms to the top of the Dutch political agenda.

Table of Contents

Executive Summary

Cloud computing is emerging as a critical political issue following the November 2024 elections in the United States, prompting global reassessment of dependencies on American tech giants. Our report considers the Dutch response to increasing cloud reliance through a case study of an Internet governance organization's migration to Amazon Web Services (AWS), the cloud computing subsidiary of tech giant Amazon. Our investigation reveals that public interest organizations moving to hyperscaler clouds undergo fundamental institutional changes that compromise their public service missions. Simultaneously, we find the current debate is problematically framed through nationalistic-militaristic concepts like "digital sovereignty" and "strategic autonomy," often leading to the harmful securitization of cloud alternatives.

In early 2024, the Foundation for Internet Domain Registration in the Netherlands (SIDN) announced plans to migrate part of its critical functioning to AWS. This decision triggered intense debate about the future of "the Dutch internet". This report examines SIDN's decision to move part of .nl to AWS.com and what this choice tells us about broader shifts in managing critical internet infrastructure. It is a compelling example of the potential harms when internet governance organizations—or other institutions with public interest mandates such as governments or universities—rely on 'hyperscale' cloud giants AWS, Google, and Microsoft.

The case study of SIDN illuminates how cloud computing is changing Internet governance by undermining its foundational public interest assumptions. Internet governance requires technical resilience and institutional independence; the turn to the cloud undermines both. This report argues that cloud move means inviting AWS, and its corporate logics, into SIDN. This pattern extends beyond SIDN to numerous public institutions increasingly entangled in commercial cloud ecosystems. To preserve the public interest in this clouded environment, this report recommends:

1. Moving the Public Debate Beyond Digital Sovereignty
2. Prioritizing Public Service over Profit in Internet Governance
3. Creating Meaningful Accountability for the Cloud Decisions of Public Institutions
4. Preserving Core Technical Capabilities and Control
5. Imagining, Funding, and Building a Public Interest Internet Infrastructure
6. Invest in Research and Development of Alternative Cloud Futures

The trend that moves Internet governance organizations toward commercial clouds is likely to continue. We argue that effectively addressing the expanding influence of commercial cloud providers requires rejecting both unregulated American corporate dominance and nationalistic solutions. Instead, we propose an alternative vision for computing infrastructure that prioritizes people over profit—providing a framework for how this approach could transform Internet governance and beyond.

1. Introduction

This is Internet governance: a seemingly routine technological decision has erupted into a profound debate about control, infrastructure, and the future of the internet. The Foundation for Internet Domain Registration in the Netherlands (Stichting Internet Domeinregistratie Nederland, or SIDN)[1], manages the country's .nl domain and serves as its critical internet infrastructure operator. In early 2024, SIDN announced a plan to migrate part of its work to Amazon Web Services (AWS), the cloud computing subsidiary of the American e-commerce giant. Cloud computing allows organizations to meet their need for computing power, software development[2], and data storage over the internet, without maintaining their physical servers and data centers. This is an interesting economic and technical proposition for many businesses and organizations, from governments, healthcare and education institutions, including those involved in maintaining critical parts of the internet.[3]

The move of .nl to AWS will transform the nature of stewardship of the .nl country-code Top Level Domain (cc-TLD), shifting from a locally managed public resource with government oversight to a black-box service (partly) run on a global corporate cloud computing behemoth.

The move of .nl to AWS will transform the nature of stewardship of the .nl country-code Top Level Domain (cc-TLD), shifting from a locally managed public resource with government oversight to a black-box service (partly) run on a global corporate cloud computing behemoth. Amazon Web Services dominates cloud computing, followed by Microsoft Azure and Google Cloud.[4] This means these American tech giants have unprecedented control over the digital infrastructure that powers much of the modern world. The debate around the appropriateness of this power is particularly relevant for operators of country-code domains like .nl, or .de, .uk and others, as this is where the push for commercial expansion through cloud services directly confronts questions of control over key internet resources and the legitimacy of current internet governance frameworks.

SIDN's seemingly straightforward AWS cloud plans quickly became contentious. Dutch headlines captured the mounting tension: "How Dutch is .NL?"[5] and "Minister Puts Brakes on SIDN's Proposed Move to AWS"[6] signaled more than bureaucratic pushback—they represented a public reckoning with the changing landscape of Internet governance in an increasingly cloud dominated world.[7] This was also reflected in the vocal critique from industry, civil society, academics, and political stakeholders following the initial announcement. The Dutch cloud community expressed profound concern.[8] Likewise, academics and tech critics warned of the dangers of surrendering "national" and "vital digital infrastructure" to a single American cloud provider.[9] Local Internet governance organizations voiced their surprise and disappointment.[10] Elected officials took notice and argued that the decision was not in line with existing policy, which requires that SIDN implements changes in consultation with the government.[11]

Beyond Digital Sovereignty: Cloud Migration Stakes

This is not merely a story about one small country's infrastructure for domain registry.

This is not merely a story about one small country's infrastructure for domain registry. This is about the myriad of harms associated with moving societal critical institutions, from registries to governments, to hospitals[12], to universities[13], to independent media outlets[14], to the public hyperscaler cloud environments of Microsoft, Google, and AWS.[15] It is about the question of what happens to the public-interest mandate of Internet governance organizations when they move to the corporate cloud, and the question as to what extent cloud companies' profit motives infuse the very core of how the internet functions. The process of "cloudification" involves the gradual migration or supplantation of digital systems from localized, sometimes publicly managed computing platforms to expansive, predominantly American cloud ecosystems.[16]

This process also involves the infusion of the cloud's corporate logics into its customers.[17] This subtle dynamic manifests as public institutions unconsciously adopting the values, priorities, and cultural frameworks of their cloud providers—emphasizing efficiency, scalability, and cost-optimization over public good, democratic governance, and local priorities. Or to put it more plainly: organizations that migrate to cloud environments often absorb the business philosophies and approaches of the tech giants providing cloud platforms, fundamentally altering their decision-making and priorities in ways that may undermine their original public-interest mission. As such, the move to the hyperscaler cloud inherently raises questions of organizational independence and technical resilience in Internet governance organizations. As well as how this move leads to the further entrenchment of the already sizable power of the major players of the cloud industry.

SIDN: A Microcosm of Broader Transformations

Public institutions' core missions, daily operations, and governance structures become subtly reconfigured by the commercial imperatives and technical architectures embedded in corporate cloud ecosystems.

The case of SIDN involves local Internet governance dilemmas that illuminate the future of the internet more broadly. It helps us understand how Internet governance is likely to evolve as cloudification continues and more of its critical functions—not just cc-TLDs like .nl—become dependent on the 'hyperscaler' clouds of market leaders AWS, Microsoft, and Google.[18] This report also speaks to the broader transformation of public institutions like governments, media outlets, healthcare organizations and universities when they migrate to cloud platforms. It provides an additional lens beyond concerns about data protection, privacy, surveillance, and digital sovereignty to examine institutional changes. This institutional change perspective reveals how public institutions' core missions, daily operations, and governance structures become subtly reconfigured by the commercial imperatives and technical architectures embedded in corporate cloud ecosystems.

A hyperscaler cloud is a large-scale cloud computing provider that operates globally distributed data centers with substantial computing resources to deliver infrastructure, platform, and software services across international markets. As opposed to a local cloud provider, which operates at a smaller regional or national scale with more limited infrastructure and services, often focusing on serving specific geographic markets or communities. These local providers potentially offer greater control to their customers as well as local know-how. Cloudification is happening across the internet industry, from telecommunications to domain registries.[19] Often, this involves a movement from trusted local communities[20] to commercial behemoths.

The scholarship argues that this shift brings the profit motive of the cloud into the functioning of government, or other public interest, organizations.

This shift can come at the expense of Internet governance organizations' public interest mandates. Yet, the potential for long-term adverse consequences for the public, beyond those related to data, privacy, and surveillance, are not sufficiently understood.[21] Research by leading experts in the field shows that organizations—such as SIDN—can change significantly when they move to the cloud.[22] The scholarship argues that this shift brings the profit motive of the cloud into the functioning of government, or other public interest, organizations. The Netherlands is replete with examples of this dynamic. Particularly noteworthy is the impact of the hyperscaler cloud on academia, the media, and governments. A number of leading academics at Utrecht University recently published an open letter calling on their Executive Board to "change course" and free their university "from this heavy reliance on services from these [cloud] companies."[23] The letter argues that the migration to Big Tech clouds compromises their institution's independence and academic freedom. Most significantly, the academics warn that cloud migration has transformed universities, "from being a source of technical innovation and knowledge distribution to consumers of services." Or in other words, they are stressing the institutional change wrought by the dependency on the corporate cloud and the harm it causes to the public mandate and daily-functioning of the university.

At the same time, there is growing resistance to hyperscaler cloud dependency across various sectors of Dutch society and in Europe.

At the same time, there is growing resistance to hyperscaler cloud dependency across various sectors of Dutch society and in Europe[24]. The City of Amsterdam is implementing a comprehensive digital independence strategy that includes seeking alternatives to Microsoft Azure cloud services, making digital autonomy a requirement in all new procurement contracts. They are collaborating with national and European partners to develop open-source alternatives to Big Tech solutions.[25] At the same time, there is growing critique of the EU's cloud choices. The European Parliament deployed Anthropic's Claude AI through Amazon's cloud services for its archives without proper assessment, despite the system providing factual errors. Recent work done by the Irish Council for Civil Liberties shows how public institutions lose control when using cloud-based AI, as the Parliament has no direct contract with Anthropic and cannot ensure the accuracy of information on its official platform.[26] Academics are also broadening the debate beyond Internet governance and government, considering how other societal critical institutions like the independent media sector 'have an [cloud] infrastructure problem'.[27] Industry experts, meanwhile, are experimenting with the development of viable alternatives rooted in public values and local governance by its cloud industry. Several local Dutch cloud providers are collectively[28] and independently[29] experimenting with alternatives to the hyperscalers, "putting their metal where their mouth is" as one entrepreneur said during our interview.

