Stacking Up

Assessing and improving the digital strategic autonomy of Dutch municipalities

Author: M. van der Wal

Date: 23-06-2025

TU Delft

Stacking Up

Assessing and improving the digital strategic autonomy of Dutch municipalities

By

M. van der Wal

In partial fulfilment of the requirements for the degree of:

Master of Science
in Complex Systems Engineering and Management

at the Delft University of Technology,
to be defended publicly on Monday July 7, 2025 at 10:00

Thesis committee:	Prof. dr. ir. N. Bharosa	TU Delft
	Dr. P.W.G. Bots	TU Delft

Executive summary

Dutch municipalities are highly digitized and experience an increased digital dependency. Between 2017 and 2025, municipal reliance on Software as a Service (SaaS) for their main tasks has increased from 16% to 70%. Municipalities are highly dependent on a small number of US cloud service providers, which together have a 75-90% EU cloud services market share. This dependency raises democratic and geopolitical concerns. US legislation, including the Foreign Intelligence Surveillance Act (FISA) Section 702, grants the US government access to data stored by US cloud service providers, regardless of where it is stored. Furthermore, US sanctions can terminate access to cloud services, as demonstrated by recent cases involving the International Criminal Court prosecutor. Simultaneously, private cloud service providers can implement unilateral changes to services used by the municipalities, without democratic oversight or municipal consent. Current dependencies are however large and run deep. Therefore, any approach should be strategic: full autonomy (autarky) is unfeasible and undesirable.

This thesis addresses these concerns through the lens of **digital strategic autonomy**, defined as the capabilities, capacities, and control to decide and act autonomously on essential digital aspects of our economy, society and democracy. Unlike the binary concept of digital sovereignty, digital strategic autonomy acknowledges degrees of control and better captures the nuanced reality of contemporary digital dependencies. Capabilities refer to the knowledge, skills and tools. Capacity refers to the amount of resources available. Control refers to the influence over capabilities, capacities, decisions and actions.

The research employs a Design Science Research Approach to develop both an analytical theory of digital strategic autonomy and an artefact for municipal application. The methodology combines literature review, semi-structured interviews, actor analysis and legal doctrinal research. The study conceptualizes digital infrastructure through a layered ‘stack’ framework, focusing specifically on the cloud, data & AI, and application layers where municipal vulnerabilities are most pronounced. The research identifies two critical dimensions of digital strategic autonomy: the geopolitical dimension, where foreign jurisdiction poses risks to data confidentiality (the panopticon effect) and service availability (the chokepoint effect), and the public/private dimension, highlighting private actors imposing private values on public service delivery.

Based on this conceptualization, the study develops a self-assessment tool that enables municipalities to evaluate their digital strategic autonomy for specific processes supported by SaaS applications. This tool operationalizes the analytical theory by providing concrete indicators across multiple dimensions. Applying self-assessment tool and an institutional analysis results in technical, institutional and governance measures.

This all culminates in recommendations on three points: Think Big, Act Now, Together. Municipalities must **Think Big** by setting concrete targets such as fully migrating away from non-EU cloud service providers for critical services and elevating digital strategic autonomy to a political priority. They must **Act Now** by applying Haven and Haven+ standards and identifying critical processes where a higher digital strategic autonomy is desirable, i.e. using the self-assessment tool. Following this identification, they are better prepared for the next procurement cycle. Most critically, they must work **Together** through i.a. the Vereniging van Nederlandse Gemeenten to pool resources, conduct and share risk assessments such as the Data Protection Impact Assessments, and leverage collective bargaining power, especially in light of the expiring framework agreement with Microsoft.

This research provides the first systematic approach to digital strategic autonomy at the municipal level by developing a novel analytical framework that synthesizes existing models and operationalizes theoretical concepts, together with an institutional analysis. Future research could further evaluate the self-assessment tool, given the focus of this research on the conceptualization and operationalisation rather than on comprehensive validation. The study contributes to both academic literature on digital strategic autonomy by taking a municipal perspective and contributes to ongoing policy discussions about government digital dependencies.

Contents

List of figures

List of tables

List of abbreviations

AI	Artificial Intelligence
AWS	Amazon Web Services
BIO	Baseline Informatiebeveiliging Overheid
Cbw	Cyberbeveiligingswet
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CoSEM	Complex Systems Engineering and Management
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
EU	European Union
FISA	Foreign Intelligence Surveillance Act
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
NIS 2	Network and Information Systems Directive 2
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
PaaS	Platform as a Service
SaaS	Software as a Service
SSI	Semi-Structured Interview
TCP/IP	Transmission Control Protocol/Internet Protocol
US	United States of America
VNG	Vereniging van Nederlandse Gemeenten
Wdo	Wet digitale overheid

1 Introduction

> “On many digital fronts, European, Dutch and local governments have become too dependent on non-European countries. To reduce that dependency, we need to increase our influence on the design and use of digital technologies and digital infrastructure. Digital independence thus involves several aspects: increasing democratic control, reducing strategic dependencies and thereby reducing vulnerabilities (including in the field of digital security).” (Vereniging van Nederlandse Gemeenten [VNG], 2024, p. 24)

Dutch government organisations and society as a whole are highly digitised. In the past years, a shift has taken place from developing, buying and licensing software and running this on premise, to using Infrastructure, Platforms and Software as a Service (IaaS/PaaS/SaaS). Often, the architecture design and source code is not open, raising concerns surrounding public values such as privacy, transparency and democratic control. Moreover, governments have become dependent on private actors to maintain the confidentiality, integrity and availability of a public service and the associated data when using such services from an external service provider. The values and interests of private actors can, however, conflict with the public values and interests of governments. Furthermore, external service providers can be subject to the jurisdiction of another country. Microsoft, Amazon and Google together hold 75-90% of the Dutch cloud market and are all US companies (Autoriteit Consument en Markt, 2022). Digital services can at the same time provide government organisations with advantages such as scalability and cost-efficiency.

This shift towards digital services can also be observed within Dutch municipalities. In 2017, only 16% of the software used by municipalities for their main tasks were SaaS-applications (M&I/Partners, 2023). In 2025, this is estimated to rise to 70%. Municipalities are mainly concerned about the control over their data when using cloud services (Vereniging van Nederlandse Gemeenten, 2023b). Another main concern is preventing an overdependency on cloud service providers; 81 out of 105 of the municipalities surveyed by the VNG uses Microsoft Azure for IaaS and PaaS (Vereniging van Nederlandse Gemeenten, 2023b).

Managing the risks related to the government’s dependency on a provider of digital services can be described by the pursuit of digital strategic autonomy. Due to geopolitical turmoil, this topic has become more prominent in recent years (Gomes & Okano-Heijmans, 2024), also on the municipal level (De Vries, 2022; Snijders & Wever, 2024; Vereniging van Nederlandse Gemeenten, 2024a; VNG Realisatie, 2024). The city council of Amsterdam unanimously adopted a proposal to investigate how the municipality can become ‘digitally independent’ in 2030 (Van Trigt, 2024).

A similar discussion plays on the EU level (Kroll, 2024) and the level of the central government, following the introduction of a national cloud policy in 2022 which allows government organisations to use public clouds (Hartholt, 2022; Krikke, 2022; van Dijck & Jacobs, 2022). As a result of the political unrest, the state secretary for digital affairs has recently halted the cloud migration of the government’s largest in-house IT service providers, SSC-ICT (Rensen, 2024). The regulator of the Dutch banking sector, De Nederlandsche Bank, also warned for an excessive concentration of the outsourcing of, inter alia, cloud and AI services among Dutch banks (Koning, 2024; Monterie, 2024).

1.1 Research problem and objective

Currently, no established definition of digital strategic autonomy exists, nor do municipalities have a clear strategy to systematically assess and improve their digital strategic autonomy. As such, a clear gap exists between the current and the desired situation. Dutch municipalities are largely dependent on US cloud service providers for the provisioning of cloud services, including the hosting of data and the provisioning of applications which enable and shape public service provisioning. This raises concerns about the availability and confidentiality of data and services, and over the protection of public values. The gap between the current and the desired situation is the lack of control over IT providers in general, and specifically regarding US cloud service providers. Municipalities often have limited resources and a lot of (other) tasks, and have a limited size compared to IT-providers. This thesis addresses this problem by defining digital strategic autonomy, operationalizing this for municipalities and by analysing possible measure to improve digital strategic autonomy. As such, it contributes both to the literature on digital strategic autonomy by providing an analytical theory of digital strategic autonomy and by developing an artefact showing the applicability of the theory within the context of municipalities. The thesis contributes to the ongoing societal and political discussion on the dependence of municipalities and other government organisations on (large, non-EU) cloud service providers.

1.2 Research questions

The following main research question and sub-questions will be answered in this thesis. A further elaboration on these questions is provided in section 2.3.

Main RQ: *What self-assessment tool will support Dutch municipalities in systematically assessing and improving their digital strategic autonomy?*

The function of the self-assessment tool will be to create awareness among municipalities on the status of their digital strategic autonomy. As such, it should function as an eye-opener and clarify what digital strategic autonomy entails when it is applied to a municipality. It is therefore an operationalisation of an analytic theory of digital strategic autonomy developed in this thesis. The tool should allow municipalities to think more focused and systematically on their status of digital strategic autonomy and on possible points of intervention. It should also serve as a tool to identify measures by which municipalities can improve their digital strategic autonomy.

Sub-questions:
RQ1: *What is digital strategic autonomy?*
RQ2: *What are indicators of the digital strategic autonomy of Dutch municipalities on the cloud, data & AI and application layer?*
RQ3; *To what extent does the prototype self-assessment tool support Dutch municipalities in assessing and improving their digital strategic autonomy in the use of cloud services?*

1.3 Relevance to the CoSEM program

The subject of digital strategic autonomy and the use of cloud services by municipalities is relevant to the CoSEM program since it concerns a large complex socio-technical system. Digital strategic autonomy is about technologies, institutions, (conflicting) values, the economy and (geo)politics,

which are all interrelated. Different stakeholders exist on different levels of government, i.e. on the central and the EU level (with values such as autonomy, accountability and transparency), and other stakeholders such as cloud service providers (with interest such as profit and protecting trade secrets). Values and goals of these stakeholders can conflict. The study of digital technologies clearly links to the I&C track of the CoSEM program. The thesis takes into account both the technology, such as cloud services and encryption, and different levels of institutions, such as the extraterritorial application of US legislation leading to digital strategic autonomy concerns. Furthermore, the thesis pays attention to the internal institutional design of the Dutch government. Process management strategies are relevant in this light to determine processes that could result in viable solutions for municipalities to improve their digital strategic autonomy. Lastly, a self-assessment tool is developed in the thesis, adding a clear design component.

1.4 Structure of the thesis

In Chapter 2, we discuss the design science research approach and methodologies. In Chapter 3, we provide a literature overview into the concepts of digital sovereignty and digital strategic autonomy, together with our interview findings. In Chapter 4, we expand on our conceptualization of digital strategic autonomy by developing a ‘stack’ of the digital, leading to our analytic theory. In Chapter 5, we zoom in on the cloud, data & AI and application layers of the stack to identify indicators, and discuss the geopolitical and the public/private dimension of digital strategic autonomy. In Chapter 6, we present the self-assessment tool for municipalities. In Chapter 7, we apply the self-assessment tool and identify measures which municipalities to improve the digital strategic autonomy of municipalities. Lastly, in Chapter 8 we present the research findings, limitations and recommendations.

2 Methodology

In this chapter we outline the research approach used. Section 2.1 introduces the Design Science Research Approach. Section 2.2. introduces the Design Science Research Methodology. Section 2.3 further specifies the research questions and Section 2.4 introduces the different methods used to answer these research questions. Lastly, Section 2.5 summarizes this in the research flow diagram.

2.1 Design Science Research Approach

“Design science is the scientific study and creation of artefacts as they are developed and used by people with the goal of solving practical problems of general interest” (Johannesson & Perjons, 2014, p. 7). According to Peffers et al. (2007), such an artefact includes any designed object that incorporates a solution to a well-defined research problem. Indeed, artefacts include constructs, models, methods and instantiations. (Hevner et al., 2004)

The goal of this research is to develop a self-assessment tool which can be used by employees of the municipality (people) to systematically assess, improve and prioritize their digital strategic autonomy (solving a practical problem of general interest). As such, this is an artefact, which renders the design science research (DSR) approach suitable for the objective of this research.

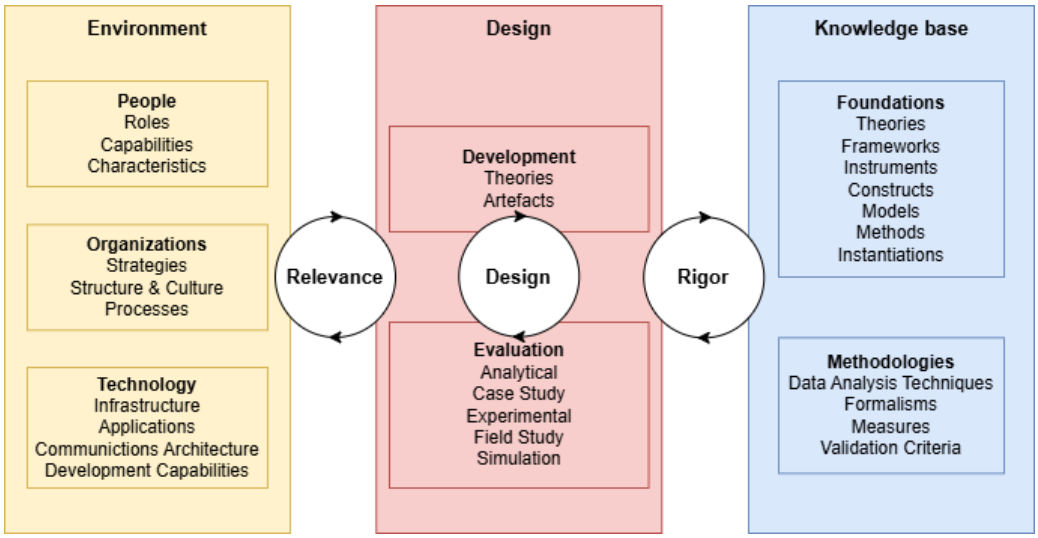
In their highly influential article, Hevner et al. (2004) propose a conceptual DSR framework in which they combine two research paradigms in Information Systems research: design science and behavioural science. This framework is presented in Figure 1. This framework assists in understanding, executing and evaluation design science research. It combines justified true beliefs (the goal of behavioural science research) with utility (the goal of design science), which are inseparable in their view. In this framework, both the ‘business’ environment and the ‘academic’ knowledge base inform the refinement and evaluation of the design, which in turn informs the environment and the knowledge base. This leads to a relevance cycle, where the environment continuously informs the design by needs, and a rigor cycle, where a knowledge base informs the design and evaluation based on previous research.

The environment defines the problem space (Vom Brocke et al., 2020) and consists of people, organizations and technologies. The starting point of a DSR project is often the identification of the actors’ needs and an analysis of the current environment

The knowledge base provides foundations and methodologies. Foundations are prior results from different disciplines which provide “foundational theories, frameworks, instruments, constructs, models, methods, and instantiations used in the develop/build phase” (Hevner et al., 2004, p. 80). Methodologies provide guidelines for the evaluation of a design.