Against this backdrop of growing awareness and resistance, it becomes even more important to closely examine the concrete effects of cloud migration on organizations with public interest mandates. The concerns expressed by critical academics about cloud-induced institutional transformation parallel the challenges faced by critical internet infrastructure organizations, making SIDN a striking case study of what this looks like in practice. The organization engages in commercial activities. There is a crucial distinction, however, between these current activities and the institutional changes to SIDN's functioning that cloud migration represents. Even having a subsection of its infrastructure and services governed by the business model of hyperscalers can lead to fundamental changes across the organization, such as reduced technical resilience and institutional self-determination, skill loss, culture change, and compromised public accountability. These changes are likely to come at the cost of Internet governance public interest mandates.

Political Tensions and Regulatory Responses

The outcome of the Dutch debate in January 2025 has seen the government approve of SIDN's move to AWS, provided it meets various new stipulations.[30] However, recent and sustained pressure by multiple political parties, especially the Greens-Labor-coalition party as well as the New Social Contract Party, shook up the debate once again. In March 2025, a motion put forward by these parties, together with the Liberals, halted the move to AWS. The motion requires a renewed 'consultation (between the Ministry of Economic Affairs) with SIDN and national cloud providers to prevent, even a limited part of, the DNS chain going to Amazon'.[31]

SIDN's choice to move to AWS challenges the assumption that organizations managing critical internet infrastructure "naturally" act in the best interest of the (Dutch) internet ecosystem.

The back-and-forth raises questions about the extent to which we can rely on the current Dutch government to understand the risk comprehensively enough to act decisively when needed. As engaged researchers and advocates, we must do our part to broaden the understanding of harms arising from cloud computing, as many are already doing.[32] This includes critically reviewing the extent to which Internet governance organizations, like SIDN, can continue to prioritize what is good for the (Dutch) internet when embroiled in the cloud. SIDN's choice to move to AWS challenges the assumption that organizations managing critical internet infrastructure "naturally" act in the best interest of the (Dutch) internet ecosystem. In the balancing act between its public service mission and its perceived need to pursue market opportunities, SIDN is choosing commercial expediency at the expense of its original mandate.

It also requires us to change the terms of the political debate about cloud harms. The complexity of cloud infrastructure and its implications for Internet governance demands more than just high-level policy discussions about ‘digital sovereignty’[33]. What’s urgently needed is close collaboration between engaged researchers who can translate technical complexities into accessible frameworks and politicians committed to building systems that prioritize people over profit. Such partnerships support governance models that center the public interest and protect democratic institutions from corporate capture, rather than focusing on territorial notions of digital sovereignty that may miss deeper power dynamics.

Report Outline and Roadmap

This report is a call for a more precise societal debate about the future of Internet governance in an age of cloudification.

This report traces how SIDN’s decision accelerates its transformation from a public and independent interest infrastructure maintainer to a hyperscale cloud-bound, for-profit digital service provider that prioritizes its commercial goals, at a particular inopportune geopolitical moment.[34] A key argument put forth by SIDN was that it was only putting a ‘sub-section of its overall work’[35] into the AWS cloud and that as such, its ability to meet its overall public service mandate would not be affected. This report questions that argument. Furthermore, the report maps the limitations of the Dutch public debate, which has focused on unclear terms like “digital sovereignty.” In the process overlooking and de-emphasizing the permanent changes, to its technical resilience and institutional functioning, brought about by SIDN’s transition to the AWS cloud. Changes that affect its ability to run .nl in the public interest as its mandate requires. In this sense, this report is a call for a more precise societal debate about the future of Internet governance in an age of cloudification.

The report will first outline a brief history of SIDN and its role in managing the .nl domain. Subsequently, it will dissect the details of the proposed AWS migration to locate the Dutch political response to this choice within a larger context of “digital sovereignty” debates and provide a critique of that response. In pursuit of better terms for debate, the report will highlight the commercial ambitions driving SIDN’s choice. Outlining how these ambitions steered its choice for the AWS cloud over its current, largely self-contained and locally sourced computing model, developed since 2011. This choice, in turn, undermines SIDN’s ability to function as a steward of the .nl domain. Their move to the AWS public cloud turns SIDN from, an independent critical infrastructure provider, into a commercial Software-as-a-Service (SaaS) provider, beholden to AWS for part of commercial ambitions. This grip of the cloud on that particular part of SIDN runs the risk of bleeding into its overall functioning, in ways that are already visible now before we know if the move will happen.

The cloudification of the internet should prompt us to ask what becomes of the public interest mandates and legitimacy of Internet governance organizations?

This report uses the case study of SIDN to map the harmful impact of cloudification on Internet governance more broadly.[36] Its analysis draws on 12 formal and informal interviews, participation in various roundtable discussions on the matter with politicians, industry experts, and other affected parties, and desk research. Ultimately, this report treats the SIDN decision as a case study that makes it possible to review whether Internet governance organizations can work for the public interest if they rely on the hyperscaler cloud environments of a handful of dominant American companies. The cloudification of the internet should prompt us to ask what becomes of the public interest mandates and legitimacy of Internet governance organizations? Or what similar harm might befall the growing cadre of other public institutions, like universities, media outlets, and governments, that are rapidly moving to the cloud.

[01] https://www.sidn.nl/en↩

[02] Gürses, Seda, and Joris van Hoboken. 2018. "Privacy after the Agile Turn." In *The Cambridge Handbook of Consumer Privacy*, edited by Evan Selinger, Jules Polonetsky, and Omer Tene, 579–601. Cambridge Law Handbooks. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316831960.032.↩

[03] https://ainowinstitute.org/publication/from-infrastructural-power-to-redistribution-how-the-eus-digital-agenda-cements-securitization-and-computational-infrastructures-and-how-we-build-otherwise; Gürses, Seda, and Joris van Hoboken. 2018. "Privacy after the Agile Turn." In *The Cambridge Handbook of Consumer Privacy*, edited by Evan Selinger, Jules Polonetsky, and Omer Tene, 579–601. Cambridge Law Handbooks. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316831960.032.↩

[04] https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/; Luitse, Dieuwertje. (2024). Platform power in AI: The evolution of cloud infrastructures in the political economy of artificial intelligence. *Internet Policy Review*, *13*(2). https://doi.org/10.14763/2024.2.1768↩

[05] https://www.nrc.nl/nieuws/2024/02/09/hoe-nederlands-is-nl-nog-a4189663↩

[06] https://www.binnenlandsbestuur.nl/digitaal/minister-trapt-op-de-rem-bij-sidn-verhuizing↩

[07] https://www.techzine.eu/news/privacy-compliance/128179/cloud-dominance-microsoft-and-amazon-under-closer-scrutiny/↩

[08] https://nos.nl/artikel/2507035-onrust-over-gedeeltelijke-verhuizing-nl-domeinen-naar-het-amerikaanse-amazon↩

[09] https://techpolicy.press/the-dangers-of-moving-key-internet-governance-functions-to-amazons-cloud-the-case-of-the-netherlands↩

[10] https://isoc.nl/nieuws/isoc-nl-teleurgesteld-door-keuze-nl-registratie-in-amerikaanse-cloud-onder-te-brengen/↩

[11] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2024Z01500\&did=2024D03406↩

[12] Luitse, Dieuwertje. (2024). Platform power in AI: The evolution of cloud infrastructures in the political economy of artificial intelligence. *Internet Policy Review*, *13*(2). https://doi.org/10.14763/2024.2.1768.↩

[13] https://www.uu.nl/en/opinion/open-letter-to-the-executive-university-board-calling-for-a-transformation-to-digital-autonomy↩

[14] https://www.techpolicy.press/independent-media-has-an-infrastructural-problem/↩

[15] A topic that is increasingly central to debates in the Netherlands and across Europe, see for example: https://www.bnr.nl/podcast/de-technoloog/10568644/we-bouwen-ons-eigen-cloudbedrijf-in-tijden-van-trump.↩

[16] Stocker, Volker, Guenter Knieps, and Christoph Dietzel. 2021. "The Rise and Evolution of Clouds and Private Networks – Internet Interconnection, Ecosystem Fragmentation." SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.3910108; Widder,

David Gray and West, Sarah and Whittaker, Meredith, Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI (August 17, 2023). Accepted to appear in Nature, Available at SSRN: https://ssrn.com/abstract=4543807 or https://dx.doi.org/10.2139/ssrn.4543807.↩

17 Gürses, Seda, and Joris van Hoboken. 2018. "Privacy after the Agile Turn." In *The Cambridge Handbook of Consumer Privacy*, edited by Evan Selinger, Jules Polonetsky, and Omer Tene, 579–601. Cambridge Law Handbooks. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316831960.032; Balayn, Agathe, and Seda Gürses. 2024. "Misguided: AI Regulation Needs a Shift in Focus." Internet Policy Review, https://policyreview.info/articles/news/misguided-ai-regulation-needs-shift/1796↩

18 Lehdonvirta, Vili, Bóxī Wú, and Zoe Hawkins. 2024. "Compute North vs. Compute South: The Uneven Possibilities of Compute-Based AI Governance Around the Globe." *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* 7 (1): 828–38. https://doi.org/10.1609/aies.v7i1.31683; Stocker, Volker, Guenter Knieps, and Christoph Dietzel. 2021. "The Rise and Evolution of Clouds and Private Networks – Internet Interconnection, Ecosystem Fragmentation." SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.3910108; Amoore, Louise. 2016. Cloud geographies: Computing, data, sovereignty. *Progress in Human Geography* 42 (1):1–21. https://doi.org/10.1177/0309132516662147.↩