Designing is an iterative process, cycling between development and evaluation. This leads to the total of three cycles in the DSR framework: the relevance cycle, the design cycle and the rigor cycle. An overemphasis on rigor often results in a lowering of relevance (Lee, 1999; Hevner et al., 2004; Benbasat & Zmud, 1999). According to Hevner et al. (2004, p. 88), who side with i.a. Applegate (1999), “it is possible and necessary for all [DSR] paradigms to be both rigorous and relevant.

Figure 1: Design Science Research Framework (Hevner et al., 2004, p. 80)



In the context of our research, Dutch municipalities (and relating organisations such as the central government and the VNG) make up the environment, together with the technologies they use. According to Hevner et al. (2004), the environment specifically also includes the roles of people and the structure and culture of organizations. Therefore, it also includes the institutions in the environment (Williamson, 1998), which we will add. Because the problem space is defined by this environment, the relevance cycle is employed to ensure that the self-assessment tool on digital strategic autonomy is relevant to municipalities. The knowledge base, consisting of *inter alia* the design science research methodology presented in the next section, the literature on digital strategic autonomy, and methodologies presented in section 2.4 ensures academic rigor.

In this thesis, we develop a theory, namely a conceptualization of digital strategic autonomy. Gregor (2006) has proposed a taxonomy for classifying theories[1] based on the extent and manner in which they address four primary goals of theory: analysis, explanation, prediction, and prescription. Following this taxonomy we classify the theory developed in this thesis an analytic theory.[2] The theory developed will primarily describe what digital strategic autonomy is and how it can be analysed. Based on this analytic theory, we operationalize digital strategic autonomy for a part of the 'digital' and develop an artefact, which is the self-assessment tool for municipalities to determine their digital strategic autonomy on a specific process. Lastly, we propose measures to improve the digital strategic autonomy of municipalities. These proposed measures serve as an argument for the utility of both the analytic theory and the self-assessment tool.

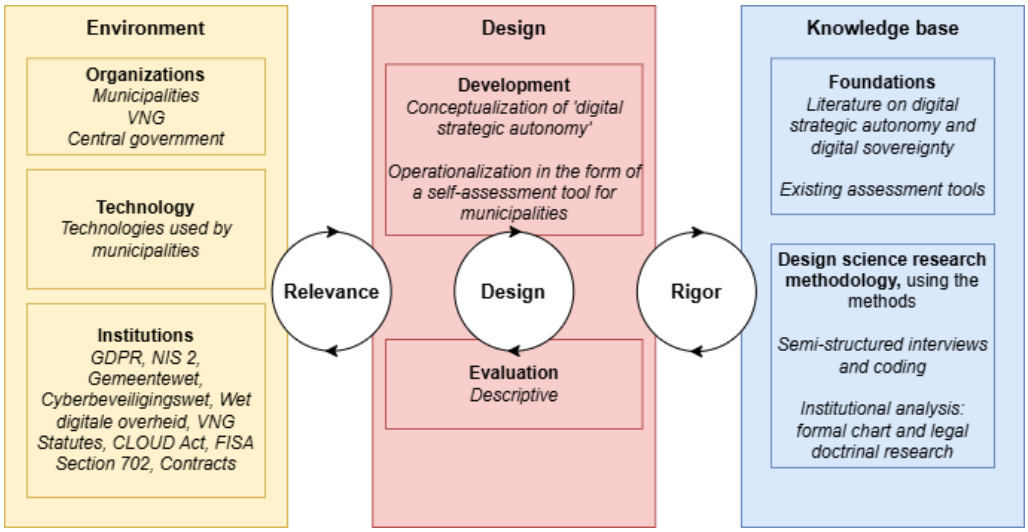
Figure 2 shows on a general level how we use the Design Science Research Framework in this thesis. We will elaborate on the different elements in the next sections.

---

[1] Gregor (2006) takes a wide view on theory, which we will follow: *"the word theory will be used here rather broadly to encompass what might be termed elsewhere conjectures, models, frameworks, or body of knowledge'* (p. 614).

[2] As we will show in Section 4.2, the analytic theory developed does imply causality because of the 'vertical' conceptualization of the digital, where different layers are interdependent. However, the *causa finalis* of the theory is analysis, not explanation.

Figure 2: Adapted Design Science Research Framework

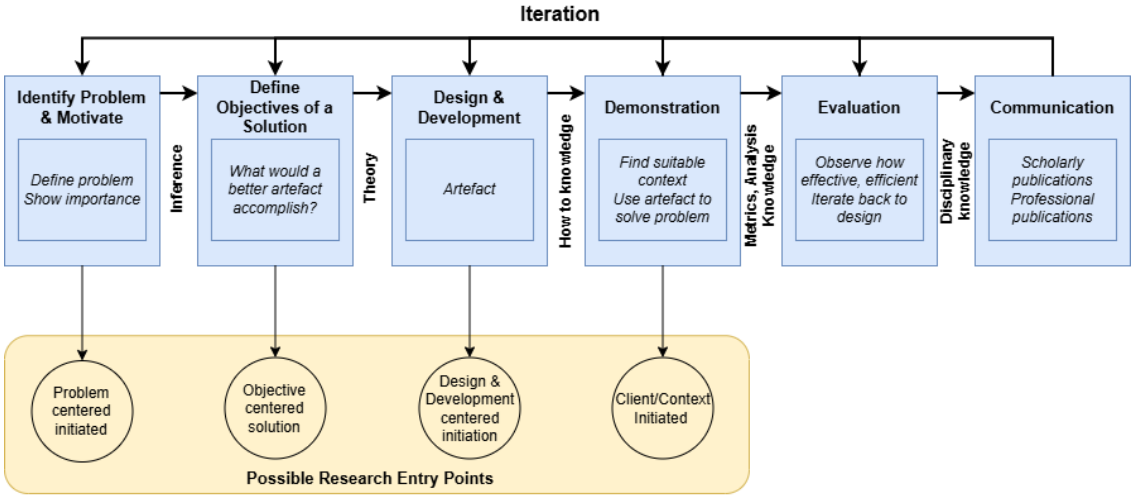


2.2 Design Science Research Methodology

Although Hevner et al. (2004) proposed a conceptual DSR framework and introduced a number of guidelines (design an artefact, problem relevance, design evaluation, research contributions, research rigour, design as a search process, and communication of research), they did not propose a specific process model or methodology. Various process models exist for carrying out DSR, with the model proposed by Peffers et al. (2007) being the most referenced (Vom Brocke et al., 2020). This model is also closely followed in a standard work on design science by Johannesson and Perjons (2014). Peffers et al. designed their methodology based on a consensus-building approach, analysing the process steps in seven articles from different disciplines (namely Archer, 1984; Eekels & Roozenburg, 1991; Hevner et al., 2004; Nunamaker et al., 1990; Rossi & Sein, 2003; Takeda et al., 1990; Walls et al., 1992).

The DSR methodology of Peffers et al. (2007) consists of six process steps (or 'activities'): problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation and communication. The authors describe these steps in a sequence, although any of the first four process steps can be taken as the 'entry point'. A researcher can than iteratively work backwards and forwards through the process steps to provide rigor. Although Peffers et al. (2007) acknowledge the importance of iteration steps, their process model prescribes the first iteration only after the evaluation phase, which itself only follows after the design and demonstration stages. This limits opportunities to assess each step individually and refine the design earlier in the research process (Vom Brocke et al., 2020). In contrast, Sonnenberg and Vom Brocke (2012) advocate for continuous evaluation throughout the process. We present a version of the general DSR methodology with added iteration steps in Figure 3.

Figure 3: Design Science Research Methodology Process Model (based on Peffers et al., 2007, p. 54)



The digital strategic autonomy of municipalities is still uncharted territory, without clarity on the problem definition. For this reason, the research will be problem centred initiated. The main contribution of this thesis lies in the first steps of the process model, namely the conceptualisation and operationalisation of digital strategic autonomy, specifically in the context of Dutch municipalities. We develop the self-assessment tool based on the operationalization of the theory of digital strategic autonomy. Given the limited scope of the thesis, we give less attention to the demonstration and evaluation of the self-assessment tool. As discussed above, we do this descriptively, by building an informed argument of the utility of the conceptualization and self-assessment tool. The measures suggested in Chapter 7 also serve this purpose.

2.3 Research questions

The main research question is: *What self-assessment tool will support Dutch municipalities in systematically assessing and improving their digital strategic autonomy?* We will answer this research question via the following three subquestions.

2.3.1 RQ1: What is digital strategic autonomy?

Because of the novelty of the concept, a separate research question is devoted to the definition of digital strategic autonomy. As part of answering this research question, the concept will be placed in the broader (academic) debate around similar concepts such as digital sovereignty. The research question will be answered based on literature and semi-structured interviews with experts from different perspectives. We will answer this research question by developing an analytic theory of digital strategic autonomy. The 'digital' will be conceptualized as a stack of different layers, which informs the second research question.

2.3.2 RQ2: What are indicators of the digital strategic autonomy of Dutch municipalities on the cloud, data & AI and application layer?

In order to develop a self-assessment tool for municipalities, we must operationalize digital strategic autonomy. The answer to this research question distinguishes indicators of digital strategic autonomy,

specifically for the cloud, data & AI and application layers. We will answer this research question based on literature, semi-structured interviews and institutional analysis. In answering this question, we make the step from theoretical language to observational language within the meaning of Carnap (Koningsveld, 2006, pp. 60–65). After all, a term like ‘control’ cannot be observed, but has to be operationalized by e.g. observing whether certain provisions are included in a contract.

2.3.3 RQ3: To what extent does the prototype self-assessment tool support Dutch municipalities in assessing and improving their digital strategic autonomy in the use of cloud services?

In answering the third research question, we develop a self-assessment tool for municipalities to assess and improve their digital strategic autonomy of a certain process. Part of answering this research question is an analysis of potential measures to improve the digital strategic autonomy of municipalities. We will connect this to the self-assessment framework, but also include overarching or transcending measures, because of the limited scope of the self-assessment tool. The measures will be structured according to the analytical framework of Koppenjan & Groenewegen (2005) and are derived based on literature, the semi-structured interviews and the actor analysis.

2.4 Methods

In our research we have applied two types of methods, namely semi-structured interviews and the coding hereof, and an institutional analysis, based on an actor analysis and legal doctrinal research.

2.4.1 Semi-structured interviews

Semi-structured interviews (SSI), sometimes referred to as elite interviewing, depth interviewing and qualitative interviewing, hold a balance between fully structured interviews and unstructured interviews (Qu & Dumay, 2011). With SSI, the researcher asks (prepared) closed and open-ended questions, together with (unprepared) follow-up questions. This results in a dialogue which provides the opportunity to dive into unforeseen elements. (Adams, 2015). Indeed, semi-structured interviews are “better when it comes to investigating complex issues, as the respondents can express their ideas and feelings in a more unrestricted way” (Johannesson & Perjons, 2014, p. 57). The ill-defined concept of digital strategic autonomy is such a complex issue. Other advantages of the semi-structured interviews are that participants can provide information that cannot be obtained elsewhere, can assist in interpreting (their own) documents and can generally be helpful in understanding the context of the research topic (Richards, 1996). Three interviewees have published papers with a position on digital strategic autonomy (POL-NAT, POL-MUN, COM), which renders these interviews even more useful.

We based the semi-structured interviews on a predefined list of interview questions, which can be found in Appendix C. We expanded on some topics, depending on the background of the interviewee (Qu & Dumay, 2011). Furthermore, the list of questions was a living document during the research: “in the field, as feedback quickly begins to accumulate, adjustments will need to be made” (Adams, 2015, p. 499). We ended each interview with an open-ended question, asking whether the interviewee thought there were any other topics deemed relevant which we did not yet cover. This verified the completeness of the acquired information and enables new information or additional insights (Richards, 1996; Solarino & Aguinis, 2021).

A limitation of this methodology is that the analysis of the interviews can be time-intensive. Another (potential) limitation is that the answers are contingent on the interviewer (Qu & Dumay,

2011). Different researchers with the same predefined SSI-protocol ask different follow up questions, using a different language and in a different way. We countered this disadvantage by comparing the answers of interviewees with (gray) literature on the topic and by explicitly acknowledging this as a research limitation. See section 8.2 on this point. The disadvantages do, however, not outweigh the advantages of semi-structured interviews: obtaining nuanced knowledge of in-depth personal experience with digital strategic autonomy, especially within the context of municipalities.

Appendix A lists the different interviewees and their relevance for this research. We found the interviewees via the network of the researchers and via other research activities discussed in Section 2.4.5. We approached interviewees based on their expertise on and/or professional involvement in digital strategic autonomy. We held the interviews in the native language of the interviewees (Dutch) and they took approximately 45 minutes. We translated all quotes used in this thesis into English. Any translation error is the fault of the researchers.

2.4.2 Coding the interview transcripts

We transcribed all interviews in full and coded the transcripts using ATLAS.ti 25. “Coding is not a precise science; it’s primarily an interpretative act” (Saldana, 2009, p. 15; Sipe & Ghiso, 2004, p. 482). The SSI-guideline presented in Appendix C provides more transparency on our interpretation of the answers, by showing the language and concepts we used in the questions. We coded the transcripts with a combination of deductive and inductive coding. We determined ‘a priori’ codes based on the outcome of the literature overview, which is a form of a deductive approach. This formed a general coding frame. Because of the novelty of the concept, we used an inductive approach in parallel, where we added other codes based on the interviews.

After the first coding cycle, we performed a second cycle. During this axial coding cycle, we grouped codes in categories depending on overlapping themes. These categories are the different ‘axes’. Each cycle implies an iterative process, during which codes from a previous cycle are reassessed and changed accordingly. Appendix D presents the codes and their groundedness.

2.4.3 Actor analysis – formal chart

As part of the problem explication phase, we performed an actor analysis to identify the relevant actors and their relations by means of a formal chart. We followed the steps described by Enserink et al. (2022) in doing so. Indeed, the digital strategic autonomy of municipalities includes the relationship of municipalities to other actors. We present this formal chart in Appendix E.

2.4.4 Legal doctrinal research

As part of the institutional analysis we performed legal doctrinal research. Following this method, applicable laws and policies can systematically be described (Tjong Tjin Tai & Verbruggen, 2022). We employ this methodology to describe applicable US legislation diminishing the control of municipalities over their data and services. We also apply it to discuss legislation which can contribute to digital strategic autonomy. Relevant legal provisions are analysed based on the legal provisions, case law, secondary literature and parliamentary documents.

2.4.5 Other research activities

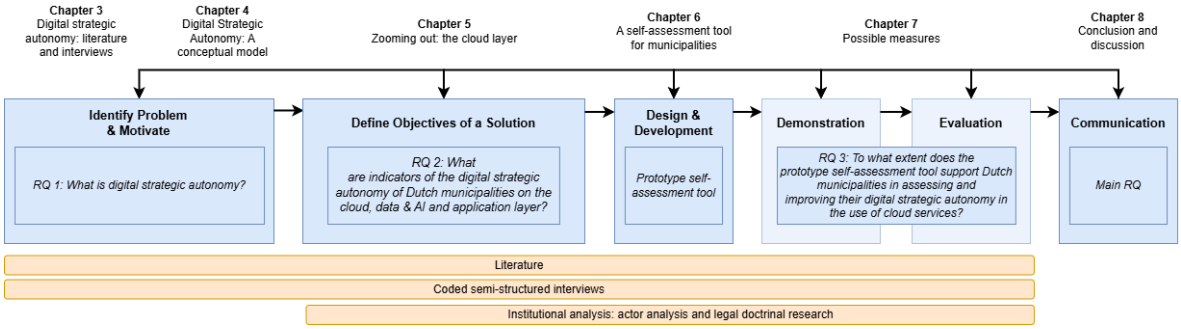
During this thesis, we regularly worked at the offices of Digicampus. Digicampus is an innovation ecosystem in the Netherlands where government, business, academia and citizens (a ‘quadruple helix’) explore digital public services. Working at their offices gave us the opportunity to regularly discuss our research with various employees, including those who had experience with and connections to municipalities. Digicampus is also initiating a Centre of Compentence on Digital

Autonomy, together with AMS Institute, the municipality of Amsterdam, TU Delft, VNG and the Ministry of the Interior and Kingdom Relations. Its ambition is to share knowledge, develop norms and practical tools to increase the digital strategic autonomy of the public sector. During some of their project group meetings, we presented our work and discussed our research. Lastly, we participated in an expert session of Platform voor de InformatieSamenleving and AMS-IX on identifying all the arguments for and against the use of large non-European cloud services (Platform voor de InformatieSamenleving & AMS-IX, 2025). All these provided us with further insight into the environment.

2.5 Methodology overview

The above is summarized in Figure 4. As can be seen, and as argued in Section 2.1-2.2, the main focus of the research lies in the conceptualisation and operationalization of digital strategic autonomy. We present the self-assessment tool and connected it to potential measures. However, this is only done to a limited extent due to the scope of the thesis. Instead, attention is drawn to other possible measures based on an analysis of the relevant institutions and actors.

Figure 4: Methodology overview



3 Digital strategic autonomy: literature and interviews

This chapter will provide a literature overview on various concepts related to digital sovereignty and digital strategic autonomy. This overview is enriched with the data obtained from the interviewees. Firstly, we introduce the conception of digital sovereignty and digital sovereignty *claims*. Secondly, we draw attention to the shortcomings of this concept and introduce an alternative concept, namely digital strategic autonomy. Lastly, we synthesize our findings and argue why we follow the definition of digital strategic autonomy presented by Timmers (2024).

3.1 Digital sovereignty and digital sovereignty claims

In 1996, John Perry Barlow famously published 'A Declaration of the Independence of Cyberspace', linking the digital with (a lack of) state sovereignty:

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." (Barlow, 1996)

The decades hereafter, however, showed that this hope did not hold (Harvey & Moore, 2023; Pohle & Voelsen, 2022; Svantesson et al., 2023). States do try to control the digital realm. Digital sovereignty can be seen as a discursive practice rather than as *one* organisational concept of the digital (Pohle & Thiel, 2020). Various definitions and connotations of the concept exist. Generally, digital sovereignty relates to "ideas of independence, control and autonomy" for an actor in the digital realm (Couture & Toupin, 2019, p. 2317). Or as Falkner et al. (2024) put it: "the core of digital sovereignty stipulates the need for control of the digital" (p. 2102).

Floridi (2020) conceptualizes digital sovereignty as the "control of the digital", and control as "the ability to influence something (e.g. its occurrence, creation, or destruction) and its dynamics (e.g. its behaviour, development, operations, interactions), including the ability to check and correct for any deviation from such influence" (2020, p. 371). Roberts et. al follow these two definitions and define digital sovereignty as "a form of legitimate, controlling authority over—in the digital context—data, software, standards, services, and other digital infrastructure, amongst other things" (2021, p. 6). Understandings differ, however, depending on the actor, the national contexts and the form of self-determination prioritized. This diversity of narratives on digital sovereignty can be seen as "not a bug, but a feature" (Lambach & Oppermann, 2023, p. 705). The broadness of the concept makes it attractive to use for different actors (Pohle et al., 2024). As such, it functions as an umbrella construct (Hirsch & Levin, 1999).

Pohle & Thiel (2020) distinguish three types of digital sovereignty *claims* based on different types of self-determination. The first type of claims are what Pohle & Thiel describe as the "most prominent category of digital sovereignty claims, [where] the emphasis is on the idea that a nation or region should be able to take autonomous actions and decisions regarding its digital infrastructure and technology deployment" (2020, p. 8). These types of claims are driven by concerns surrounding state autonomy and national security. Typical state measures stemming from this concern are data localisation, where the processing of data is moved and confined to the territory of the state.

Furthermore, states invest in their own knowledge and resources to develop and maintain their own digital infrastructure.

The second type of claims is focused on the autonomy and competition of states in the digital economy. Here, the prime concern is the economic interests in the digital environment and especially the relation between the national economy and foreign technology providers. Typical state measures stemming from this concern are policies to improve the local economy and competitors, such as via subsidies and trade restrictions.

The third type of claims is based on the self-determination of citizens (as opposed to nation states in the first two types). Here, digital sovereignty is the capacity of individuals to "take actions and decisions in a conscious, deliberate and independent manner" (Pohle & Thiel, 2020, p. 11). Typical measures for these claims are economic incentives to develop user-friendly technology and the introduction of privacy enhancing technologies.

All of the types of digital sovereignty claims described by Pohle & Thiel (2020) concern the self-determination of a certain actor in the digital sphere. Meiring et al. (2023) also adopt this approach of distinguishing digital sovereignty *claims* in the context of the academia. For the European context, Pohle and Thiel (2020) argue that digital sovereignty is often used as a shorthand "for an ordered, value-driven, regulated and therefore reasonable and secure digital sphere" (p. 13), which effectively combines the three types of claims described above (Pohle et al., 2024). Pohle et al. (2024) furthermore point out that digital sovereignty, in almost all understandings of the term, is mainly seen as a process opposed to a status. They argue that actors rarely see digital sovereignty as an attainable endpoint, and that the path to improve it depends on the specific context.

Building upon the claim that digital sovereignty is best seen as a discursive practice, Pohle (2023) stresses that this does not imply that the concept should be seen as a buzzword or merely a policy principle. She argues that digital sovereignty in the EU context is an expression of the understanding that the 'open and free' internet, resembling the whole digital sphere, did not live up to the expectations in terms of that openness and freedom. Especially the revelations of Edward Snowden in 2013 showed how Europe was dependent on digital infrastructures controlled by states and entities not in their sphere of influence (Glasze et al., 2023). This realisation formed a sharp contrast with the libertarian perspective on the internet as a sphere escaping the control of states, expressed by e.g. Barlow (1996). Furthermore, the realisation grew that Europe mainly depends on non-European IT service providers for almost all digital technologies. As such, Pohle (2023) argues that the European call for digital sovereignty should be understood as a shift in "the belief system that underlies our perception of global digital connectivity" (p. 4). This shift is according to Pohle best understood in the context of the historical developments described above, and not as a form of protectionism or authoritarianism.

Pohle et al. (2024) point out that a neglected question in digital sovereignty research is the question how the sovereign powers (the actor claiming self-determination) itself can be controlled. They argue that it is insufficient to propose that private actors without democratic legitimacy and accountability (Pohle & Thiel, 2020) are being submitted to public institutions. In their view, it is also necessary to constitutionalize digital sovereignty and design procedural frameworks that allow for public reflection on, and control of, the public institutions themselves. Similarly, Maciel argues that "The decision-making and governance of policies being adopted under the banner of digital sovereignty must be socially anchored and socially driven" (Maciel, 2025). Roberts (2024) agrees that most digital sovereignty research focuses solely on the *control* over digital technologies, instead of on *legitimate* control, which is a normative view on the authority of the sovereign. We acknowledge that this is a valuable line of research, although it is not the primary focus of this thesis.

3.2 Shortcomings of the concept 'digital sovereignty'

In the European context, the pursuit of digital sovereignty also includes the protection of human rights and democratic values, enshrined in for example the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. Pohle (2023) argues that the concept of "sovereignty" might not be the most suitable in this regard, as it is traditionally more associated with control and authority than with the aforementioned values. An interviewee from a government organisation argues along similar lines: "Sovereignty [as a concept] also comes up a lot, but that is actually also difficult to position, because it might have the connotation of "a sovereign Netherlands". At the same time, though, we are connected in European and international contexts." (GOV-VNG-1).

Another conceptual problem with digital sovereignty is that sovereignty traditionally, from an international law perspective, refers to the exclusive right of a state to exercise the functions of a state inside of its territory.[3] No widely recognized concept of digital sovereignty exists in international law: "Often, what people mean when they now speak of "digital sovereignty" and related concepts is simply "control." Thus, those who speak of digital sovereignty […] merely make use of the weight and status that the term "sovereignty" lends to the underlying goals pursued under the banners of "digital sovereignty" (Svantesson, 2023, p. 70; see also Svantesson et al., 2023).

Sovereignty is anchored in territoriality and of a binary nature (the right is *exclusive*) (Svantesson et al., 2023). As one of the interviewees said: "I myself always say "digital sovereignty doesn't actually exist". [In the European context] you can only hope and dream of strategic autonomy. Because sovereign is 1 or 0. You either are or you are not" (GOV-VNG-2).

The digital sphere, or cyber*space*, does not have the borders or territories of traditional nation states, although territorial sovereignty could apply to, for example, data centres on the territory of a state (Michels et al., 2023). Furthermore, only nation states can claim to have sovereignty in international law, and translating the concept to supranational organisations such as the EU, or local bodies such as provinces and municipalities, poses difficulties. Authors arguing for this, such as Floridi (2020) and Michels et al. (2025), often adopt a political sciences perspective of the concept of sovereignty. In turn, sovereignty can also only be violated by other states or non-states actors whose conduct is directed or controlled by a state. A state cannot be held responsible for the actions of private entities that do not meet this requirement. Conceptualizing digital sovereignty in line with the established concept of sovereignty in international law would therefore leave acute concerns stemming from the direct dependency of government organizations on private companies out of scope (Roberts, 2024).

Another more practical objection to the concept was raised by two interviewee's who signalled that companies use the term to market their products and services (see also Grohmann & Alexandre Costa Barbosa, 2024; Hoepman, 2025). As one of the interviewees said:

> "Sovereignty, digital sovereignty, it is then often called, is a concept that unfortunately has also been quite hijacked by a number of large companies, including hyperscalers. They say, we can offer that too, ignoring especially the geographical sovereignty component of 'what if we actually get into a trade conflict, for instance, or tensions increase, or there are other circumstances in which we as the Netherlands or in EU cooperation must be able to produce and deliver services ourselves and can no longer lean on other superpowers.' That makes that I do prefer autonomy." (POL-NAT)

[3] This is also known as the Westphalian notion of sovereignty, based on the treaties of the Peace of Westphalia in 1648.

Lastly, from an international law perspective, sovereignty is based on the normative ideal that nation states are legally equal, which ignores actual power differences and differences in abilities between states (Glasze et al., 2023; Michels et al., 2025). The different concerns and digital sovereignty claims described above relate to those actual power differences.

For all of these reasons, we will shift attention to the concept of digital strategic autonomy, which better captures these power differences. Digital strategic autonomy can then be understood as the means to achieve sovereignty (Moerel & Timmers, 2021)

3.3 Digital Strategic Autonomy

3.3.1 Definition

Moerel & Timmers (2021) state that digital sovereignty is currently the common terminology in debates and literature, but that digital strategic autonomy is a better term to describe the means to achieve sovereignty and operationalize it. Digital strategic autonomy refers to the digital dimension of strategic autonomy, which is a concept that originated in French military thinking and Indian diplomacy (Timmers, 2024; Česnakas & Juozaitis, 2023).

Digital strategic autonomy can be defined as: “the capabilities, capacities, and control to decide and act autonomously on essential [digital] aspects of our economy, society and democracy” (Timmers, 2024, p. 577; see also Moerel & Timmers, 2021, p. 8; Timmers, 2019a, p. 12, 2019b, pp. 2–3, 2022).

Capabilities refer to the knowledge, skills and tools. Capacity refers to the amount of resources available. Control refers to the influence over capabilities, capacities, decisions and actions. Democracy can also be seen as the institutions of economy and society, which renders the definition applicable for non-democratic countries. (Timmers, 2019a, 2019b). The definition is largely non-normative in nature, although the identification of “essential aspects” is subjective and holds a normative component (Timmers, 2019b). Furthermore, Timmers argues that the element “our” depends on “who ‘we’ are and how we interpret sovereignty, which is not a matter of definition but rather of assessment and judgment” (2024, p. 577).

This definition of digital strategic autonomy, with a specific mention of economy, society and democracy, encompasses different types of digital sovereignty claims described by Pohle & Thiel (2020) and discussed in Section 3.1. Two interviewees also referred to this definition in their interview (POL-NAT and GOV-VNG-2). Contrary to the concept of digital sovereignty, digital strategic autonomy captures concerns stemming from the direct dependency of government organizations on (large) private companies (Roberts, 2024; Schaake, 2024), for example because this could diminish their control.

Economic interests concern the economic ecosystem, value creation and knowledge. A lack of innovation could result in new dependencies and less autonomy, because newly developed technologies have to be sourced from abroad. This dependency can deepen - new AI services for example often require large amounts of computational power from cloud services, leading to multiple new or stronger dependencies.

Social and democratic interest concerns (the trust in) the rule of law and the functioning of the state. This also relates to democratic legitimization and accountability. The digitalization of government processes always results in new vulnerabilities and dependencies which could disturb the functioning of the state (Dutch Council of State, 2018). An example is the use of election software and hardware from the French company Safran during the 2017 elections in Kenya, which ultimately led to the annulment of the election results and unrest (Passanti & Pommerolle, 2022; Schaake, 2024).

This definition links closely to EU policy definitions of digital strategic autonomy, such as the one proposed by the European Political Strategy Centre: “the capacity of a political entity to pursue its own course in international relations, that is, to set its own objectives and act upon them” (2019). Furthermore, multiple Dutch government organisations follow this definition of digital strategic autonomy (Cyber Security Raad, 2021; Netherlands Court of Audit, 2025).

3.3.2 Strategic approaches

Moerel & Timmers (2021) identify three approaches to digital strategic autonomy, which further describe the ‘strategic’ aspect: the (i) risk management approach, the (ii) strategic partnerships with like-minded actors approach and the (iii) global common goods approach. A fourth approach would be autarky, where one actor tries to have full control and all capabilities and capacities, and thereby would have full digital autonomy (Timmers, 2024). This approach would, however, economically and practically be undesirable and hardly feasible. States would not benefit from economies of scale, specialisation and global supply chains and are currently highly interdependent, either directly or indirectly on foreign providers, as we will further show in this thesis.

The approaches are not mutually exclusive, but in analysing and designing policies, one of the approaches can often be identified as the basic premise.

The *risk management approach* is the most open approach, where the measures taken depend on the risk at hand. That is, they are proportionate to the how critical and sensitive an object is. The risk is determined by the product of the Likelihood of an event occurring and the Impact it has. Examples of this approach are legislation such as the General Data Protection Regulation (data protection) and the NIS 2 Directive (cyber security) and the obligations set out herein. For this approach, various institutions are possible.

The *strategic partnerships approach* is focused on collaborating with like-minded actors, which can be both public and private organisations. An important element of this approach is excluding or limiting dependencies on actors that are not like-minded. Moerel & Timmers (2021) argue that this intention does not exist in the risk management approach. This is partly because risk management focuses on determining case-by-case risks and argues that even risks from not-like-minded actors could in principle be mitigated. Examples of this approach are multi-lateral agreements and contractual public-private partnerships. A variation of this approach is the *strategic interdependency* approach, where not-like-minded actors share mutual dependencies (Bendiek, 2018).

The *global common goods approach* focuses on protecting or establishing commons and common goods on a global level. Here, solutions are developed based on shared, global interests that transcends national interests. Examples are the original vision on the internet and still existing elements of the internet such as the Domain Name System and climate treaties.