19 See above.↩

20 While the local cloud is not a panacea for the various harms arising from hyperscaler cloud adoption, this report focuses on it first given the rapid capture by hyperscalers of the internet industry. For alternative models of compute, see https://www.adalovelaceinstitute.org/project/global-public-compute/; https://ainowinstitute.org/publication/policy/compute-and-ai/; https://ainowinstitute.org/redirecting-europes-ai-industrial-policy/.↩

21 There is an ongoing debate in the Netherlands about these concerns as they relate to SIDN's choice to move to AWS, as well as the ongoing migration of the Dutch government to the Microsoft cloud. See for example: https://berthub.eu/articles/posts/communicating-without-musk-and-trump-cloud-kootwijk/.↩

22 Balayn, Agathe, and Seda Gürses. 2024. "Misguided: AI Regulation Needs a Shift in Focus." Internet Policy Review, https://policyreview.info/articles/news/misguided-ai-regulation-needs-shift/1796; these leading scholars focus on 'computational infrastructure, which they define as the cloud and end-devices, this report focuses on the cloud part of that infrastructure.↩

23 https://www.uu.nl/en/opinion/open-letter-to-the-executive-university-board-calling-for-a-transformation-to-digital-autonomy↩

24 Bria, Francesca, Johnny Ryan, Sophie Bloemen, Matthias Pfeffer, Leevi Saari, Fabian Ferrari, and van Dijck, Jose. 2024. 'Time To Build A European Digital Ecosystem', 9 December 2024. https://feps-europe.eu/wp-content/uploads/2024/12/Time-to-build-a-European-digital-ecosystem.pdf; Bria, Francsesca. 2025. EUROSTACK: Building a European alternative for technological sovereignty. https://www.euro-stack.info/; Baur, Andreas. (2023). European Dreams of the Cloud: Imagining Innovation and Political Control. *Geopolitics*, *29*(3), 796–820. https://doi.org/10.1080/14650045.2022.2151902.↩

25 See https://ibestuur.nl/artikel/amsterdam-presenteert-verkenning-naar-digitale-onafhankelijkheid/.↩

26 https://www.iccl.ie/press-release/how-not-to-deploy-generative-ai-the-story-of-the-european-parliament/↩

27 https://www.techpolicy.press/independent-media-has-an-infrastructural-problem/↩

28 https://berthub.eu/articles/posts/communicating-without-musk-and-trump-cloud-kootwijk/↩

29

https://fonkmagazine.nl/artikelen/tech/hostingprovider-lanceert-eigen-nederlands-cloud-72306.html↩

30 https://berthub.eu/tkconv/document.html?nummer=2025D01629↩

31 https://www.tweedekamer.nl/debat_en_vergadering/plenaire_vergaderingen/details/activiteit?id=2025A02077↩

32 See for example: https://berthub.eu/articles/posts/taking-the-airbus-to-the-ikea-cloud/; Balayn, Agathe, and Seda Gürses. 2024. "Misguided: AI Regulation Needs a Shift in Focus." Internet Policy Review, https://policyreview.info/articles/news/misguided-ai-regulation-needs-shift/1796; https://www.techpolicy.press/the-dangers-of-moving-key-internet-governance-functions-to-amazons-cloud-the-case-of-the-netherlands/; https://www.uu.nl/en/opinion/open-letter-to-the-executive-university-board-calling-for-a-transformation-to-digital-autonomy; https://www.techpolicy.press/independent-media-has-an-infrastructural-problem/.↩

33 As various academics have repeatedly stated, including in the context of the cloud: Rone, Julia. (2024). 'The sovereign cloud' in Europe: diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. *Journal of European Public Policy*, *31*(8), 2343–2369. https://doi.org/10.1080/13501763.2024.2348618; Baur, Andreas. (2023). European Dreams of the Cloud: Imagining Innovation and Political Control. *Geopolitics*, *29*(3), 796–820. https://doi.org/10.1080/14650045.2022.2151902.↩

34 For more information about how cloud infrastructure is part of a global tussle for power, see: Lehdonvirta, Vili, Bóxī Wú, and Zoe Hawkins. 2024. "Compute North vs. Compute South: The Uneven Possibilities of Compute-Based AI Governance Around the Globe." *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* 7 (1): 828–38. https://doi.org/10.1609/aies.v7i1.31683. And Lehdonvirta, Vili, Bóxī Wú, and Zoe Hawkins. 2024. Weaponized interdependence in a bipolar world: How economic forces and security interests shape the global reach of U.S. and Chinese cloud data centres. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4670764.↩

35 See this SIDN document, p.3 https://www.sidn.nl/downloads/4phkOz5fA2lWdEVb3fWAex/25b4d8d43bd03e4f27d77a8c190bae3e/Achtergronden_bij_onze_keuze_voor_public_cloud_en_AWS.pdf.↩

36 This is happening across different organizations, including SIDN, the Internet Engineering Task Force (IETF), and the *Réseaux IP Européens* Network Coordination Centre (RIPE NCC).↩

2. A Brief History: The Management of .nl

SIDN has long held a crucial role in the intricate ecosystem of digital governance in the Netherlands. A non-profit foundation entrusted with managing the .nl country code top-level domain (cc-TLD), SIDN is the steward of the Netherlands' online identity. Registered in 1986, the .nl country-code top-level domain (cc-TLD) stood as one of the world's first digital national identifiers, predating the commercial internet explosion by nearly a decade. Unlike many national technological initiatives driven by governmental mandates, the .nl internet began as a grassroots collaborative endeavor, led by a small collective of engaged technologists and academics.

Registering .nl and Founding SIDN

The .nl domain was initially managed by the Center for Mathematics and Computer Science (CWI)[37] in Amsterdam. In 1996, SIDN—the Foundation for Internet Domain Registration in the Netherlands—was born. It was established by Piet Beertema, who initially registered .nl, in collaboration with Ted Lindgreen and Boudewijn Nederkoorn. All three were involved in the development of the early Dutch internet industry. It might seem odd for a self-appointed collection of men to take on the stewardship of such vital digital infrastructure. Yet, this origin story is common across early management initiatives for the internet's infrastructure.[38] Groups of well-educated, sufficiently resourced, and university-affiliated men often spearheaded local internet efforts.[39] In the 1980s, when these initiatives were first undertaken, it was not yet evident that this network-of-networks would grow to become indispensable for global commerce, communication, media and politics.

SIDN has matured with the internet. As the non-profit foundation managing the .nl domain registry, SIDN maintains the central database of Dutch domain names. It also oversees the Domain Name System (DNS) security of the .nl domain space. It does so by validating domain names, preventing abuse and defending them against cyber threats. SIDN also administers new domain registrations. These are fundamental tasks that supported over 6 million registered .nl domains as of 2023. This volume positions .nl as Europe's third-largest country-code top-level domain, notably surpassing France's .fr registry[40] despite the Netherlands having a population only one-third the size of France's.

Given this distinct historic trajectory, SIDN has always operated from its public interest mandate to prioritize social benefit over commercial interests. In its words, SIDN tries to ensure its ambitions of building "(...) a single, global internet that is open and accessible to all and reflects the world's diversity of cultures, languages and scripts'.[41]

SIDN positioned itself as part of the movement that is advocating for, and technically implementing, a different, less centralized internet. In their words:

The problem of declining strategic digital autonomy is strongly felt in the Dutch vital infrastructure. If this vital infrastructure fails, it could cause major societal disruption. However, the discussion around digital autonomy often lacks attention to internet infrastructure. And this while the infrastructure forms the foundation for everything online. Therefore, we are looking at new internet properties and techniques that better match the reliability requirements that our current and future digital society demands.[42]

This ethos is also clearly visible throughout its broader work. Beyond its technical responsibilities, SIDN participates in Dutch internet policy development through collaborations with government and industry stakeholders. The foundation implements security measures, including DNSSEC (Domain Name System Security Extensions),[43] and provides incentives for customer adoption of these protocols. Its research division, SIDN Labs[44], studies internet security, stability, and emerging technologies. Its findings inform both technical decisions and policy discussions. Additionally, SIDN operates a grantmaking foundation[45] that distributes grants to Dutch research projects focused on internet infrastructure improvements and public-interest technology development.

SIDN's Oversight and Governance Model

Given this broad array of tasks, how is SIDN regulated? SIDN maintains a functional relationship with Dutch government agencies and stakeholders. The relationship between SIDN and the Dutch government operates within a formal covenant that outlines fundamental functional principles while preserving institutional autonomy.[46] This framework stipulates two primary requirements: 1. SIDN must consult with the broader internet community in its decision-making processes, and 2. it must maintain a substantive connection to the Netherlands. While this arrangement falls short of direct government control, it does build in national oversight over SIDN's latitude and strategic decision-making.

These formal ties notwithstanding, the foundation retains significant discretion in its decision-making. The lack of more substantive oversight means that it remains insulated from the whims of day-to-day politics. This is significant in light of the continued turbulence in Dutch politics.[47] SIDN tries to maintain the 1980s cultural ideals that characterized its origins, at least on paper. The foundation's institutional independence[48] remains a defining characteristic of its structure and governance. This autonomy, formally codified in the foundation's statutes, serves as a mechanism to ensure the neutrality and integrity of the .nl domain space—to the occasional chagrin of its most direct stakeholders, the registries. The registries note that SIDN is often disconnected from their needs. Or as one industry observer I spoke to put it, "The registries really hate SIDN." SIDN, however, prides itself on its independence.

SIDN's Infrastructure Choices and their Impact

SIDN relinquishes the control over its work that justifies its role as .nl's steward.