3.4 Additional interview insights

Multiple interviewees noticed that a lack of consensus exists on the concepts and their definition: “There is a lot of debate about it. There is no single fine definition that everyone embraces” (SCI), “The terminology still sometimes goes from left to right. From digital independence to digital dependence, from digital sovereignty to strategic digital autonomy. Actually, I don't think we know it very well. It is mostly something we have to start doing” (GOV-VNG-2), “Then we said, that also falls under the broader umbrella of digital independence/dependence/strategic autonomy. And that terminology is really not yet unambiguous” (GOV-VNG-1), “I still haven't quite figured out exactly what the differences are [between the concepts], it's more about the idea behind it for me” (POL-MUN), “I

talk about autonomy more often for several reasons. I think you can use terms fairly interchangeably and generally do talk about the same concepts*"* (POL-NAT). In contrast, one of the interviewees distinguished the concept as follows:

> "You actually have sovereignty and you have a kind of independence. And those two things get mixed up sometimes. Very simply put, sovereignty is really "Who has the last word?", and that's mainly about privacy and data. And dependency is more of "where are your dependencies and where are you yourself not in complete control?" (ENG-SCC)

This comment aligns with our finding that sovereignty is of a binary nature (you have the last word, or you don't) and that digital strategic autonomy is about control, capabilities and capacities. However, the question 'who has the last word' is also a dimension of control. Therefore, we can conceptualize this as a part of digital strategic autonomy.

3.5 Subconclusion

Synthesizing the findings from the literature and interviews, digital strategic autonomy serves as a more precise and actionable concept than digital sovereignty. It captures the ability of an actor to independently decide and act on essential digital aspects of its economy, society, and democracy by having sufficient capabilities, capacities, and control. The definition acknowledges that, unlike the binary and territorially anchored notion of sovereignty, digital strategic autonomy is context-dependent, more operationalizable, and better suited to address power differences, including those arising from direct reliance on large private actors. The definition from Timmers (2024) which we opt to use ("*the capabilities, capacities, and control to decide and act autonomously on essential [digital] aspects of our economy, society and democracy"*) does not yet address the 'digital aspects' that are the object of digital strategic autonomy and of capacities, capabilities and controls. Therefore, we expand on this in the next chapter.

4 Digital Strategic Autonomy: a conceptual model

In the previous chapter, we argued why we opted to use the definition of digital strategic autonomy presented by Timmer, namely "*the capabilities, capacities, and control to decide and act autonomously on essential digital aspects of our economy, society and democracy"* (2024, p. 577). In this chapter, we will introduce the model of the stack to further define those 'digital aspects'. From this chapter on, we will use consistently use the concept 'digital strategic autonomy', even though authors referenced might use different terminology. Based on a synthesis of different stacks, we propose our own stack, the 'working stack' for this thesis. We show the interdependency of the different layers in stack, and based on this analysis zoom in on the digital strategic autonomy for the cloud, data & AI and application layers.

4.1 Verticality and the stack

Multiple authors refer to 'the digital' in the sense of digital strategic autonomy by distinguishing different layers and a certain verticality.

Floridi (2020, pp. 370–371) refers to data, software, standards and protocols, processes, hardware, services, and infrastructure. Roberts et al. (2021) distinguish between "data, software, standards, services, and other digital infrastructure, amongst other things" (p. 6). Falkner et al. (2024) describe the "physical layer (resources, infrastructure, devices), the code layer (standards, rules, design), and the information layer (content, data)" (p. 2102) - Chander & Sun (2021) distinguish the same layers. Tretter (2023) argues that both "analog infrastructures and hardware as well as digital data and software" (p. 19) are important in determining digital strategic autonomy. In their analysis of the technopolitical configuration of the internet, Pohle and Voelsen (2022) explicitly refer to an infrastructure layer and an application layer.

Sheikh (2022) refers to other authors who describe the digital in vertical terms; Van Dijck (2021) suggests the image of a tree as a constitutive metaphor to analyse platforms "whose operative power is wielded through hierarchical and interdependent layers" (p. 2802). Floridi (2014) uses the following image to describe a vertical order: "As in a classic Renaissance house, we now inhabit the *piano nobile*, the upper, noble floor, not even knowing what happens in the ground floor below us, where technologies are humming in the service rooms" (p. 37).

A set of different layers organized vertically is also called a *stack*. A stack provides a certain product or a service. The layering is *vertical*, because each layer typically depends on the layers below. The highest layer in the stack is often closest to the user. An example of a stack is the Open Systems Interconnection (OSI) stack, which is a reference model for data communication standards (International Organization for Standardization, 1994). Another example is the TCP/IP stack, or the Internet protocol suite, which prescribes protocols used for the internet. That stack is based on one of the earliest stack models, for the ARPANET (Advanced Research Projects Agency Network). That network was a predecessor of the internet, developed for and funded by the United States Department of Defense.

Multiple respondents also referred to a stack in the context of digital strategic autonomy (POL-MUN, POL-NAT, GOV-VNG-2). For example:

> "That makes that I do prefer autonomy. Which is about being able to exercise a high degree of control over the technological means you use. And there are degrees of autonomy in that too. In the broadest form, you would have the whole supply chain, from raw materials and chips to the software application layer - the whole stack" (POL-NAT).

In contrast, another respondent focussed mainly on data and information (SCI), or on dependencies it saw in a concrete case, such as identity and access-management and a database (ENG-SCC).

In his highly speculative and philosophical work[4] *The Stack: On Software and Sovereignty*, Bratton (2015) proposes the model of 'The Stack' as "a way that we might map political geography, but also for how we understand the technologies that are making that geography" (p. 4). This vertical political geography is tuned to what Bratton calls the era of planetary-scale consumption. It marks a break with the global order of Westphalian nation-states: the world divided in borders on a horizontal plane. As such, "The Stack provides a new [vertical] global governing logic through which sovereignty operates" (Couture & Toupin, 2019, p. 2311). Bratton distinguishes six interdependent layers: *Earth, Cloud, City, Address, Interface* and *User*. The Stack is a model of a complex system, "an *accidental* megastructure, one that we are building both deliberately and unwittingly and is in turn building us in its own image" (Bratton, 2015, p. 5). As such, The Stack describes an emergent structure with non-linear logic.[5]

Sheikh (2022, 2024) adopts Bratton's notion of distinguishing different layers of a global stack which structures the digital world. Sheikh introduces his own stack with seven different vertical layers: *resources, chips, network, cloud, intelligence, applications and connected devices*. This framework serves as "an analytical tool that maps dynamics in the digital world" (Sheikh, 2022, p. 27). He adopts the definition of digital strategic autonomy proposed by Timmers (2022), and determines the capacities and different policies of the EU on each of the layers via desk research. Based on the analysis, Sheikh proposes different policy directions. This model of the stack has since been adopted by multiple authors (Hoeksema, 2024; Roberts, 2024; Rone, 2024; Kotulski et al., 2024).

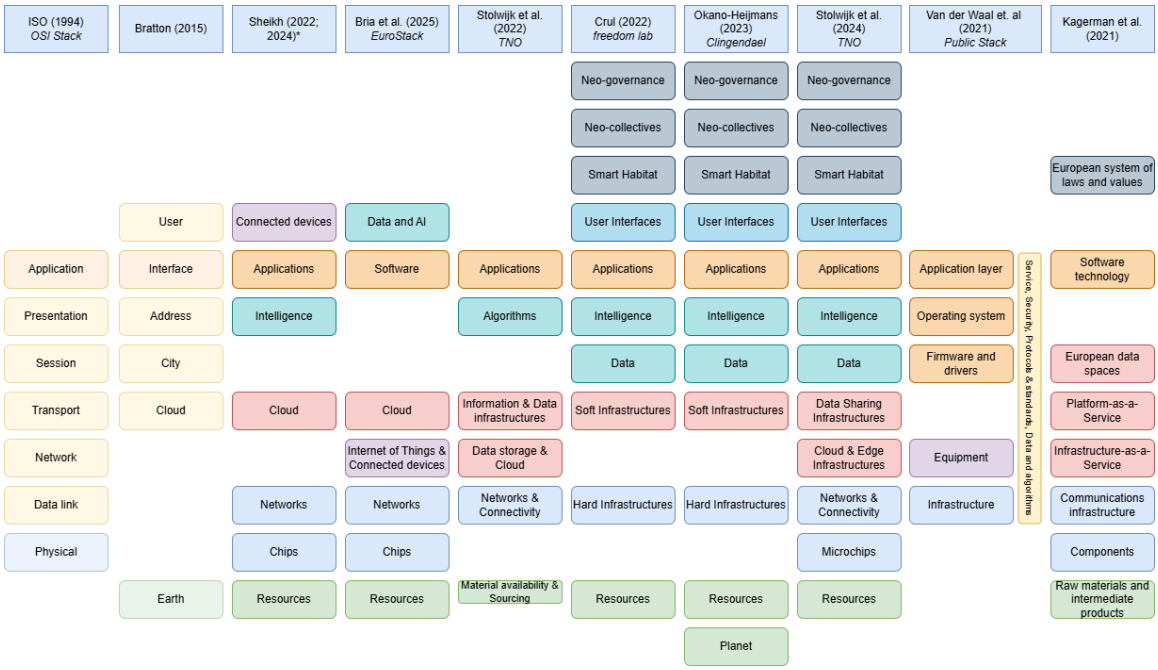
Sheikh does not argue whether his framework provides analytical value on different levels of government, such as a single country or a municipality. It is also yet unclear is this framework is helpful in determining controls and capabilities, next to capacities. Furthermore, a validation for the analytical value of the specific layers is lacking. Reference is made to "common industry distinctions" (Sheikh, 2022, p. 25), but it remains unclear whether these specific seven layers provide the most analytical clarity. This question is even more pertinent when the layers are compared to other proposed stack serving as an analytical model (Bria et al., 2025; Crul, 2022; Kagermann et al., 2021; Okano-Heijmans, 2023; Stolwijk et al., 2022, 2024; van der Waal et al., 2021). Indeed, as Lovink (2020) rhetorically asks in response to Bratton (2015): "Does the one stack exist or should we rather speak of The Stacks, a rainbow of a thousand stacks" (p. 721). A comparison of the different stacks is provided in Figure 5.

---

[4] Bratton (2015, p. XVII) categorises his work as follows: "This book is both technical and theoretical. It is unapologetically interdisciplinary in its perspective and its project; it is a work of political philosophy, and architectural theory, and software studies, and even science fiction."

[5] The model has been criticized for being too infrastructural (as opposed to societal) and as a "static metaphysical view", lacking a perspective on the role of different actors, their interests and their ideologies (Lovink, 2020, p. 722).

Figure 5: A comparison of different stack frameworks



We coloured the layers based on their (perceived) overlap to improve the interpretability of the comparison. It is immediately apparent that the different stacks have differences and overlap, and that some are based on each other; Okano-Heijmans (2023) and Stolwijk et al. (2024) for example are based on Crul (2022), which in turn draws inspiration from Bratton (2015). Not all stack models presented here are explicitly designed to determine capacities, capabilities or control in the context of digital strategic autonomy. However, all of these models do serve an analytical purpose touching on this, as we will now show.

Bria et al. (2025) propose the 'EuroStack initiative' as a policy strategy for the European Union, with the goal of strengthening its digital strategic autonomy, understood as "the capabilities, capacities, and control in the digital domain that are necessary to safeguard sovereignty" (Bria et al., 2025, p. 42; Timmers, 2022). Part of their initiative is the proposal to develop a European common digital stack. Their model of the stack is also used to identify key countries and leading firms for each layer. The EU position is also assessed, leading to the recommendation to strengthen capabilities within individual layers of the digital stack. The stack is based on, but distinguishes slightly different layers in a different order compared to, Sheikh (2022). Connected devices & IoT are in the middle of the stack, while Sheikh puts the similar 'connected device layer' on top of the stack. It could be argued that the approach of Bria et al. presents a verticality where every higher layer is more virtual (or more abstract, or less material) than the one beneath. In contrast, Sheikh's ordering is more close to the idea that the higher the layer in the stack, the closer it is to the end-user.

Stolwijk et al. (2022) present a 'technology level model' to assess the dependence of the Netherlands and Europe on foreign countries. Part of their model are five technological layers and it also encompasses influencing factors (material availability and sourcing), potential disrupting factors (smaller, cheaper and more powerful hardware and new paradigms for cryptography & quantum technology) and boundary condition factors (policies and business models). Per layer, the authors asses the digital sovereignty of the European Union and the Netherlands, which they define as the "control over the design and use of (business) critical digital systems, algorithms and the data generated and processed with them" (Stolwijk et al., 2022, p. 6; Moerel & Timmers, 2021).

Inspired by the stack of Bratton (2015), the *freedom lab* envisions a stack of ten different layers, which "presents digital technology as a layered structure of technological and non-technological components" (Crul, 2022). They argue that their stack is a tool to assess the digital strengths and weaknesses of an organization, industries or a nation. Furthermore, the stack enables the identification of opportunities and the development of new initiatives. The top three layers of the stack show the interdependence between the technological layers and cities, communities and institutions. Both Stolwijk et al. (2024) and Okano-Heijmans (2023) partly adopt this stack in their research.

Stolwijk et al. (2024) combine their previous framework (2022) with the framework of *freedom lab*. They expand the soft and hard infrastructure layers and leave their previous approach of including influencing factors, potential disrupting factors and boundary condition factors in their model. They expand on their previous definition and add that "Digital sovereignty means having the digital capabilities and capacities to produce, deliver and use digital goods, services, and infrastructures and having control over these in order to safeguard sovereignty." (Stolwijk et al., 2024, p. 3; Moerel & Timmers, 2021). Based on their updated framework, the authors discuss the capabilities, capacities and control of the EU and the Netherlands on each of these layers.

Okano-Heijmans (2023) proposes a 'Digital technology Stack' by adopting the model of *freedom lab* and adding an additional layer: the planet layer. The author argues that this extra layer can account for the planetary security and sustainability, and that this improves the usability of the model for determining actions. However, these elements are already explicitly included in the resource layer as defined by Crul (2022), which not only encompasses rare earth materials, but also specifically energy and an "economic, social and geopolitical dimension of the Stack" related to the use of space. The 'digital technology stack' is used to determine EU interest, concerns, instruments, tools, capabilities and assets on each of the layers, in light of digital strategic autonomy: "EU digital autonomy concerns the ability – as a global player, in cooperation with international partners, based on own insights and choices – to secure public interests in the digital domain and to be digitally resilient in an interconnected world" (Okano-Heijmans, 2023, p. 9). This definition is based on the definition of open strategic autonomy by the Dutch government and political in nature (Ministry of Foreign Affairs, 2022). This is also signalled by the Dutch governments use of the term digital *open* strategic autonomy (DOSA). 'Open' serves a rhetorical function signalling a policy direction. It refers to an open economy and an approach which can be summarized by "open where possible, protective where necessary" (Ministry of Foreign Affairs, 2022, p. 3). The Dutch government urges that, on an EU level, this openness in stressed. In practice, different interpretations of 'open' have led to confusion in policy debates (Timmers, 2021). The 'open' is often already captured by the 'strategic' aspect, which leaves room for different strategies as discussed in Section 3.2.2, for example via strategic interdependency (Moerel & Timmers, 2021).

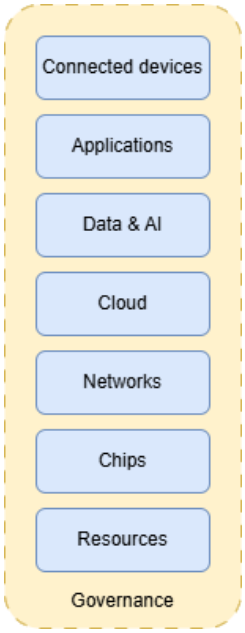
Van der Waal et al. (2021) from *Waag Futurelab* have introduced a 'public stack' framework (common values, open design process, open technology and citizens), which they distinguish from a private stack (market values, closed design process, closed technology, consumers) and a state stack (state values, closed design process, closed technology, [surveillance] subjects). Their idea of the public stack is inspired by Bratton (Lovink, 2020). Part of their framework is a technology stack, which they use to analyse technological choices and societal effects in different case studies. The proposed stack has five technology layers and four 'context layers'. Next to this, it has a foundational layer and a design process layer. Although Van der Waal et al. did not design the framework to specifically determine the digital strategic autonomy on different layers, they do mention digital sovereignty as one of the public values which can be analysed by the application of their framework.

Lastly, Kagerman et al. (2021) propose a ‘technology layer model’ to analyse different dimensions of digital strategic autonomy for Germany and the EU. They argue that their model “provides a more detailed breakdown than the usual distinction between microchips, hardware and software” (p. 8). For each of the layers, the authors identify the technologies that are deemed most relevant, feasible and require policy action.

4.2 Subconclusion: the working stack

Based on the comparison above, we synthesize the different findings in the stack presented in Figure 6. This is the ‘working stack’ for this thesis. This stack is a framework that enables the analysis of every layer for an organisation in terms of its capacities, capabilities and control: its digital strategic autonomy. The layers are in reality not strictly separated, but serve an analytical function. Furthermore, the layers are interdependent. A lack of digital strategic autonomy on a layer lower in the stack can therefore result in a lack of digital strategic autonomy on a layer higher in the stack.

Figure 6: Working Stack



The working stack is mainly based on Sheikh (2022) and Bria et al. (2025). Their division of seven layers strikes a balance between a framework that gets complicatedly large, e.g. the stack of Stolwijk et al. (2024) with twelve different layers, and a framework that is too small. Furthermore, the Eurostack report of Bria et al. has generated support from a variety of European businesses and both the German and French government, the former even mentioned it explicitly in the coalition agreement. Contrary to Bria et al., we positioned the connected devices layer at the top, adhering more the principle that the highest layer is closest to the end users.

We could zoom in on the digital strategic autonomy for each layer of the stack. Because of the limited scope of this thesis, we will focus on the cloud layer and its relation with the data & AI and applications layer. For an elaboration on other layers in light of digital strategic autonomy, see e.g. Ganz et al. (2024) on submarine cables and Aldrich & Karatzogianni (2020) on the same topic, explicitly using Bratton’s Stack as an analytical tool. Calderaro & Blumfelde (2022) discuss Artificial Intelligence and digital strategic autonomy.

The reason for our focus on the cloud layer is that a lack of digital strategic autonomy on this layer has an uniquely large influence on the digital strategic autonomy on the layers above.[6] It has been argued by Balayn and Gürses (2024) that computational infrastructures, which they view as the cloud and end devices (or in terms of our stack, connected devices), form the production environment for AI and applications. This means that the cloud not only enables its functioning, but also shapes its production. As such, a lack of capacities, capabilities and control directly shape the abilities on the other layers. Furthermore, as connected devices have become smaller in terms of capacity,

[6] Depending on the capacities, capabilities and control in this layer, the reverse may also be true. As one of the interviewees noted: *“I have never had so little vendor lock-in [and so much control]. I used to have my own data centres with VMware, Citrix – long term contracts. I can now move [my Azure zone] from Amsterdam to Frankfurt in 5 hours. […] So I've never been more flexible. It has mostly to do with automation, a little less with cloud. But cloud has made it much easier and faster to deploy and use automation. So I actually have the least vendor lock-in ever, because I'm not stuck with long-term contracts either. It's a lot of pay-as-you-go.”* (ENG-SSC).

applications, data storage and AI depends even more on the cloud for the provisioning an production hereof (Gürses & van Hoboken, 2018, p. 582). In the words of Bria et al. (2025):

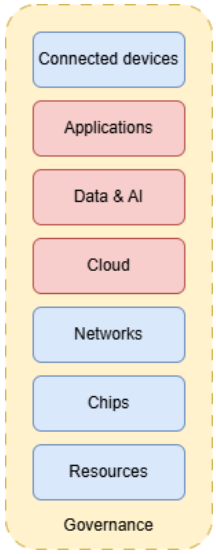
> "Cloud infrastructure has evolved far beyond its initial role as a tool for data storage or application hosting; it has become the critical backbone of the digital economy. Functioning as the "power grid" of this new economy, it provides a foundational production environment that transforms industries, public services, and operational models into tightly integrated ecosystems" (p. 65).

As we will show in Section 5.3, the majority of the EU cloud market (75-90%) is in hands of three large US cloud service providers and a significant lock-in effect is present. These unique characteristics of the cloud layer together raise significant concerns about the capabilities, capacities and controls of organizations on this layer, and form the justification of using this layer as our focal point.

5 Zooming in: the cloud layer

As explained in Section 4.2, we will now zoom in on the cloud, data & AI and applications layer, highlighted in Figure 7. In Section 5.1, we will first provide a technical definition of cloud computing. In Section 5.2, we show how the different cloud service models cover the different layers of the stack, and differ in their effect on digital strategic autonomy. Then, in Section 5.3. we highlight the dependence on US cloud service providers, both directly and indirectly as sub-vendors for other cloud service providers. In Section 5.4. we discuss the geopolitical dimension of digital strategic autonomy, referring to US jurisdiction and legislation impacting the confidentiality of data and availability of services. In Section 5.5. we discuss the public/private dimension of digital strategic autonomy, highlighting how dependencies on private cloud service providers for the provisioning of public services can diminish digital strategic autonomy. We conclude in Section 5.6.

Figure 7: Layers of the stack in scope



5.1 Technical definition of cloud computing

The US National Institute of Standards and Technology (NIST) defines cloud computing as:

> "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011, p. 2; Simmon, 2018, p. 2).

This has proven to be an influential definition, both in academia (see e.g. Lynn et al. (2021)) and in policy making (see e.g. the European Union's NIS 2 Directive[7] and the Dutch National Cloud Policy (Ministry of the Interior and Kingdom Relations, 2022)). NIST distinguishes five characteristics that are essential for cloud computing service. These are on-demand self-service, broad network access, resource pooling, rapid elasticity and measures service.

On-demand self-service refers to the ability of cloud service customers to automatically and one-sidedly provision cloud computing resources. Broad network access refers to computing resources being made available over a network with standard mechanisms, such as the internet, to devices ('clients') that vary in processing power. Note that this already shows the connection and dependency between the 'cloud' and 'connected devices' layers in the stack. Resource pooling means that a cloud service provider pools its resources, such as storage, processing and memory, and then assigns those dynamically to customers, based on the demand. This pooling dynamic creates "a sense of location independence" (Mell & Grance, 2011, p. 2), although customers are more and more able to determine the storage and processing location for some types of data at country- or regional level (Blancato & Carr, 2024). The fact that computing resources are can be provisioned and released quickly, based on demand, is called rapid elasticity. Lastly, cloud service providers monitor usage, and customers are often billed based on the used resources or the amount of accounts used.

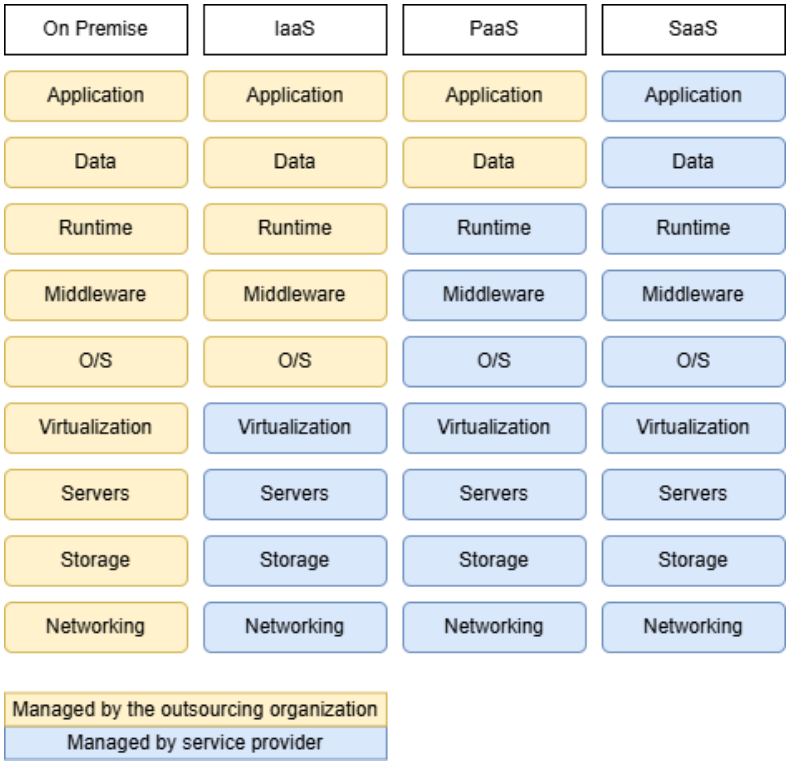
[7] Art. 6(1)(30) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ 2022, L 333).

This characteristic is referred to with measured service. The ISO-standard on cloud computing vocabulary adds another characteristic of cloud computing service, namely multi-tenancy (International Organization for Standardization, 2023). This refers to the fact that computing resources are used by multiple customers, but the data an computations are separated between customers and inaccessible to each other.

5.2 Cloud service models

NIST distinguishes three types of cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) (Mell & Grance, 2011; Simmon, 2018). Figure 8 shows the stacks layers for the different cloud service models and whether it's managed by the outsourcing organization or by the service provider. Note that 'manages' does not equate 'control'. For example, in the case of IaaS the outsourcing organisation manages the data that is stored on the infrastructure of the service provider, but the service provider can, depending on the technical measures such as encryption, have access to the metadata or content data.

Figure 8: Different cloud service models



The above is a comparison of 'ideal types' of main cloud service models and service the purpose of comparing different cloud service with each other. In its evaluation of these models, NIST observes the use of "aaS" (as a Service) as a suffix often used for marketing purposes since the introduction of their cloud definition. This "is confusing, and (unintentionally) obfuscate[es] the architecturally well-founded distinction of [SaaS, PaaS and IaaS]" (Simmon, 2018, p. 1). Other authors have observed and analysed this shift as well (Duan et al., 2015).

In practice, however, cloud service offerings change rapidly. Therefore, Hubert (2025a, 2025b) has proposed a 'cloud ladder' based on talks with industry experts and policy makers, see

Table 1. The steps of the ladder are based on the level of outsourcing to a service provider, the control that the outsourcing organisation keeps and control the outsourcing organisation has over the future (planning and cost). As such, his distinction is more empirically based compared to the more theoretical and technical cloud service model types distinguished by NIST. 'Cloud native' refers to the ability to automatically configure and activate a service.

Table 1: Cloud ladder (Hubert, 2025)

Nr.	Ladder step	Explanation	NIST category
1	No Cloud	This is the same as on-premise	
2	Renting Servers	The organisation rents virtual servers from the service provider	IaaS
3	Renting Capacity	The organisation rents capacity from the service provider. This includes container-based deployments and Infrastructure as Code (IaC)	IaaS
4	Cloud native (limited features)	The organisation also uses limited and relatively basic cloud services for its own software, such as databases or identity & access management	PaaS
5	Fully cloud native	The organisation uses more complicated services, such as globally available databases, AI services or video streaming	PaaS
6	Software as a Service	The organisation uses software from a service provider which is delivered entirely as a service. All infrastructure, platform, and operational management responsibilities are handled by the service provider	SaaS

As an organisation moves higher up the ladder, it (i) has less direct control, (ii) depends more on the provider('s specific services), (iv) needs to perform less technical work (v) requires less technical knowledge. Therefore, any analysis of cloud use depends on the specific *type* of cloud use. It can be easier to migrate between IaaS-providers than it is to migrate between PaaS- or SaaS-providers because of the reasons above.

5.3 The Dutch and EU cloud market

The Dutch Authority Consumers and Markets (Autoriteit Consument en Markt, 2022) has performed market research into the EU and Dutch cloud services market. Both markets are dominated by three large US cloud service providers, often referred to as hyperscalers. In the EU, Amazon Web Services has a market share of 35-40%, Microsoft Azure 35%-40% and Google Cloud Platforrm 5%-10%. These shares are similar in the Netherlands, with a bigger share for Microsoft Azure. According to the ACM, this is because the Netherlands is a 'relatively Microsoft-oriented country' (Autoriteit Consument en Markt, 2022, p. 37; Hubert, 2024). The ACM did not receive specific enough data to distinguish between IaaS, PaaS and SaaS market share.

The ACM did investigate the amount of services that cloud service providers and third parties offered on their marketplace in 2022. For AWS, this was 408 own products and 12183 from third parties. For Azure this was 304 and 17742 and for GCP this was 92 and 6184. These services are

dependent on the infrastructure of the cloud service provider. The more services an organisation uses, the higher it is on the cloud ladder presented in the previous section.

A characteristic of the cloud markets is the *lock-in* effect. This refers to situations where organisations cannot easily switch to a different cloud service provider, because of financial, legal or technical reasons (Opara-Martins, 2017). In terms of technical reasons, the ACM argues that processes are often intertwined with IT-systems. Switching therefore requires a changing of these processes, which requires time and knowledge of implementing and maintaining the new cloud service. Furthermore, and in line with the steps in the cloud ladder described in the previous section, specific cloud service provider services hinder switching. Although another provider might provide a similar service in terms of its purposes or functionalities, these are technically different. Organisations would have to investigate and integrate these new services. Another technical difficulty is data portability, where data cannot easily be transferred between cloud service providers. The ACM indicates that the less standardised a cloud service offering is, the harder data portability is.

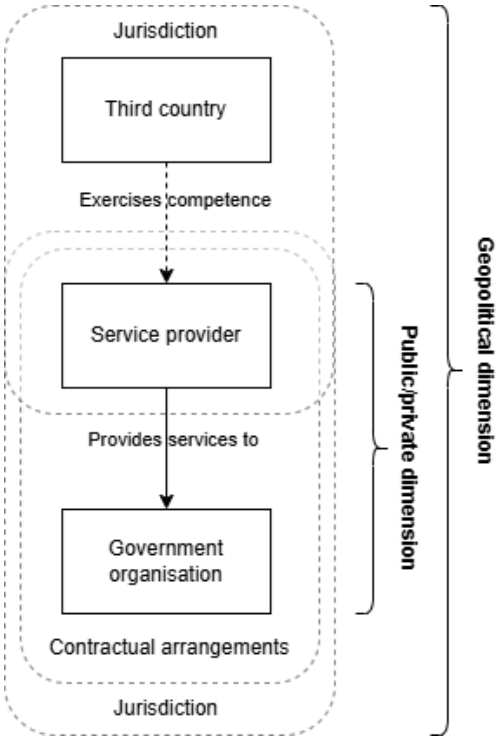
Next to technical reasons, the ACM describes financial difficulties in migrating.[8] These exist in the form of egress fees – the cost cloud service providers charge to transfer data to another cloud service provider. These costs are often complex, making it difficult to predict the cost of migration. These lock-in effects are harmful, because it 'makes it possible for companies to offer higher prices or lower quality without losing customers' (Autoriteit Consument en Markt, 2022, p. 64). Therefore, it leads to less control for organizations using these cloud services and diminishes their digital strategic autonomy.