SIDN's independence is not just institutional, but also technical. Currently, SIDN runs its software in-house and on local data centers in the Netherlands (like BIT).[49] Where it does outsource to these local providers, it often relies on decades-long interpersonal working relationships[50] to ensure that these providers' hosting architecture meets SIDN's specific demands. While the precise information about its hosting architecture and current cloud setup is not available in the public domain, several industry experts confirmed this.[51] Consulting firm Eraneos, contracted by SIDN to advise on its move to the cloud, does report on the organization's current computing set-up.[52] As does SIDN in its explainer on choice for AWS.[53] These documents suggest that SIDN relies on a combination of on-premise compute and "private" cloud with local Dutch providers.

SIDN's current computing setup demonstrates that its claims to institutional independence are backed by genuine technical self-determination and control over its compute environment. SIDN's control over its technical infrastructure legitimates its claim to be an "independent" organization. SIDN's long-time adherence to a grassroots technical stewardship model, where it works with local providers, makes the shift toward corporate cloud dependency all the more striking.

AWS's "public cloud" model involves computing resources that are shared among multiple clients on infrastructure owned and operated by a single cloud provider, whether AWS or Azure, or Google Cloud, and so on. By contrast, the "private cloud" model SIDN previously relied on features infrastructure dedicated solely to one organization, either on-premises or hosted by a third party. In the hyperscaler public cloud, users have less control over their computing environment, because they cannot directly manage the underlying infrastructure, software configurations, or services. These are under the cloud provider's control instead. A private cloud gives users more control over the entire stack, from hardware to software. By opting for a public cloud over its current model, which combines an on-premise approach with a private-cloud setup operated by local trusted providers, SIDN relinquishes the control over its work that justifies its role as .nl's steward.

If SIDN chooses to outsource only a part of its work to AWS, this concern still stands. Even the Eraneos report is clear about the impact that moving to the AWS cloud will have on the organization. The report reads, "SIDN is making a major concession to its objective of contributing to increasing digital autonomy for the Netherlands and EU and reducing internet centralization."[54] Or in other words, no matter how much or how little of SIDN's functioning ends up on the AWS cloud, it still creates a contradiction with its public interest mandate. Crucially, the Dutch value the resilience of their national domain space and the independence of its steward. The distinctive relationship between Dutch society and .nl has created unique expectations around SIDN's institutional role in stewarding (its subsection of) the internet, and the heated political debate about this move only makes sense against this background.

“How Dutch is .nl?”[55]: Digital Sovereignty and its Limits

Traditionally, the internet is romanticized as a borderless realm, a digital commons unfettered by geographical constraints. Yet, within this seemingly unbounded landscape, country code Top-Level Domains (cc-TLDs) emerge as cartographic instruments, drawing digital boundaries that reveal where many consider global networks to intersect with national interests. The current controversy around cloudification and SIDN only makes sense when .nl is apprehended as a digital artifact that is more than mere technical infrastructure. The domain has become a shorthand for the country’s national technological identity.

Unlike generic Top-Level Domains (gTLDs) like .com or .org, cc-TLDs function as interfaces between global infrastructure and national borders. This connection to nationalism makes intuitive sense; .nl is derived from the Netherlands, .fr from France, .uk from the United Kingdom, and so on. For many Dutch stakeholders I interviewed, .nl stands for “the Dutch internet” itself. While technically incorrect, as anyone across the globe can buy a .nl domain, the sense that .nl is Dutch resonates across governmental, business, and civic domains. The Dutch government’s formal classification of SIDN’s Domain Name Service (DNS) provision as a “vital infrastructure”[56] further underscores the domain’s perceived national significance.

This soft national connection between cc-TLDs is also visible in the Internet governance bodies that maintain them. In the Domain Name System (DNS), each country is allocated a specific two-letter code[57], with national organizations often responsible for managing their respective cc-TLDs. In the case of the Netherlands, the Internet Corporation for Assigned Names and Numbers (ICANN) delegates the management of this domain to SIDN—an arrangement the Dutch government signs off on. SIDN’s website re-emphasizes the national significance of .nl. “Whenever you type a .nl address,” SIDN proclaims on its website, “we make sure that you are directed to the correct site. That’s what managing the .nl domain is all about. And it means that we operate at the heart of the Dutch internet community.”[58] Similarly, its 2023 annual report explicitly states that the organization, “also undertake[s] to maintain .nl’s ties with the Netherlands and to keep SIDN based in the country.”[59] Both international governance bodies and those tasked with .nl’s domestic management thus frame the domain through a distinctly national lens.

This cultural connection between .nl and Dutch national identity plays a significant, perhaps even disproportionate role, in the public debate about SIDN’s move to AWS. SIDN carefully cultivated an image of domestic expertise, “we deliver high-quality services linked to innovative, secure domains and digital identities,” its website reads, and “by doing that, we add to the social and economic value of the internet for the Netherlands and the wider world.”[60] This made the foundation’s decision to move to a public cloud model perplexing to its key stakeholders, including the industry and its regulators. The choice seemed to fundamentally contradict SIDN’s claim to be an independent, principled guardian of the Dutch internet.[61]

Without taking statements about .nl as “national infrastructure” at face value, it is important to note that Dutch political actors and industry do view the domain through this prism. Cloudification seemed to imperil the Netherlands’ “digital sovereignty”: its ability to govern its domains as desired, in the cloud as on the ground. The Dutch government eventually, and reluctantly, greenlighted the time-limited move to AWS in early 2025. Only to have that decision halted by parliament towards the spring. In no small part due to developments in the US, that see its government becoming a less reliable geopolitical actor. This demonstrates the limits of a debate that considers cloudification through the lens of “digital sovereignty”, being dictated by fast-changing political relations, as opposed to or in addition to, the broader harms and drivers of cloudification.

The debate’s narrow focus on digital sovereignty prevented a more substantive discussion of cloudification’s harms.

The commercial drivers and dangers that motivated SIDN to move to AWS were not debated. The focus on digital sovereignty hampered critical discussion of how SIDN’s role as an autonomous steward of the public interest would be impacted by these profit-seeking motives in an increasingly cloud-native economy. The debate’s narrow focus on digital sovereignty[62] prevented a more substantive discussion of cloudification’s harms to SIDN’s institutional functioning, and subsequently to the internet’s resilience. To understand the full implications of this case, we first need to examine in detail how the public discussion around SIDN’s move to AWS unfolded.

[37] https://www.cwi.nl/en/about/↩

[38] Abbate, Janet. 2000. *Inventing the Internet*. Cambridge, MA: The MIT Press.↩

[39] Nooney, Laine. 2023. *The Apple II Age: How the Computer Became Personal*. Chicago, IL: University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/A/bo195231688.html.; Cath, Corinne. 2023. Loud men, talking loudly.Rreport https://criticalinfralab.net/wp-content/uploads/2023/06/LoudMen-CorinneCath-CriticalInfraLab.pdf.↩

[40] One reason for this reality is that it was comparatively easy to register a .nl domain, where especially in the early days it was very difficult to register a .fr domain.↩

[41] https://web.archive.org/web/20240926170727/https://www.sidn.nl/en/about-sidn/what-we-stand-for↩

[42] SIDN Annual Report 2021, page 6, https://jaarverslag.sidn.nl/jaarverslag2021/pdf/SIDN_Jaarverslag_2021.pdf translated by the author.↩

[43] https://www.sidn.nl/en/modern-internet-standards/dnssec↩

[44] https://www.sidnlabs.nl/en↩

[45] https://www.sidnfonds.nl/↩

[46] https://www.sidn.nl/downloads/56DacSOZcIMeLOnTyZ5s0l/2de9fb026cdf46fec781d9819f17052d/Convenant_waarborging_nl_domein_2022_2029.pdf↩

[47] https://www.nytimes.com/2023/11/23/world/europe/dutch-election-results-far-right-geert-wilders.html↩

[48]

Which to be clear does not mean to imply that SIDN can operate without the support of other actors in the ecosystem, the Internet as a network-of-networks can not function without relying on others. Rather, independence here–based on SIDN's own documents and public statements–refers to its ability to control its functioning and maintain a level of autonomy and self-determination in how it operates.↩

49 BIT, for example, specially positions itself as a Netherlands-based and privacy friendly alternative to hyperscale cloud companies AWS, Microsoft and Google: https://www.bit.nl/.↩

50 This cultural practice of the internet and Internet governance organizations running on trust between individuals is key and fairly common across the industry, for more see Mathew, Ashwin J. 2016. "The Myth of the Decentralised Internet." *Internet Policy Review* 5 (3): 1–16. https://doi.org/10.14763/2016.3.425.↩

51 From SIDN's most recent financial reports, its not possible to dissect how much of its computing needs are done in house or outsourced to others, as the breakdowns do not enter that level of detail. https://jaarverslag.sidn.nl/jaarverslag2023/documents/SIDN_Financieel_verslag_2023.pdf.↩

52 See: https://www.sidn.nl/downloads/1Uv1nlp2S8Le6jNkyfoDh1/30329fb5f13cd5806eaf5a8d5bb3dcb7/Eraneos_Sourcingstrategie_SIDN_toelichting.pdf see page 11, 17-21.↩

53 Interestingly, in their explainer SIDN state that the move to AWS is beneficial because it would allow them to move away from 'a self-managed cloud model', see page 2 https://www.sidn.nl/downloads/4phkOz5fA2lWdEVb3fWAex/25b4d8d43bd03e4f27d77a8c190bae3e/Achtergronden_bij_onze_keuze_voor_public_cloud_en_AWS.pdf.↩

54 https://www.sidn.nl/downloads/1Uv1nlp2S8Le6jNkyfoDh1/30329fb5f13cd5806eaf5a8d5bb3dcb7/Eraneos_Sourcingstrategie_SIDN_toelichting.pdf, page 7, translated by the author.↩