5.4 The geopolitical dimension

This section focuses on the lack of digital strategic autonomy as a result of the US claiming jurisdiction over US cloud service providers, which diminishes control. In short: the geopolitical dimension. The amount of control is, however, also influenced by the direct relationship between the government organization and the cloud service provider: the public/private dimension. These two dimensions are depicted in Figure 9. The public/private dimension is discussed in the next section.

[8] Which originate directly from the switching providers. Indirect financial costs (retraining or hiring of employees, transaction costs in terms of investigating service offerings) also exist.

Figure 9: The geopolitical and the public/private dimension



In the cloud, data & AI, and application layers, a lack of digital strategic autonomy exposes organizations to third-country jurisdictional risks, which manifest as two distinct threat types: breaches of (meta)data confidentiality and disruptions to data and service availability (Michels et al., 2023; Blancato & Carr, 2024; Michels et al., 2025).[9] US cloud services, which provide network access to computing resources, can be seen as central nodes in a global network. Farrell and Newman (2019) argue that:

> "states with political authority over the central nodes in the international networked structures through which money, goods, and information travel are uniquely positioned to impose costs on others. If they have appropriate domestic institutions, they can weaponize networks to gather information or choke off economic and information flows, discover and exploit vulnerabilities, compel policy change, and deter unwanted actions" (p. 45).

The authors describe two strategies countries can use to weaponize the existing interdependence: the *panopticon* and the *chokepoint* effect. Both effects are enabled by the claimed political authority, i.e. jurisdiction, of third countries over these cloud service providers.[10] Michels et al. (2025) also draw this connection, but their further analysis focuses merely on the use of US hyperscalers by EU customers in the private sector.[11]

The panopticon effect, named after Bentham's architectural concept where few actors observe many, enables states to leverage network centrality for surveillance purposes. This mechanism allows states with jurisdiction over hub nodes to extract information. In practice, this

[9] This distinction indicates a link between digital strategic autonomy and information security, as it aligns with two core components of the well-known CIA triad: confidentiality and availability.

[10] Here we assume a functioning rule of law. Both strategies could also be employed by governments outside of the rule of law, as long as they have authority over cloud service providers and the institutions to weaponize the panopticon and chokepoint effects.

[11] They note: *"Many of the same concerns arise with (and often apply more strongly to) public sector use of US hyperscalers. However, organisations in the public sector can face additional constraints, including whether their use of cloud is consistent with the principles of good public administration, such as transparency, accountability, and oversight"* (Michels et al., 2025, p. 9)

manifests as the capacity to monitor communications, analyse (meta)data, and intercept data traversing these central nodes. The visibility afforded by this position creates an "informational advantage in understanding adversaries' intentions and tactics" (Farrell & Newman, 2019, p. 55) that proves strategically valuable in international relations. The risk that the US is interested in (government) data from its allies and willing to use its power is not imaginary, as the Wikileaks revelations showed. The NSA has previously wiretapped two French ministers of Finance between 2011 and 2014 (Reuters, 2015a) and 125 German government officials, including the chancellor, for decades (Reuters, 2015b).

The chokepoint effect refers to the ability to deny or restrict access to these same central nodes, i.e. cloud services. As Farrell and Newman (2019) elaborate: "because hubs offer extraordinary efficiency benefits, and because it is extremely difficult to circumvent them, states that can control hubs have considerable coercive power and states or other actors that are denied access to hubs can suffer substantial consequences" (p. 56). This effect enables states to exclude targeted entities from network participation and to use exclusion as a threat to put pressure on targeted entities for other purposes.

Table 2 provides an overview of the argument we will make next in, namely that the United States can and does already apply the panopticon and chokepoint effect via its (personal) jurisdiction over US cloud service providers and its legislation, regardless of where the services are provisioned and the data is stored. This effects the confidentiality and availability of (data processed in) cloud services and applications. It is important to note that we focus on current legal powers of the US to illustrate the panopticon effects and the chokepoint effect. These could change in the future.

Table 2: The panopticon and chokepoint effect and US cloud services

Asset element	Threat mechanism	Threat scenario
Confidentiality	Panopticon effect	US uses intelligence powers (e.g. FISA Section 702)
		US uses law enforcement powers (e.g. the CLOUD Act)
Availability	Chokepoint effect	US orders service provider to change availability of services (e.g. by imposing sanctions)

Many of the respondents perceive a higher risk, i.e. an increased likelihood of the threats materializing, because the geopolitical situation has changed, particularly since the Trump administration (POL-NAT, POL-MUN, COM, ENG-SCC, GOV-VNG-2, GOV-VNG-3). All respondents have mentioned third-country jurisdiction, specifically from the US, as a threat to digital strategic autonomy.

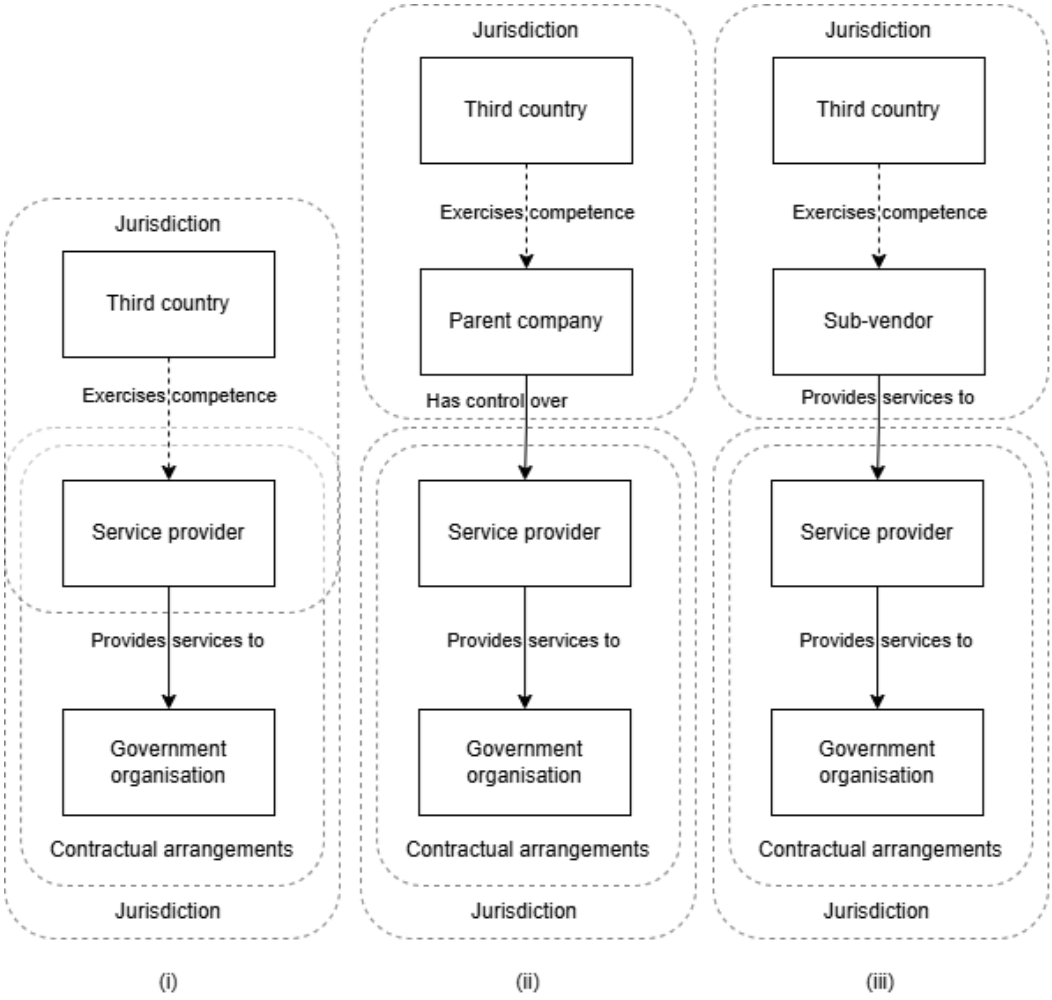
5.4.1 US jurisdiction and relevant legislation[12]

The US claims jurisdiction over US legal entities, over any foreign entity with sufficient contacts with the US and over foreign entities with a branch in the US (Ramos et al., 2022). This is a "longstanding US principle" (Abraha, 2020), also called 'personal jurisdiction'. Indeed, the US Department of Justice states: *"US jurisdiction is not limited to US corporations, US headquartered companies, or companies owned by US persons"* (U.S. Department of Justice, 2019, p. 17). It highly depends on the specific facts of a case whether an EU entity has sufficient contacts with the US and is subject to its jurisdiction, which is determined by i.a. the nature, quantity and quality of the contacts (Abraha, 2020).

[12] The sections 5.4.1-5.4.2 partly draw on earlier work from the author (Van der Wal, 2024).

Figure 10 shows the possible interplay between foreign jurisdiction, (cloud) service providers and their parent company and/or sub-vendors. More specifically, it shows how the US can use its legislation to demand data or a change in cloud service availability from (i) a service provider directly, when it is a subsidiary from a US company or meets the sufficient contacts test for establishing personal jurisdiction, (ii) from the US parent company which has control over the service provider or (iii) from a sub-vendor used by an EU entity.

Figure 10: Cloud service providers and foreign jurisdiction



The contract between a cloud service provider and a government organisation cannot fully mitigate the risk as a result of US jurisdiction applying, because this only binds the parties to the contract (Irion, 2012). As van Hoboken et (2013) al write:

> "Contractual obligations on cloud providers to resist requests with all legal means or to be as transparent as possible do have some value. But ultimately, the impossibility to build a trust relationship about access to data by governmental agencies between cloud customer and provider is exactly the problem for potential cloud customers that worry about access to their data abroad" (p.14).

In conclusion, the US claims jurisdiction over US cloud service providers (and their subsidiaries), regardless of where the processing takes place and data is stored.[13] The next sections explain how this jurisdiction together with legal competences is (or can be) used by the US and threatens the confidentiality and availability of cloud services

5.4.2 Confidentiality: FISA Section 702 and the CLOUD Act

The US can use two types of legislation to compel cloud service providers to disclose data under their control, thereby threatening the confidentiality of data. Namely laws relating to national security and laws relating to law enforcement (van Hoboken et al., 2013; Michels et al., 2023, 2025).

An example of a law relating to national security is FISA Section 702[14], which allows the authorized targeting of non-US persons with the goal of obtaining foreign intelligence information.[15] On 19 April 2024, the US Senate extended thit Section for another two years after serious debate (Foran & Barrett, 2024).[16] The US is very much aware of their informational advantage due to US cloud service providers being dominant, an example of the panopticon effect. In an evaluation of FISA Section 702, the President's Intelligence Advisory Board and Intelligence Oversight Board (2023) stated:

> "As a world leader in telecommunications, U.S. telecommunications services are ubiquitous, and the intelligence community can leverage this national advantage to collect foreign intelligence information by lawful, court-approved methods in order to protect America from its adversaries and support foreign policy decisions that help advance America's standing in the world." (p. 3).

FISA Section 702 allows the National Security Agency (NSA) to direct US cloud service providers[17] to provide them with all 'information, facilities, or assistance' needed on an authorized target.[18] This can be both content data and meta-data. The cloud service provider is still allowed to encrypt data as part of its regular service provisioning, but has to produce the key if it is under its possession, custody or control, and otherwise has to produce the encrypted data to the NSA (Rosenthal, 2025). If a cloud service provider does not comply with the directive, the Attorney General can request the Foreign Intelligence Surveillance Court to order the cloud service provider to do so.[19] A failure to comply with such an order can be punished as contempt of court.[20] The NSA uses its FISA Section 702 powers on behalf of itself and on CIA or FBI requests.[21]

Cloud service providers have to do comply with the directive or court order in a way that protects the secrecy of the order and with a minimum of service interference.[22] Therefore, cloud service providers cannot inform their customers. They are allowed to publish semi-annual reports on

---

[13] The US also asserts personal jurisdiction over its nationals. This enables another way the US can exercise authority over a central node, namely via a subpoena to a US national who holds or controls data abroad. This way, the US can even obtain data from foreign entities over which it does not have jurisdiction. We will not elaborate on this further, see on this point Ramos et al. (2022, pp. 10–12).

[14] 50 U.S.C. § 1881 et seq.

[15] Foreign intelligence information includes data relating to the ability of the US to protect itself from foreign threats such as terrorism, espionage, weapons proliferation, drug trafficking and hostile acts by foreign powers. It also encompasses information about foreign powers or territories related to US national defense, security, or foreign affairs. When involving U.S. persons, the information must not only be relevant, but necessary for these purposes. For the exact definition, see 50 U.S.C. 1801(e).

[16] Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, 138 Stat. 862 (2024).

[17] US cloud service providers fall under the broad term 'electronic communication service prover', as defined in 50 U.S.C. § 1881(b)(4).

[18] 50 U.S.C. § 1881a(i)(1)(A).

[19] 50 U.S.C. § 1881a(i)(5)(A).

[20] 50 U.S.C. § 1881a(i)(5)(E).

[21] 50 U.S.C. § 1881e(a)(1) jo. 1806.

[22] 50 U.S.C. § 1881a(i)(1)(A).

the amount of FISA orders and targeted accounts, but only in bands of 1000 or 500.[23] As one expert interviewed by Michels (2025b) put it:

> "Microsoft, AWS and Google, they say: 'we don't receive a lot of requests'. The reality is we don't know, 'cause they're not allowed to tell us. You could say, well, that's just a theoretical risk, but whether it has been realised or not, we have no way of knowing." (p. 10)

An example of a law relating to law enforcement is the Clarifying Lawful Overseas Use of Data Act (CLOUD Act),[24] which amended the Stored Communications Act.[25] Reading the paragraph that the CLOUD Act added clearly shows how this law applies to all data within a cloud service provider's 'possession, custody, or control' that is under its jurisdiction, regardless of the location of the data:

> "A provider of electronic communication service or remote computing service[26] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[27]

In the words of Abraha (2020, p. 32): "US-based service providers cannot escape the reach of US authorities by merely moving data out of the country". The SCA bypasses the traditional Mutual Legal Assistance Treaties (MLAT) between countries, which have been deemed to slow in the context of criminal investigations (Blancato, 2024). The EU Data Protection Advisors have argued that this circumvention of treaties interferes with "the territorial sovereignty of an EU member state" (Article 29 Working Party, 2017a, p. 28).

A US law enforcement agency has to show to a court that reasonable grounds exist to believe that the content data sought is relevant to an ongoing criminal investigation in order to obtain a court order,[28] or show probable cause that a crime has occurred and that data can contain evidence to obtain a warrant.[29] US law enforcement agencies can also request non-content and meta-data on e.g. a customer's name, address, IP-number and service use based on an administrative subpoena.[30] It does not have to demonstrate probable cause for doing so (Brier, 2017).

The CLOUD Act applies to all content within the 'possession, custody, or control' of a cloud service provider. This is not further defined in the CLOUD Act. Possession and custody refer to the physical possession of content, but the test for 'control' is more ambiguous, especially with a US parent company and a subsidiary. Two types of tests can be distinguished in this regard: the test whether the subject of the order has legal right (with regards to the corporate structure) to obtain the content (legal control), or the test whether the subject has the practical ability to do so as part of the day-to-day operations (*de facto* control) (Hemmings et al., 2020). This analysis depends highly on the specific facts of a case, "so no hard-and-fast rules can be drawn from the case law" (Ridgway, 2018; see also Ramos et al., 2022). US Courts have previously applied both tests in different cases. (Abraha, 2020; Hemmings et al., 2020).