55 This title was taking from a piece written by a Dutch journalist, https://www.nrc.nl/nieuws/2024/02/09/hoe-nederlands-is-nl-nog-a4189663.↩

56 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2022Z13965&did=2022D28820↩

57 https://upload.wikimedia.org/wikipedia/commons/d/d1/World_TLD_Map.jpg↩

58 https://web.archive.org/web/20240926170727/https://www.sidn.nl/en/about-sidn/what-we-stand-for↩

59 https://jaarverslag.sidn.nl/jaarverslag2023/documents/SIDN_Annual_Report_2023.pdf, page 22.↩

60 https://web.archive.org/web/20240926170727/https://www.sidn.nl/en/about-sidn/what-we-stand-for↩

61 While SIDN has long relied on others for its computing power, such as its long-term data center provider partner BIT, this shift is still remarkable. BIT and other collaborators are run locally and their strategic directions are not determined by global shareholders.↩

62 For future debate about the limits of digital sovereignty or the role of the state in the governance of TLDs see: Mueller, Milton. 2002. Ruling the Root: Internet Governance and the Taming of Cyberspace. Cambridge, USA: MIT Press. And Mueller, Milton. 2010. Networks and States. Cambridge, USA: MIT Press.↩

3. A Storm of Critique: .nl Moving to AWS

On January 29, 2024, SIDN's new Chief Technology Officer (CTO) published a short blog.[63] In it, he announced that the organization would outsource part of its registry work[64] to the US cloud behemoth Amazon Web Services (AWS). The foundation's excitement provoked an unexpectedly forceful response across Dutch technical and policy circles. The intensity of the backlash appeared to surprise SIDN, suggesting that the organization underestimated the extent to which its cloud migration would be taken up as a threat to Dutch 'digital sovereignty'. The government, industry, and others raised a spectrum of concerns about the AWS move. These concerns were, however, narrowly organized around the flexible and limiting concept of 'digital sovereignty'.

An Overview of the Public Response and What it Missed

SIDN cultivated trust within the Dutch internet community not only through its commitment to in-house operations and demonstrated independent technical expertise but also through its stated adherence to public interest principles. Trust in SIDN's understanding of the local digital landscape has been waning, however.[65] The sense of .nl as an essential national infrastructure, despite the technical reality that these domains are globally accessible, has remained stable.

The Dutch political establishment had come to view .nl as an extension of national sovereignty, despite the cc-TLDs inherently global nature.

Digital and Data Sovereignty

When it seemed that the "Dutchness" of .nl would be entrusted to a commercial, American, corporation, the debate about the move centered on digital sovereignty. Members of the Dutch parliament across the political spectrum—from Labor and Green parties to Christian and Liberal Democratic parties—raised formal questions about the move.[66] The Ministry of Economic Affairs, which oversees digital infrastructure matters through its covenant with SIDN, announced an investigation into potential risks to the Netherlands's "digital open strategic autonomy." This swift mobilization exemplified how deeply the Dutch political establishment had come to view .nl as an extension of national sovereignty, despite the cc-TLDs inherently global nature.

The decision became a flashpoint in broader debates about European digital sovereignty[67] and growing concerns regarding the future political direction of the United States. Dutch parliamentarians portrayed SIDN's move as symptomatic of Europe's increasing dependence on American tech giants, arguing it undermined regional efforts to build 'sovereign' digital infrastructure. Digital sovereignty advocates insisted that critical systems like domain registries should remain under direct—ideally Dutch, but otherwise European—control. Local cloud providers enthusiastically endorsed this position, bristling at SIDN's public assertion that "no European providers could do the job".[68] As an industry executive I interviewed noted with evident frustration, "That's a rather sweeping conclusion to reach without actually consulting any of us about our capabilities."

Data sovereignty emerged as another central point of contention. While SIDN promised that all data would reside on AWS's European servers, critics noted that the servers' geographic location would offer insufficient protection against U.S. surveillance powers. In particular, the Clarifying Lawful Overseas Use of Data Act, or CLOUD Act, raised concerns.[69] This is a 2018 U.S. federal law that empowers American law enforcement to access data held by U.S. technology companies on any servers worldwide while creating mechanisms for foreign governments to request data through bilateral agreements. The CLOUD Act, Dutch critics argued, could compel AWS to surrender data to U.S. authorities regardless of its physical storage location. While domain registration data is largely publicly available, the prospect of foreign government access sparked particular concern. SIDN's apparent oversight of these surveillance risks in its technical assessment struck many observers as remarkable, given how prominently such concerns have featured in European and Dutch digital policy discussions since Edward Snowden's revelations in 2014.

The debate furthermore focused on control of vital "national" infrastructure and data. Critics raised scenarios ranging from routine service disruptions to geopolitical conflicts that could compromise AWS's relationship with European clients. Recent years have seen multiple such disruptions[70], and several Dutch technology experts suggested that the current US administration might leverage cloud dependencies for political advantage.[71] Security specialists, while acknowledging AWS's robust security credentials, warned about the systemic risks of concentration: any significant AWS outage or cyber-attack could cascade beyond SIDN's services to affect multiple critical systems that rely on SIDN's offerings.

In early 2024, SIDN's defenders still dismissed such concerns about cloud dependency as largely theoretical, citing AWS's technical expertise. However, the July 2024 CrowdStrike outage, which disabled millions of Microsoft cloud-based systems across the globe, lent new credence to these warnings.[72] SIDN's initial response to reliability concerns emphasized AWS's scale and market dominance rather than specific technical safeguards. When pressed on this point, however, the foundation eventually acknowledged this oversight. This "oversight" was outlined clearly in SIDN's 2021 and 2022 annual reports[73], however.

SIDN's omissions did not, initially, sway the debate. As mentioned, in early 2025, the Dutch government gave SIDN a reluctant go-ahead.[74] They noted that there were "significant national security risks" in doing so, however, but proposed that these could be addressed. In an addendum to the current covenant with SIDN, they mandated stricter oversight going forward. "Important," one expert I asked about the impact of this change sighed, "but mustard after the meal"—a Dutch expression for an intervention so late as to be wholly ineffective. The government's decision was both surprising and disappointing. At the time of writing this report, parliament has unanimously forced the government to revisit this decision. Whatever the outcome, narrowly focusing on safeguarding digital sovereignty[75] means any proposed solutions will overlook—just as the public debate did—the insurmountable incompatibility between SIDN's public service mandate and its commercial cloud ambitions. This narrow focus fails to address how the hyperscaler cloud fundamentally changes SIDN's functions and undermines its ability to fulfill its public interest obligations. To truly understand this incompatibility, we must examine how SIDN's pivot toward commercial, and AWS cloud-bound, Software-as-a-Service ambitions fundamentally reshapes its stewardship role.

The hyperscaler cloud fundamentally changes SIDN's functions and undermines its ability to fulfill its public interest obligations.

Stewards to SaaS: Global Domain Business

In the original blog by the foundation's CTO, there is a brief mention of SIDN's intention to turn domain name registration into Software-as-a-Service (SaaS). SIDN's initial announcement also mentioned a partnership with the Canadian Internet Registry Association (CIRA)[76], .nl's Canadian counterpart responsible for running .ca. In the blog SIDN states, "To make Fury even more accessible, we are going to migrate that platform to the public cloud together with the Canadians over the next 2 years. That will be a joint development effort. An additional advantage is that afterwards we can offer Fury as a kind of 'DRS-as-a-service' to other registries." CIRA had previously entered the registry software market with its Fury platform and SIDN aimed to partner with CIRA, to provide its domain registration as a service.

This meant that SIDN would also be beholden to whatever cloud computing decision, and perhaps more importantly, contracts CIRA already had in place. Various interlocutors explained that CIRA already had a contract with AWS when they entered into a partnership with SIDN. Whether this is correct or not, whatever concerns SIDN previously expressed about relying on a single provider, like AWS[77], seem to have dissipated to keep the CIRA partnership moving forward.

SIDN explained this choice in terms of its future financial resilience: entering the SaaS market provides a new source of income beyond the fees it collects for .nl domain registrations, its identity solutions, and other existing income sources. It felt this expansion was a diligent choice, given recent dynamics in its industry. While the foundation's primary revenue comes from domain registration and renewal fees—a model that has been sufficiently lucrative to support robust infrastructure investment and technical innovation—SIDN argues that it operates in an increasingly competitive landscape. The domain name industry is experiencing a notable shift in growth patterns, with traditional country-code Top Level Domains (cc-TLDs) like .nl seeing stagnation, while newer TLDs (like .music or .bot) show growth. In response to this market dynamic, several larger cc-TLD operators have begun offering registrar and back-office services to smaller cc-TLD operators, diversifying their business models beyond their traditional role of managing their national domains.

SIDN is no exception. In addition to generating new income through a SaaS model, SIDN is also seeking to cut costs through the cloud-move. The technological overhaul of .nl's domain registration infrastructure, as outlined in SIDN's CTO's blog post, marks a significant shift in the foundation's strategy. After years of maintaining DRS5, its proprietary domain registration software, SIDN determined that its system needed a refresh. SIDN's rationale for the move to the public cloud over its reliance on in-house hardware and local data centers emphasized "modernization", "efficiency", and the necessity of keeping up with the trend across various commercial industries.[78] Furthermore, the organization claimed that it had been spending "more and more time, attention, and resources" on its domain registration system and the underlying infrastructure, which was built on "outdated technology." By leveraging hyperscaler public cloud infrastructure, SIDN argued that it could focus more on its core services while reducing the costs of running its hardware and software.