---

[23] 50 U.S.C. § 1874(a)(1). Some other reporting options with lower bands are allowed, but only if the number communicates more aggregated information or if the reporting is done annually.
[24] 18 U.S.C § 2713.
[25] 18 U.S.C § 2701 et seq.
[26] This is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system" in 18 U.S.C. § 2711(2). Section 5.1 shows that cloud computing services fall within this definition, and they also qualify as an electronic communication service (Ramos et al., 2022).
[27] 18 U.S.C § 2713, emphasis added by the author.
[28] 18 U.S.C. § 2703(d).
[29] 18 U.S.C. § 2703(a).
[30] 18 U.S.C. § 2703(c). This is also possible via a court order or a warrant.

Ramos et al. (2022) state that the CLOUD Act is “encryption-neutral”, and does not prohibit encryption of data.[31] The court could however order to provide the key alongside encrypted data, but only when the key itself is under its possession, custody or control. Therefore, encrypting the data without being in possession of the key to decrypt the data could prevent a court from establishing that the cloud service provider has ‘control’ over data relevant to the investigation (Ramos et al., 2022; European Data Protection Supervisor, 2024, para. 427). We discuss encryption further in Section 7.7.

A US law enforcement agency can request a court to prohibit a cloud service provider from notifying any other person, including the customer or the target, of the existence of a warrant, subpoena or court order.[32] This is also called a ‘gag order’. Microsoft has previously objected to the ‘overuse’ of these orders: “They are often approved even for routine investigations without any meaningful analysis of either the need for secrecy or the orders’ compliance with fundamental constitutional rights.” (Burt, 2021)

An analysis of the transparency reports of cloud service providers, which i.a. show the amount of request based on the CLOUD Act, resulted in the conclusion that “it is fair to conclude that the risk of disclosure of EU residents’ personal data or other data under the CLOUD Act is low” (Jongen et al., 2022, p. 3).

Both laws diminish the control that organizations have over their data stored in the cloud, and therefore diminish their digital strategic autonomy. But comparing the two legal powers above, we see that the scope of FISA 702 is much broader in terms of types of data, namely the broadly defined ‘foreign intelligence information’ as opposed to the CLOUD Act, which requires a US Law enforcement agency to show to the court probable cause in relation to a specific criminal investigation over which it has jurisdiction.

Multiple authors have observed that policymakers regularly miss the distinction between these two regimes in the context of governmental access to cloud services. Already in 2013, van Hoboken et. al write: *“In the context of cloud computing surveillance, however, policymakers seem to systematically confuse intelligence and law enforcement practices”* (p. 14). Michels (2025a) observes how the Netherlands Court of Audit (2025) in a recent report on the cloud use of the Dutch central government also overlooked this difference.

5.4.3 Availability: US Sanctions

Michels et al. (2025) note that “unlike the panopticon effect discussed above, we are not aware of any existing legal power that would allow the US government to cut European customers off from US cloud services” (p. 15). A comprehensive analysis of the powers exercised by the U.S. government in this context falls outside the scope of this thesis. However, the United States has asserted its jurisdiction to restrict customers' access to US based cloud services in several instances.

The regulator of the Dutch banking sector, De Nederlandsche Bank (DNB), has previously warned for the availability risks as a result of outsourcing cloud services among Dutch banks (Monterie, 2024). The DNB referred to the Dutch branch of a Russian bank that went bankrupt as a result of the discontinuation of their US cloud services:

> “After the Russian invasion of Ukraine and subsequent sanctions, Microsoft was no longer allowed to serve that company. The ATB was highly dependent on Microsoft for its communications. As a result, the bank went bankrupt, although it still had plenty of money.” (Koning, 2024)

---

[31] See also 18 USC. § 2523(b)(3).
[32] 18 U.S.C. § 2705(b).

The Russian bank was put on a EU-sanction list, but the Dutch branch was not. The US did however put the Dutch branch on their national sanction list, as a result of which all US companies were obliged to stop its service delivery. Microsoft notified the Dutch branch 3 days after it was added to the US sanction list and closed it off from all its services 3 days later.[33] After the bankruptcy, Microsoft refused to provide the curators with access to the account of the Dutch bank, which was needed to access the administration. Because of this, they started proceedings at the Dutch court. The court stated that Microsoft was only guided by its own interests:

> "The trustees are dealing with a large and powerful American party that wants to avoid at all costs any risk that it might run worldwide as a result of the sanctions, however small, and is guided only by its own interests. In the run-up to these summary proceedings (the lawyer of) Microsoft played hide-and-seek by not disclosing which Microsoft company had to be subpoenaed and by not yet wanting to reveal anything of its defence."[34]

The court concluded that it would be unlikely that providing the curators access to the Microsoft environment would act against the spirit or reasoning behind the sanctions. Nor did the court found it likely that Microsoft would face any significant criminal or financial risks by complying with the request.

The second example is the discontinuation of Microsoft cloud services to Karim Khan, the prosecutor of the International Criminal Court (ICC). The ICC is an intergovernmental organization and international tribunal located in The Netherlands. It is established by the Rome Statute, a treaty to which 125 states are a party. The ICC has jurisdiction with respect to the crime of genocide, crimes against humanity, war crimes and the crime of aggression.[35] On February 6th 2025, the US imposed sanctions on the ICC Khan via Executive Order (EO) 14203, arguing that the ICC had no legitimate basis to assert jurisdiction over and open preliminary investigations into US or Israeli personnel and to issue arrest warrants against the Israeli Prime Minister and former Minister of Defense.[36]

The EO mandates all United States persons to block and freeze all properties and assets of persons on the sanction list that are within their possession or under their control.[37] Furthermore, United States persons are prohibited to provide funds, goods or services that benefit any person on the sanction list.[38] A United States person comprises both individuals and entities,[39] and includes foreign branches and subsidiaries of US companies and their employees.[40] This is therefore another clear example of personal jurisdiction.

The Executive Order contains a provision to add other non-US persons to the sanction list in the future, when they i.a. "have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of [ICC investigations into protected persons as defined by the EO]".[41]

The EO is based on multiple United States laws, among which the International Emergency Economic Powers Act (IEEPA).[42] This Act determines that "It shall be unlawful for a person to violate,

---

[33] District Court of Amsterdam, 3 May 2022, ECLI:NL:RBAMS:2022:4452, 2.2-2.3.
[34] District Court of Amsterdam, 3 May 2022, ECLI:NL:RBAMS:2022:4452, 4.3.
[35] Rome Statute of the International Criminal Court, July 17 1998, 2187 *UNTS* 90, article 5.
[36] Executive Order No. 14203, "Imposing Sanctions on the International Criminal Court", February 6th 2025, *90 Fed. Reg.* 10195, available at https://www.govinfo.gov/content/pkg/FR-2025-02-12/html/2025-02637-2.htm. This EO fits within a longer trend of US hostility towards the ICC (Galbraith, 2025).
[37] EO 14203 Section 1(a)(i) jo. Annex.
[38] EO 14203 Section 3(a).
[39] EO 14203 Section 8(a).
[40] EO 14203 Section 8(c).
[41] EO 14203 Section 1(a)(ii)(A-C). On June 5th, the US Department of State (2025) added four ICC judges to the sanction list based on Section 1(a)(ii)(A).
[42] 50 U.S.C. § 1701 et seq.

attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter".[43] The EO is such an order. A civic penalty can be imposed to any person that commits such an unlawful act.[44] A criminal penalty can be imposed to any person that "wilfully commits, wilfully attempts to commit, or wilfully conspires to commit, or aids or abets in the commission of, an unlawful act".[45] Natural persons can also be imprisoned for up to 20 years. Therefore, committing an act prohibited by US sanctions can have severe consequences for US persons, both companies and individuals alike.

As a result of these sanction, according to Associated Press, "Microsoft […] cancelled Khan's email address, forcing the prosecutor to move to Proton Mail, a Swiss email provider, ICC staffers said" (Quell, 2025). In terms of the EO: Microsoft, as a United States person (or as its foreign branch) has stopped providing its services to Khan, the person on the sanction list. ICC staff has indicated that because of the sanctions, the ICC cannot hardly conduct its basic tasks anymore.

In a response to the Dutch magazine *iBestuur*, Microsoft stated that it indeed discontinued its services to Khan: "Since February, we have been in contact with the International Criminal Court (ICC) throughout the process and remained in constant dialogue. This eventually led to the disconnection of a sanctioned officer from Microsoft services" (Trigt, 2025; see also Satariano & Smialek, 2025). Microsoft states it did not pause or discontinue any services to the ICC *organization*. However, the US could in the future add other ICC staff to the sanction list, or impose sanctions to the ICC as an organisation (Kersten, 2025). Furthermore, the sanctions can have effect beyond their legal implications in a strict sense,[46] as was also apparent in the bank case discussed above:

> "the mere fact [of the] sanctions existence and potential to add sanctioned persons might, with time, exhort enough pressure and/or panic on companies such as Microsoft for them to proactively remove themselves from the court." (Thorne, 2025)

5.5 The public/private dimension

The public/private dimension of digital strategic autonomy captures the concerns of the increasing reliance on large private actors, driven by private values, for public service provisioning. This is especially true in the cloud domain, where three US private companies dominate the market (Section 5.3) and where cloud services shape and determine the layers above it in the stack (Section 4.2 and introduction Section 5). Schaake (2024) characterizes the growing dominance of major technology corporations, particularly cloud service providers, within government, democratic institutions, and society at large as 'The Tech Coup', a term that also serves as the title of her book.

Sharon and Gellert (2024) have coined the term 'sphere transgression', which describes how big tech companies inappropriately cross the boundaries between different societal domains, often consolidating power in ways that challenge traditional norms of justice and governance:

> "As the ongoing digitalisation of societal sectors increasingly requires a computational infrastructure to run properly, this may lead to a deep dependence of public sectors on these [private Big Tech] firms for their main task, the provision of public services and goods. Yet, these actors are not held accountable to serving the public interest in the way that public actors are, nor are they upheld to public scrutiny in ways that enable redress." (p. 2657)

---

[43] 50 U.S.C. § 1705(a).

[44] 50 U.S.C. § 1705(b), the amount cannot exceed the greater of $250,000 or *"an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed"*.

[45] 50 U.S.C. § 1705(c), the amount cannot exceed $1,000,000.

[46] This is also called overcompliance (Human Rights First, 2025).

Bozeman and Bretschneider (1994) distinguish between a “core approach” to publicness, where an organization’s public character is determined solely by its legal form (government vs. private ownership) and a “dimensional approach”, which sees publicness and its converse, privateness, as degrees defined by the extent to which an organization is subject to external authority: political authority imposing public values (e.g., accountability, transparency, human rights) or economic authority imposing private values (e.g., profit maximization). We adopt the dimensional approach because it accommodates the nuance that private actors can uphold public values so long as sufficient public control exists, a perspective likewise embraced by Van Dijck et al. (2016, pp. 13–14) in their study of platforms and public values.

A lack of control over a cloud service provider does therefore impact the publicness of public tasks performed by a government organisation and diminishes its digital strategic autonomy, and more fundamentally threatens public values (Passchier, 2021).[47] We will illustrate this with two concrete examples, where the SaaS-model exemplifies how technological architecture can shift the balance from political to economic authority, and therefore from publicness to privateness, as cloud service providers maintain unilateral control over software updates and feature implementations.

Microsoft Teams, a form of cloud (SaaS) is widely used by government organizations for their internal communication.[48] Recently, Microsoft automatically enabled voice and face recognition for all Microsoft Teams users (Microsoft, 2025b). Microsoft’s ability to enforce this change stems from the SaaS model’s architecture, which allows providers to push continuous updates at will. Although Microsoft announced the feature on its roadmap, it rolled it out on an opt-out basis rather than requiring (user) consent. The New South Wales education department only discovered this functionality after a month to their great dissatisfaction (Taylor, 2025). (Other) generative AI functionalities are also turned on automatically (Hubert, 2024; Speed, 2025; Warren, 2024). Government organisations can often (with difficulty) disable these functionalities, but large cloud service providers automatically and one-sidedly introduces these functionalities in public processes.

Another example illustrates how software providers push organisations towards adopting SaaS. In terms of the stack, the result of this push is that the service provider controls the data & AI and cloud layers below the application layer in the stack, thereby exercising more control. In October 2025, Microsoft will discontinue all its technical support (bug fixes and (security) updates) for its on-premise mail server software Exchange Server 2016 and Exchange Server 2019.

Microsoft has announced two solutions for customers: either migrate (or update) to Exchange Server Subscription Edition (SE)[49] which becomes available in July 2025, or to Exchange Online, which is the SaaS-version of Exchange. The price for on-premise Exchange Server products will increase with 10-20% compared to the 2016 and 2019 versions, while the price for Exchange Online stays the same (Carlson, 2025), strongly nudging customers towards the cloud/SaaS solution (Hubert, 2025c). The shift to SaaS allows Microsoft to further integrate its email services with other cloud service offerings (Czerwonka, 2024). As the company writes:

> “We strongly believe that you get the best value and user experience by migrating fully to Exchange Online or Microsoft 365. Migrating to the cloud is the best and simplest option to

[47] As stated in Section 3.1, the question whether this control by governments itself is legitimate and sufficiently transparent and accountable is important, but out of scope.

[48] And sometimes external communications, you can e.g. report crimes to a Dutch police department via Microsoft Teams (Politie Noord-Holland, 2024).

[49] The ‘Subscription Edition’ refers to the fact that the licensing model changes from perpetual (as was the case with the 2016 and 2019 versions) to an annual license. As such, from the perspective of customers, this shifts expenses from capital expenses (capex) to operational expenses (opex). A customer also needs to maintain a Software Assurance (SA) next to his SE license to keep his usage rights and have access to updates. As Microsoft writes: “If you *don't* buy cloud subscription licenses, then Server licenses and CALs you buy *must have* Software Assurance” (The Exchange Team, 2024).

help you retire your Exchange Server deployment. When you migrate to the Microsoft cloud, you make a single hop away from an on-premises deployment and benefit from new features and technologies, including advanced generative AI technologies that are available in the cloud but not on-premises" (The Exchange Team, 2025).

Importantly, migrating from self-hosted or EU-hosted solutions to a US based SaaS model pulls service provisioning into the geopolitical dimension of digital strategic autonomy by subjecting it to foreign jurisdiction. In the case of Exchange Online, US legislation directly threatens email confidentiality and availability (see Section 5.4.2).

5.6 Subconclusion

This chapter provided an overview of cloud computing, discussing its technical functioning and exploring different cloud service models which covered the cloud, data & AI and application stack layers. US hyperscalers are highly dominant on the Dutch and EU cloud market, either as SaaS-providers themselves or sub-vendors for other SaaS-providers. The specific type of cloud used impacts the level of control of an organisation. As an organization uses functions specific to the cloud service provider, it has less direct control, depends more on these provider('s specific services), and requires less technical knowledge and expertise, leading to fewer in-house capacities and capabilities. The geopolitical dimension to digital strategic autonomy highlights the lack of control as a result of foreign jurisdiction over de cloud service provider, i.e. US jurisdiction. With legislation such as FISA Section 702 and sanctions, a foreign country can impact the confidentiality and availability of clouds service used for public service provisioning. We refer to this as respectively the panopticon and the chokepoint effect. The public/private dimension highlights how a lack of digital strategic autonomy leads to private values, determined by economic authority instead of political authority, impacting public processes. This clearly shows the risk of a lack of digital strategic autonomy for government organizations in the cloud, data & AI and application layers of the stack.