AWS is an obvious choice, but only with the CIRA partnership and the SaaS ambitions in mind. These commercial ambitions underlying SIDN's decision to move to AWS deserve closer scrutiny than they received in the public debate[79], especially against the background of an increasingly cloud-native software industry.[80] If SIDN had only been interested in moving some of its DRS5 functions to the cloud to reduce costs, the organization could have opted for a small European provider, or set of providers. As one local data center provider I interviewed said, "SIDN's regular computing needs can be run on my Macbook." However, if its intention was always to become a global commercial SaaS company through its partnership with CIRA—AWS is indeed one of the few providers capable of meeting that particular demand.[81] AWS's global infrastructure provides scalability that would be beneficial for offering commercial services, so that CIRA and SIDN can reach an international client base of worldwide registries.

The global reach baked into SIDN's SaaS ambitions, and the centrality of the public hyperscaler cloud to the SaaS industry, are key to understanding the registry's choice for AWS—even if it was not explicitly stated in the initial announcements and subsequent communications. This distinct double business angle, of SIDN turning to global domain name SaaS while the software industry is becoming increasingly cloud-native[82], was missing from the public debate in The Netherlands. But it is crucial to understand what is at stake. SIDN primarily claimed that the move to AWS was a technical necessity, but this analysis demonstrates it most likely came about in response to the commercial opportunity sparked by its partnership with CIRA.

These recent developments further stress that there is nothing inevitable about the choice for the hyperscaler clouds of AWS, Google, and Microsoft. Cloudification is neither a strict technical nor an economic necessity for SIDN. Rather than confining itself to .nl management, as some of its European counterparts (such as DENIC, which manages .de in Germany)[83] do, the organization aimed to monetize its expertise by developing its domain registration software into a globally available software service. The pivot to AWS, while potentially commercially advantageous in the short run, raises fundamental questions about SIDN's priorities. It raises significant barriers to SIDN's ability to achieve the technical control and institutional independence it needs to meet its public interest mandate, as it becomes dependent on the AWS cloud.

In addition to generating new income through a SaaS model, SIDN is also seeking to cut costs through the cloud-move.

These specific concerns have been notably absent from Dutch public discourse. This is a critical oversight. Commercial ambitions that rest on the hyperscaler cloud stand to erode the trust in SIDN's resiliency that has historically legitimized the organization's stewardship of the "Dutch" domain space. What changes about the public debate on cloud harms when we attend to this dimension of the decision? How do the commercial opportunities opened up by AWS impinge on SIDN's public interest mandate? How does the cloud reshape public institutions and which visions for the future are needed now?

[63] https://web.archive.org/web/20250120144021/https://www.sidn.nl/nieuws-en-blogs/we-blijven-pionieren-door-de-inzet-van-de-beste-en-modernste-standaardtechnieken↩

[64] SIDN from the start has been clear to state that they would not move the DNS: 'DNS is not part of the migration to AWS. For the availability of the .nl domain for end users, for example website visits and email traffic, we are therefore not dependent on AWS. We will not use AWS DNS services in the future and will continue to work with multiple different DNS operators. This keeps .nl and the DNS diverse and decentralized, which are important technical principles for internet availability and scalability.' p. 3 https://www.sidn.nl/downloads/4phkOz5fA2lWdEVb3fWAex/25b4d8d43bd03e4f27d77a8c190bae3e/Achtergronden_bij_onze_keuze_voor_public_cloud_en_AWS.pdf.↩

[65] Take, for example, this 2020 piece in the Dutch Financial Times by the Association of Registrars who called for further government oversight of SIDN: https://fd.nl/ondernemen/1361344/bedrijven-willen-dat-minister-beheerder-nl-domein-onder-toezicht-stelt.↩

[66] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2024Z01500&did=2024D03406↩

[67] Bria, Francsesca. 2025. EUROSTACK: Building a European alternative for technological sovereignty. https://www.euro-stack.info/.↩

[68] Interestingly, even the consulting group that advised SIDN on its cloud move suggests while SIDN's commercial ambitions might make AWS an attractive choice, there are other available options that would be less detrimental to its stated commitment to independence https://www.sidn.nl/downloads/1Uv1nlp2S8Le6jNkyfoDh1/30329fb5f13cd5806eaf5a8d5bb3dcb7/Eraneos_Sourcingstrategie_SIDN_toelichting.pdf.↩

[69] https://www.congress.gov/bill/115th-congress/house-bill/4943↩

[70] https://www.theregister.com/2024/07/19/microsoft_365_azure_outage_central_us/↩

[71] <https://www.dutchnews.nl/2024/01/criticism-as-dutch-domain-registry-plans-move-to-amazon-cloud/↩

[72] https://www.nytimes.com/2024/07/19/business/microsoft-outage-cause-azure-crowdstrike.html↩

[73] SIDN had explicitly warned against the dangers to the stability of .nl were it to move to a single global provider in its 2021 and 2022 annual reports. For example, its 2022 states: "The centralization of the internet, both infrastructure and services, brings

significant challenges. Digital systems like DNS services and cloud storage are increasingly being developed and managed by a small number of large companies from the United States and China. A handful of online platforms like Facebook and YouTube hold dominant positions in our society. These parties' control over our knowledge, data, and technologies is taking irresponsible forms. This puts pressure on Dutch and European internet users' autonomy and Dutch and European values and norms." p. 23 Likewise the 2021 annual report, pages 5-6 read: "Only 3 parties host 48% of all active .nl domain names. Additionally, major outages at providers like Akamai and OVHcloud did not lead to better name server distribution. For nearly half of .nl domain names, the nameservers are in 1 network. An outage at a single party managing a large portion of nameservers could cause many .nl domain names to stop working. This poses a risk to the stability and security of .nl."↩

[74] https://berthub.eu/tkconv/document.html?nummer=2025D01629↩

[75] A number of researchers and critics are investigation the limits of the digital sovereignty debates, see for example: https://www.digitalfutureslab.in/publications/provocations-on-ai-sovereignty-confronting-complexities-and-shaping-future-strategies; https://www.diplomacy.edu/blog/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/.↩

[76] https://www.cira.ca/en/↩

[77] SIDN had explicitly warned against the dangers to the stability of .nl were it to move to a single global provider in its 2021 and 2022 annual reports: "The centralization of the internet, both infrastructure and services, brings significant challenges. Digital systems like DNS services and cloud storage are increasingly being developed and managed by a small number of large companies from the United States and China. A handful of online platforms like Facebook and YouTube hold dominant positions in our society. These parties' control over our knowledge, data, and technologies is taking irresponsible forms. This puts pressure on Dutch and European internet users' autonomy and Dutch and European values and norms." SIDN Annual report 2021, pages 5-6. https://jaarverslag.sidn.nl/jaarverslag2021/pdf/SIDN_Jaarverslag_2021.pdf, translated by the author. "Only 3 parties host 48% of all active .nl domain names. Additionally, major outages at providers like Akamai and OVHcloud did not lead to better name server distribution. For nearly half of .nl domain names, the nameservers are in 1 network. An outage at a single party managing a large portion of nameservers could cause many .nl domain names to stop working. This poses a risk to the stability and security of .nl." SIDN Annual report 2022, page 23, https://jaarverslag.sidn.nl/jaarverslag2022/pdf/SIDN_Jaarverslag_2022.pdf, translated by the author.↩

[78] https://web.archive.org/web/20240828053345/https://www.sidn.nl/nieuws-en-blogs/we-blijven-pionieren-door-de-inzet-van-de-beste-en-modernste-standaardtechnieken↩

[79] With some exceptions, including Bert Hubert and the author of this report: https://www.techpolicy.press/the-dangers-of-moving-key-internet-governance-functions-to-amazons-cloud-the-case-of-the-netherlands/↩

[80] Gürses, Seda, and Joris van Hoboken. 2018. "Privacy after the Agile Turn." In *The Cambridge Handbook of Consumer Privacy*, edited by Evan Selinger, Jules Polonetsky, and Omer Tene, 579–601. Cambridge Law Handbooks. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316831960.032.↩

[81] https://www.techpolicy.press/the-dangers-of-moving-key-internet-governance-functions-to-amazons-cloud-the-case-of-the-netherlands/↩

[82] Balayn, Agathe, and Seda Gürses. 2024. "Misguided: AI Regulation Needs a Shift in Focus." Internet Policy Review, https://policyreview.info/articles/news/misguided-ai-regulation-needs-shift/1796.↩

[83] DENIC (German Network Information Center), for example, operates as a cooperative with over 300 member organizations. It manages the .de country code top-level domain (cc-TLD) through a self-regulatory model. Members must be organizations providing domain registration services, and they collectively make strategic decisions through

general assemblies. DENIC is funded through registration and membership fees. See https://www.denic.de/en/about-denic.↩

4. Getting to the Core: Harms and Futures

AWS's cloud infrastructure could gradually reshape SIDN's core mission, its future functioning, and public service mandate.

The linkage between commercial ambition and the potential harm of the subsequent cloudification is rarely part of the debate. Critics largely focus on the most obvious risks of the transition to AWS: it is a decision that would be hard to reverse were it to backfire, since doing so would involve considerable costs.[84] In response to the initial public outcry over the move, SIDN committed to developing an exit strategy. This would mean, at least in theory, that the organization could source some of its cloud computing locally. However, these backups are meant to function only as backups, with the primary processes happening on the AWS cloud.[85] More importantly, this solution distracts from the more fundamental harm associated with its commercial ambitions. AWS's cloud infrastructure could gradually reshape SIDN's core mission, its future functioning, and public service mandate. How would this happen? Which of these harms are already visible now, when SIDN has not completed its move to AWS yet?

New Dependencies: From Cloud Farmers to Cloud Wholesalers

Historically, SIDN has met its public interest mandate by shoring up its technical resilience and institutional independence. Both come under threat as a result of the commercial ambitions realized through, and by, AWS. SIDN achieves technical oversight by relying on local cloud providers—known informally as "hosting boer," or "cloud farmer" in Dutch—with whom the organization has a history of collaborating. The farmers are in charge of the land they make available to others. In this private cloud model, the computational environment is tailored to SIDN's needs, since the cloud is set up for exclusive use by a single organization. This organization then has extensive control over its functioning and customization. This control over the whole stack, from hardware to software, has allowed SIDN to claim the technical oversight necessary to legitimate its role as a public service provider.

This is not possible with AWS. Public cloud services inherently cater to multiple customers. Relying on a cloud infrastructure owned by third-party providers such as AWS, Microsoft Azure, or Google Cloud means that organizations have limited ability to directly manage the underlying infrastructure, hardware configurations, or the digital services provided by third-parties on that platform. In the words of leading academics in the field, "When they [cloud customers] adopt digital services, [these] deployers, however much they may want to serve the public interest, become heavily dependent on both the quality of the service and the business interests of the many providers bundled into the services they adopt."[86] The concern about SIDN moving to the cloud is thus not only about the cloud infrastructure but also about the many third-party providers that provide the services that come with it. What could this look like in the case of SIDN?

Currently, the migration of SIDN to AWS is halted. However, we can speculate on the impact of its growing dependency on the cloud. If SIDN were to migrate, for example, its verification services for registration data[87] to AWS it becomes entangled in a complex web of dependencies. If registration data fraud detection systems suddenly begins flagging legitimate Dutch government registrations as suspicious, SIDN cannot easily determine whether the issue stems from an AWS infrastructure update, changes to the fraud detection service they are using, or modifications to the underlying data processing system. Despite SIDN's critical role in maintaining .nl, they might lack the capacity to contest AWS's business decisions about such changes that might impact the reliability of the Dutch domain space. Such dependencies compromise SIDN's ability to fulfill its public interest mandate, as the organization charged with maintaining a cornerstone of Dutch digital infrastructure becomes subject to corporate priorities and technical choices made in Seattle.

This is a crucial difference: by opting for the public corporate AWS cloud over its current on-premise and private cloud setup with local trusted providers, SIDN relinquishes control over its work—and subsequently over its guarantee of being able to build an internet 'open and accessible to all'—that has long justified its role as .nl steward.

Another place to see permanent institutional changes, which lead to the loss of control and independence, is in the hiring choices made by the organization. Its 2023 annual report indicates that SIDN successfully hired 9 new employees, a significant subset of whom were hired specifically to manage the move to the AWS cloud, according to my interviewees. The new cohort demonstrates how cloudification affects the organization's overall functioning. The IT department is becoming increasingly oriented around AWS's specific computing environment, which will be felt across all of SIDN's work. Previously, staff were trained to operate .nl across multiple computing environments. Several industry observers mentioned in interviews that long-term IT experts within the organizations have tried to resist this change or left in response. The broad public interest task of managing .nl narrows into the broadly applicable work of managing AWS servers—this is a loss of expertise and a change to .nl technical resilience, which puts pressure on SIDN's public interest mandate and overall functioning.

SIDN's institutional resilience also stands to suffer from a move to AWS. The shift to a public cloud model necessitates an institutional relationship with AWS as a corporation. Recent research[88] suggests that it is likely that the move to AWS will lead SIDN to optimize its functioning in accordance with the business interests of its new cloud owner—this is a form of dependence that extends much beyond the digital sovereignty concerns related to data or privacy. This is aggravated by the fact that in AWS's vast commercial ecosystem, SIDN becomes just another customer, subject to standardized service levels. This means SIDN might be relegated to the back of the queue during critical outages[89], potentially leaving key Dutch government, hospital, university, and media websites inaccessible for extended periods of time, with potentially life-threatening consequences. This subservient position also imperils SIDN role as a critical public infrastructure steward, which requires specialized attention, access, and control.

We should ask whether SIDN can still be trusted as a steward of .nl?

Furthermore, the move to AWS, however limited, also contradicts its aims of prioritizing social benefit over commercial interests, as its choice for AWS directly contributes to the consolidation of power in the tech industry. SIDN's commercial SaaS ambitions, to be realized through the public cloud, clearly stand to affect its ability to safeguard the public interest now and in the future. It is not enough to question whether alternatives to AWS have been adequately considered. Instead, we should ask whether SIDN can still be trusted as steward of .nl, taking its choice for the cloud as its backbone as a sign of how the organization weighs its public interest mandate against its commercial ambitions—given these fundamental changes to how the organization will function under AWS.

Caught in the Cloud?

In defense of its decision, SIDN inadvertently highlighted the structural harms of moving to the AWS cloud. SIDN maintained that AWS's sophisticated infrastructure and security capabilities offered advantages that outweighed potential risks. They noted the widespread adoption of major cloud platforms by critical services across sectors and argued that appropriate safeguards could mitigate concerns. They also drew attention to a different kind of risk: resisting cloud migration, they argued, would leave the organization behind as government and industry alike shift toward cloud computing.

This is not true. Germany and France, for example, have made the explicit choice to run their cc-TLDs in-house and in the public interest. While deeply flawed, the reasoning underneath the fear of being left behind exemplifies the underlying and significant trend this report emphasizes: the quasi-permanent surrender of vital Internet governance organizations to hyperscale cloud companies. The transfer to these cloud companies can fundamentally alter Internet governance's organizations' stewardship of the infrastructure they are meant to steward. The stated benefits of the move to AWS have not been sufficiently balanced against the full spectrum of harms it poses to SIDN's functioning, visible in the AWS impact on its self-stated mandate of independence and its primary public good responsibilities. Naming and researching these risks, in their entirety, is crucial for understanding the impact of cloudification on Internet governance and its implications for the future of the internet.

For the various flaws in SIDN's choice, we must acknowledge its role in sparking a much-needed and broad debate about the wisdom of moving an array of public institutions to the American cloud. Most notably, there has been a heated public debate about halting the planned shift of the Dutch government to the Microsoft cloud, which has resulted in an informed and robust debate at the highest levels of government.[90] Likewise, it has encouraged Dutch academics to research the functional changes to their universities under the hyperscaler cloud and demand alternatives.[91] Furthermore, the SIDN controversy sparked a collective of tech entrepreneurs to develop such alternatives.[92] Clearly, it is possible to envisions alternative infrastructural futures for the internet,[93] beyond the hyperscaler paradigm. The next section will explore some visions of the future.

The SIDN/AWS situation is a symptom of a larger issue: the lack of a collective vision for what kind of digital backbone both our internet and our society require.

Future Visions: Retaining Domain Expertise

The SIDN/AWS situation is a symptom of a larger issue: the lack of a collective vision for what kind of digital backbone both our internet and our society require. Right now, decisions about the internet are in the hands of individual organizations that increasingly prioritize profit over their public interest mandates.

The SIDN case also reveals the limits of our guardrails: when commercial ambitions override a public service mandate, we often lack strong recourse. When harms extend beyond questions of privacy, digital sovereignty, and consumer surveillance we lack an established discourse to discuss and mitigate these harms. The cloudification of critical infrastructure providers, like SIDN fundamentally, transforms their functioning: their governance, technical decision-making, and institutional culture in ways that current regulatory frameworks and public discussions cannot effectively address. This report is part of a broader push in the Netherlands to develop new vocabularies and action repertoires for cloud accountability.

In January 2025, the Dutch government reluctantly permitted SIDN to proceed with its AWS plans. The move has now been temporarily halted, due to the intervention of a small set of tech-savvy parliamentarians, supported by a broad network of tech critics. The government's initial green light, in spite of widespread concerns, demonstrates how existing oversight mechanisms may be insufficient to protect the public interest in the face of cloudification. As a growing number of Internet governance organizations move to the cloud, we urgently need to revisit the existing guardrails and ensure that they are still capable of protecting the public interest, beyond shallow questions of digital sovereignty.

The cloud changes how SIDN works, shifting it away from its role as public interest infrastructure provider.

At this point, it is unclear what the full impact of AWS on SIDN will be. Yet even now, long before we know whether the full plan will be completed, harms are visible: the cloud changes how SIDN works, shifting it away from its role as public interest infrastructure provider. Across various key facets, from control over computational environments, to its technical self-determination and institutional independence, the organization is bending to the needs and requirements of AWS rather than those of its stakeholders. This is especially concerning, given SIDN itself continues to stress that they are only moving a small part of its work to AWS. Yet, this report demonstrates how even a seemingly small change can come at the overall expense of SIDN's in-house expertise, independence, and public interest commitment. That is, it comes at the expense of the qualities that justify its stewardship of .nl.

The SIDN case study also reveals weaknesses in our current Internet governance regimes. How might it help us articulate visions for the future? Based on the report's analysis, here are six key recommendations for managing critical digital infrastructure in an increasingly commercialized and clouded internet ecosystem:

1. Move Beyond Digital Sovereignty

The debate about cloud harms must move past superficial concerns, and territorial notions, of 'digital sovereignty', which inherently overlook deeper power dynamics. Instead, it is crucial to examine how cloud dependencies restructure Internet governance organizations from within, by changing their level of institutional and technical independence and functioning. These changes impact the overall ability of cloud-bound organizations to serve the public interest, irrespective of potential solutions for concerns rooted in digital sovereignty. Regulatory frameworks for considering cloudification in Internet governance will need to structurally evaluate these institutional changes alongside questions of data, sovereignty, surveillance, or privacy impacts. If we fail to do so, we will not be able to address some of the permanent harms arising from the cloudification of internet governance, and other impacted public interest sectors.

2. Prioritize Public Service over Profit

Organizations like SIDN should prioritize their core mandate, which is to serve as public infrastructure operators, a realization that should put into question the pursuit of commercial Software-as-a-Service (SaaS) expansion through hyperscale clouds. Existing revenue streams from core services are often sufficient without compromising independence. When additional funding is needed, Internet organizations with public interest mandates should explore cooperative or community-owned models that preserve public interest priorities and do not further cement big tech power. The consolidation of such infrastructural power is antithetical to the continued existence of a resilient, open, accessible and affordable internet for all, which is a priority for Internet governance writ large.

3. Create Meaningful Accountability for Cloud Decisions

Cloudification requires oversight frameworks specifically for critical infrastructure and public interest organizations. Such frameworks should be followed where they already exist. They should be (further) developed and implemented beyond government and (Internet) governance organizations, to include other critical industries and sectors, such as telecommunications, media, energy, water, education and healthcare institutions. Their reliance on the hyperscaler cloud is growing at unprecedented rates. At a minimum, such frameworks should include mandatory stakeholder consultation, transparent documentation of decision rationales, evaluation of alternatives, and "red lines" outlining when cloud dependencies prevent organizations from fulfilling their public service missions.

4. Preserve Core Technical Capabilities and Control

Internet governance organizations must maintain essential control over their computational environments and service delivery. This means prioritizing diverse in-house technical expertise and dedicated budgeting and planning for maintaining on-premise or local computing options, as well as internal technical training and knowledge retention. The aim should be to maintain the ability to operate core infrastructure and preserve technical and institutional resiliency, and potentially reverse cloud migrations if needed. In doing so, it will be important for these organizations to follow a multistakeholder process that consults its stakeholders, while also weighing government oversight against maintaining some level of independence from political interference.

5. Imagine, Fund, and Build a Public Interest Internet Infrastructure

Internet governance organizations should move beyond narrow technical and economic metrics when evaluating infrastructure choices. Instead, organizations should lead the public in examining how cloud computing perpetuates extractive practices through profit optimization, massive energy consumption, resource exploitation, and the centralization of power. This requires directing resources, not just away from profit-driven cloud expansion but also toward emergent alternative models of computing. Non-profit foundations, governments, and other grantmaking organizations must step up with substantial, long-term funding commitments to support the development, maintenance, and growth of public interest tech alternatives. We must pursue genuine alternatives to hyperscalers while remaining accountable to values beyond shareholder returns. The aim would be to effect a broader ideological reorientation in Internet governance, which should prioritize people over profit.

6. Invest in Research and Development of Alternative Cloud Futures and Dependencies

The transformative impact of cloud reliance demands a dedicated research agenda and investment in alternatives. We should be willing to refuse the cloud. Academic institutions, public research organizations, and civil society organizations require funding for research into the long-term institutional effects of cloud adoption on (public service) organizations. This research should document emerging harms, develop assessment frameworks for evaluating cloud dependencies, and propose governance models that maintain public interest mandates. In parallel, significant investment is needed to develop and scale viable alternatives to hyperscaler clouds—from community-owned infrastructure cooperatives to open-source cloud platforms and services designed specifically for public institutions. Without dedicated funding streams for both the research and technical development components, public institutions will remain captive to an increasingly consolidated commercial cloud ecosystem with no practical alternatives, however limited.

[84] https://berthub.eu/articles/posts/de-totale-keuze-voor-microsoft/↩

[85] As of this writing, SIDN has not yet developed a plan for what this exit option would look like.↩

[86] Balayn, Agathe, and Seda Gürses. 2024. “Misguided: AI Regulation Needs a Shift in Focus.” Internet Policy Review, https://policyreview.info/articles/news/misguided-ai-regulation-needs-shift/1796, p. 4.↩

[87] https://www.sidn.nl/en/nl-domain-name/verification-of-registration-data↩

[88] https://ainowinstitute.org/publication/from-infrastructural-power-to-redistribution-how-the-eus-digital-agenda-cements-securitization-and-computational-infrastructures-and-how-we-build-otherwise↩

[89] Outages that as we saw on the 19th of July 2024 after the Crowdstrike-Microsoft debacle, are not unthinkable.↩

[90] This latter debate has also been increasing in intensity against the backdrop of the contentious Trump-Zelensky meeting in the White House in February 2025 https://www.lemonde.fr/en/international/article/2025/03/01/europe-shocked-by-explosive-trump-zelensky-white-house-row-prepares-for-a-decisive-summit_6738706_4.html.↩

[91] https://www.uu.nl/en/opinion/open-letter-to-the-executive-university-board-calling-for-a-transformation-to-digital-autonomy↩

[92] https://berthub.eu/articles/posts/communicating-without-musk-and-trump-cloud-kootwijk/ this effort is commendable but it is important to remark that its reference and deference to “Radio Kootwijk” is concerning given the imperial and colonial motives that drove the development of Radio Kootwijk, and its political project of maintaining Dutch control over the various countries it colonized.↩

[93] Paris, Britt S., Corinne Cath, and Sarah Myers West. 2023. “Radical Infrastructure: Building beyond the Failures of Past Imaginaries for Networked Communication.” *New Media & Society*, February. https://doi.org/10.1177/14614448231152546.↩

5. Conclusions

Even if ideal solutions existed for addressing cloud surveillance, sovereignty and data privacy concerns raised in public debates, this fundamental issue of harmful institutional change would remain unresolved.

Can Internet governance organizations fulfill their public interest missions when they no longer maintain control over core functions and services, having moved them to hyperscale cloud providers? This report answers this question with a resounding no. Cloudification instigates permanent, structural changes within clouded-organizations. The case study of SIDN offers a glimpse of what this can look like: the loss of technical resilience and institutional independence, as organizations now shape themselves in accordance with a cloud infrastructure that focuses on profit rather than public need. Even if ideal solutions existed for addressing cloud surveillance, sovereignty and data privacy concerns raised in public debates, this fundamental issue of harmful institutional change would remain unresolved.

Equally concerning is how many alternative cloud initiatives are framed through problematic lenses of "digital sovereignty" or "strategic autonomy"—concepts rooted in militaristic thinking that risk further securitizing digital infrastructure. Such framing often leads to nationalistic approaches that can be equally harmful to public interest values. The challenge is not simply to build a "Dutch cloud" or "European cloud" as nationalistic alternatives, but to develop alternative visions for the role of computing in society that prioritize people over profit maximization. Genuine digital transformation demands more than replacing foreign technology with local equivalents—it requires reimagining the underlying political economy that shapes how digital systems function. Perhaps the most revolutionary alternatives won't aim to match hyperscalers at their own game but will instead question whether we need so much computing in the first place.[94] The growing recognition of cloud computing's massive energy consumption[95] and resource demands add an environmental dimension to this resistance.

You can only remain the maintainer if you continue to maintain.

In terms of Internet governance: This report advocates for a frank and clear discussion of the points at which commercial ambitions, especially cloud-bound SaaS ambitions, come at the expense of the Internet governance commitments to technology that serves the public interest. Technical and institutional resilience is essential to the safeguarding of this mission. SIDN's legitimacy to maintain .nl requires that *they* actually maintain it. Its choice for AWS, which cannot provide the same public interest guarantees and does not allow SIDN full control over the cloud environment it uses, undermines that legitimacy. This puts us at a crossroads: either SIDN should consider alternative hosting architectures, or we should consider alternative hosts for .nl. You can only remain the maintainer, if you continue to maintain. “Stew, if you are a steward,” to quote one of the Dutch academic experts I interviewed. This report uses the SIDN-AWS controversy to demonstrate that we need a vision of Internet governance that understands critical public infrastructure as incompatible with the profit motives of the hyperscaler cloud. The internet should not be turned into someone else’s cloud. While it will be challenging to reverse the trend toward cloudification, we must prepare for a future where the limitations of commercial cloud services in preserving public interest agendas become evident. Luckily, at the time of writing, decision-makers in the Netherlands and Europe are heeding this call.

The internet should not be turned into someone else’s cloud.

This case study also responds to that call by providing an opportunity to think beyond popular anxieties around “digital sovereignty.” Rather than fixating on re-establishing national control over infrastructure—the seemingly contradictory political project that drives Dutch and European digital sovereignty and industrial policy agendas—we must focus on imagining and building an internet that works for all, in an increasingly cloud-driven economy. SIDN struggled after the 2024 announcement of the AWS move, and its choice for this cloud giant amplified limited and limiting discourses around “digital sovereignty.” This should serve as a warning: digital sovereignty concerns can crowd out concerns about the full spectrum of harms associated with the reconfigurations of public institutions in the era of the cloud.

The SIDN-AWS controversy will have lasting impacts on Internet governance in the Netherlands. In the short term, it has led to more stringent governmental oversight of SIDN’s functioning and much needed public debate. There is potential for the development of additional regulatory frameworks for managing vital digital infrastructure in the Netherlands, including the .nl domain SIDN presides over. In the longer term, and extending beyond the Dutch context, the controversy could influence how other countries approach similar decisions about their digital infrastructure. While these immediate regulatory responses are significant, the implications of this case extend far beyond a small Dutch organization’s infrastructure choices.

The SIDN case represents more than a singular controversy. It marks a pivotal moment in the evolution of Internet governance. The choices Internet governance organizations make in the face of the cloudification trend will shape not only the technical architecture of the internet but also the extent to which it remains a public resource. Will the internet become just another profitable service embedded in Big Tech’s cloud empires? This question extends beyond SIDN to numerous public institutions increasingly entangled in commercial cloud ecosystems. Can public institutions, like governments and universities, maintain their missions when running on a corporate hyperscaler cloud? The evidence from cases across Europe suggests that technical dependencies quickly evolve into deep organizational and strategic dependencies as well. When organizations with public interest mandates, like SIDN, chase commercial dreams, they risk losing sight of their public interest missions in the fog of someone else's cloud.

[94] https://www.nrc.nl/nieuws/2025/04/13/we-moeten-anders-nadenken-over-onze-vervuilende-digitale-economie-a4889457↩

[95] https://techpolicy.press/is-more-clouds-the-future-we-want-a-dispatch-from-the-ftc-ai-tech-summit↩

crıtıcal
Infrastructure
lab