6 A self-assessment tool for municipalities

With a conceptualization of digital strategic autonomy and an identification of indicators thereof in the cloud, data & AI and application layers, we will now develop a self-assessment tool for municipalities. To do so, we first introduce the municipalities and the Vereniging van Nederlandse Gemeenten (VNG). Then we zoom in on the current cloud use of Dutch municipalities. We then identify requirements for the self-assessment tool, compare similar tools and present the developed tool.

6.1 Dutch municipalities

Presently (summer 2025), the Netherlands has 342 unique different municipalities, varying widely in size and population. Municipalities are the third level of government in the decentralised unitary state, after the central government (Rijksoverheid) and the provinces. As such, they are the body of government closest to citizens (Vereniging van Nederlandse Gemeenten, 2017).

Municipalities have different tasks and responsibilities, based on autonomy or on co-governance (Broeksteeg, 2021). The autonomous tasks and responsibilities are laid down in the *Gemeentewet* (Municipalities Act).[50] Examples are their responsibility for public order and safety, housing and the autonomy they have to provide subsidies. Municipalities are also responsible for implementing national laws, called co-governance (medebewind).[51] Examples are laws in the social domain. In 2015, the national government introduced three 'unprecedented' major decentralizations in this domain, namely *Wet maatschappelijke ondersteuning,* the *Participatiewet* and the *Jeugdwet* (Social Support Act, Participation Act and Youth Act) (Broeksteeg, 2021). Because of this (increased) decentralization, and the freedom of municipalities regarding the implementation, larger differences between municipalities exist, which has been met with criticism (Elzinga, 2023; Vonk, 2016). This, in turn, leads to larger differences in processes and IT-systems between different municipalities.

6.1.1 Vereniging van Nederlandse Gemeenten

All Dutch municipalities are a member of the Vereniging van Nederlandse Gemeenten (VNG, *Association of Dutch Muncipalities*).[52] The VNG has formulated three pillars. Firstly, the VNG supports knowledge sharing between municipalities. Secondly, the VNG represents the interests of municipalities vis-à-vis the central government. Thirdly, the VNG focuses on service provision, where the VNG supports municipalities in implementing legislation. In total, the association employs around 300 FTE's (Vereniging van Nederlandse Gemeenten, 2024b).

Although the VNG has an important role in representing municipalities, it is not a governing body. It is a private-law legal entity without public authority (Jak, 2011; Peters, 2011). The main reason for this is that the VNG does not have a ground in public law to determine the legal status of other legal persons. Therefore, "it should be noted that VNG is and remains an ordinary association, even though it only possesses public-law legal persons as members and all kinds of association bodies are composed of (members of) municipal administrative bodies" (Peters, 2011, Section 2).

---

[50] Article 124(1) of the Dutch Constitution formulates a constitutional freedom for the administration of municipalities (and provinces) to 'regulate and administer their households'.
[51] Article 124(2) of the Dutch Constitution.
[52] This is not mandated by law/

This has certain implications, such as that legislation around transparency of government and the freedom of information, i.e. the *Wet open overheid*, is in principle not applicable to the VNG. Furthermore, the VNG cannot, by its statutes, legally bind its members to the agreements it makes with the central government. The VNG does however concludes governance agreements with the central government. These agreements are political rather than legal in nature. As Zijlstra (2019) notes:

> "Actually, one cannot speak of "governments" because they [governance agreements] are concluded with VNG […], interest groups of municipalities […] that often do not have power of representation. One can (therefore) also question the agreement character of administrative agreements, which often have to be regarded as political administrative declarations of intent." (Section 106)

The VNG has a general assembly, which is the supreme body of the VNG. In the assembly, a representative of a municipality can vote.[53] With a majority of the votes, the VNG can incur obligations at members' expense. Members are obliged to implement and comply with standards which are set by the board of the VNG after consultation among its members.[54] These standards have the goal of 'improving the quality and efficiency of joint municipal implementation'.[55] Three different levels of commitment to the standards exist: advised, comply-or-explain and mandatory. Currently, the VNG has set two mandatory standards: the Baseline Information Security Government (BIO, based on the ISO-standard for information security) and a processing agreement. Both standards are closely tied to legal obligations that municipalities have anyway. Insofar the statutes of the VNG contains provisions to unilaterally bind its members, such as the standards setting provision just mentioned, this "does rest[s] […] on the circumstance that the members [the municipalities] have entered into a legal relationship with the association and have therefore voluntarily submitted to the possibility of being unilaterally bound by the association" (Jak, 2011, Section 2). It is therefore still a form of self-regulation. As we will show, this position of the VNG and its members has implications for the governance possibilities around digital strategic autonomy. In a paper for a roundtable conversation, the VNG (2025a) formulated three problems with regards to digital strategic autonomy:

> "1. Our data is never completely safe with a US company, even if the data is in the EU. The US government can always retrieve it; 2. Our processes are too dependent on one or a few large companies. As a result, these companies can adjust conditions (including raising prices); and 3. When there is a technical problem at such a company, our entire service is down." (p. 1)

This maps well to the geopolitical dimension to digital strategic autonomy (1) and the public/private dimension (2 and 3), as described in Section 5.4 and 5.5.

6.2 Cloud use of Dutch municipalities

In 2022, the VNG commissioned multiple reports on the cloud-use of municipalities, the obstacles they face and on their expectations vis-à-vis the VNG. In 2017, only 16% of the software used by municipalities for their main tasks were SaaS-applications (M&I/Partners, 2023). In 2025, this is estimated to rise to 70%. M&I/Partners mentions as a reason that one of the larger service providers

[53] Every municipality has one vote for every 1000 inhabitants, with a minimum of 1 and a maximum of 75 ex Article 11(3) of the VNG Statutes (Vereniging van Nederlandse Gemeenten, 2020).
[54] Article 7(2) jo. 2(3)(b) jo. 17(3)(b) of the VNG Statutes.
[55] Article 2(3)(b) VNG Statutes.

for municipalities, Centric, will shift the focus of their services tot SaaS. New service providers often only supply their services as SaaS.[56]

The VNG also held a survey among its members, with 131 respondents on a total of 342 municipalities (Vereniging van Nederlandse Gemeenten, 2023b, 2023a).[57] 63% of the respondents have a cloud strategy, of which 86% choose for a SaaS-first approach. 7% of the respondents themselves develop software. For SaaS, 46% of the respondents think they have sufficient control in light of the BIO (Baseline Information Security Government) and the GDPR. 68% of the respondents use PaaS or IaaS, mainly Azure (91%). 40% of the respondents think they have sufficient control over these services.

The responding municipalities mention as a main concern the lack of control they have over data (74%). Another concerns are how to acquire personnel with the right knowledge (63%) and how to prevent a (too) large supplier dependency (61%). Framing these concerns in light of digital strategic autonomy, municipalities experience a lack of capabilities, capacities and control in the cloud domain. Municipalities have asked the VNG to provide an example cloud policy, strategy and roadmap (66%), define standards and guidelines (60%) and make collective agreements with cloud service providers (59%).

The magazine *Binnenlands Bestuur* has also investigated the use of Microsoft services by local governments (Hartholt, 2025a). 44 municipalities responded to the investigation. 91% of the respondents deem it neither achievable nor realistic to switch to another provider. Local governments mention a lack of knowledge among personnel and lack of sufficient alternatives in the market as reasons for this. The municipality of Zeewolde points out that a lot of (SaaS) suppliers only support Microsoft services, forcing municipalities to go along. Some municipalities, such as Hoekse Waard, have adopted a 'Microsoft, unless' strategy. The municipality of Heusden states that without Microsoft, the municipality cannot function. Nearly all municipalities fear the implication of US legislation such as the CLOUD Act. As a result of this *lock-in*, local governments fear price increases, especially when the current VNG Framework Agreement with Microsoft will expire in 2027. Until that time, the prices are fixed. Of all the surveyed municipalities, only Amsterdam is working on alternatives for Microsoft or other US technology. 44% of respondents are in favour of an investigation into alternatives for Microsoft.

6.3 Developing the self-assessment tool for in-use SaaS supporting municipal processes

6.3.1 Requirements

The function of the self-assessment tool will be to create awareness among municipalities on the status of their digital strategic autonomy. As such, it should function as an eye-opener and clarify what digital strategic autonomy, as theorized in this thesis, entails when it is applied by a municipality. It should allow municipalities to think more focused and systematically on their status of digital strategic autonomy for a certain process enabled by Software as a Service, and determine possible points of intervention. As such, the tool should answer the question for a municipal employee: "Am I actually dependent, and to what extent?" (GOV-VNG-1) and "Function as a conversation starter" (GOV-AMS).

[56] In Dutch, this shift is often called *verSaaSing* (making things SaaS).

[57] This is 38,3% of municipalities, which raises questions about the representativeness of the survey. We assume that other municipalities have even less capacities, capabilities and control.

Our choice to focus on SaaS is supported by the fact that municipalities rely more and more on SaaS for their service provisioning. As one of the interviewees stated: “so the problem exists mainly via dependency on SaaS-suppliers” (GOV-VNG-3), and another: “When you consider that 75% of the application landscape in municipalities consists of SaaS solutions, we should actually focus more on those SaaS solution” (GOV-VNG-2). New service providers often only provide their services via SaaS to municipalities (M&I/Partners, 2023)

The self-assessment tool should include a measure determining the sensitivity of data and the importance of the process enabled by the SaaS. As one of the interviewees noted: “In my opinion, this analysis hinges on data classification. What data are you going to process and how sensitive is that data? That more or less dictates the provisions you need to make” (GOV-VNG-2). And another: “What are the interests to be protected, what is the data and what are the services for which continuity is needed?” (GOV-AMS). As we’ve seen in previous sections, sub-vendor dependency is an important part of digital strategic autonomy. As such, the self-assessment tool should adress this (also mentioned by GOV-AMS).

Furthermore, because the developed tool is a self-assessment tool, it should not become to complex. Other indicators in the self-assessment tool are based on the interviews and the previous Sections, with attention to both the geopolitical dimension and the public/private dimension.

6.3.2 Existing assessment tools

A comparison and a description of different existing instruments for determining a level of digital strategic autonomy is discussed in Appendix F. The instruments differ in scope, but serve as input for the self-assessment tool presented in the next Section.

6.4 Subconclusion: the self-assessment tool

The self-assessment tool, developed based on the formulated requirements and input, is presented in Table 3. We explicitely added *“I don’t know”* as an answer option. This feature meets the requirement of the tool not becoming too complex. Similar to the central government (Netherlands Court of Audit, 2025), municipalities have a lack of knowledge on the use of cloud services, which is also confirmed by the interviews and the research discussed in Section 6.2. This lack of knowledge itself would indicate a lack of capacities, capabilities and control with regards to the digital strategic autonomy of municipalities. Answer options to the left indicate a low digital strategic autonomy, answer options to the right indicate a high level of digital strategic autonomy.

Table 3: Self-assessment tool

Preliminary questions	**Answers**			
What is the process?				
Who is the SaaS-provider?				
What is the criticality of the process?[58]	I don't know	Low	Medium	High

[58] To assess the criticality of the process, classify it as follows. Low criticality indicates that the process has minimal impact on municipal operations and can be temporarily disrupted without significant consequences. Medium criticality indicates that the process is important to the municipality, and its disruption could lead to operational challenges and potentially delaying services or outcomes. High criticality indicates that the process is essential to the municipalities' core functions, and any disruption could result in severe

What is the sensitivity of the data?[59]	I don't know	Low	Medium	High
Capacities and capabilities				
Does the municipality have a fallback option?[60]	I don't know	No	Yes	Yes and we tested it
Does the municipality have an exit-strategy in place?	I don't know	No	Yes	Yes and we tested it
Has the municipality made a risk assessment (general, DPIA)?	I don't know	No		Yes
Does the municipality have in-house employees with knowledge on SaaS in general?	I don't know	No	Yes, one or two people	Yes, more than two people
Could the municipality provide the SaaS-functionality themselves?	I don't know	No	Yes, partly	Yes, fully

Control				
Where is the SaaS-provider based?	I don't know	Outside of the EU	In the EU	In the Netherlands
Where is the data stored and processed?	I don't know	(Partly) outside of the EU	In the EU	In the Netherlands
Does the municipality have an overview of the sub-vendors used by the SaaS-provider?	I don't know	No	Partly	Yes, in full and updated
Does the SaaS provider use sub-vendors based outside of the EU?	I don't know	Yes		No
Have (non-EU) takeover attempts been made on the SaaS-provider?	I don't know	Yes		No
Do agreements on digital strategic autonomy exist in the contract between the municipality and the provider?[61]	I don't know	No		Yes

consequences, including financial loss, legal issues, or significant harm to citizens or others. Processes on one of the following two lists should be considered highly critical: (Informatiebeveiligingsdienst, n.d.-a, n.d.-b).

[59] To assess the sensitivity of the data, classify it as follows. **Low sensitivity** includes data that, if disclosed, would cause minimal or no harm to individuals or the municipality, such as publicly available information. **Medium sensitivity** includes data that could cause moderate harm or inconvenience if disclosed, such as internal communications or operational data. **High sensitivity** includes data that could result in significant harm if disclosed, including special categories of data and BSN-records, financial records, or any other data which is subject to heightened legal protection.

[60] This is not the same as an exit-strategy. A fall-back option is a system or a process which can be used when the SaaS application would become unavailable. This can be a backup system, or an alternative process. One interviewee (GOV-AMS) drew the comparison with an intersection. When traffic lights stop functioning, a traffic controller could be send to the intersection. Alternatively, the markings on the road guide traffic. The last fall-back option is the regular traffic rules guiding traffic.

[61] Examples could be agreements on termination of the contract under certain circumstances, e.g. a take-over by a non-EU party.

Are audit-agreements included in the contract between the municipality and the provider?	I don't know	No	Yes	Yes, and audits take place
Are measures against foreign government orders included in the contract between the municipality and the provider?	I don't know	No	Yes, some measures such as notification obligations	Yes, complete organizational and technical measures

Diagnostic questions				
How many times, out of 15, did you fill in 'I don't know'?				
Based on this self-assessment tool, where do you lack capabilities, capacities or control?				

7 Possible measures: the self-assessment tool in action

In this chapter we discusses possible measures municipalities can take to improve their digital strategic autonomy. Municipalities can use the self-assessment tool in the previous chapter to assess their digital strategic autonomy in a certain process enabled by SaaS. The measures in this chapter can then be used to improve this. Other institutional measures are also explored. As one of the interviewees noted: “You can create a process-level guideline […], but that's more like treating the symptoms. The core of the problem is [that we are] poorly organized.” (GOV-VNG-2). Another interviewee also argued that a process-level tool could miss the risks on the level of all municipalities together (GOV-VNG-3).

7.1 Applying the self-assessment tool

The self-assessment tool provides an high-over impression of the digital strategic autonomy of a municipality in the use of a certain process. The answer options most to the right indicate the highest level of digital strategic autonomy. The following sections provide measures municipalities can use to increase their level of digital strategic autonomy on some points. To provide an example, table 4 shows part of the tool regarding sub-vendors and a low digital strategic autonomy.

Table 4: Selection of the self-assessment tool regarding sub-vendors

Do agreements on digital strategic autonomy exist in the contract between the municipality and the provider?	I don't know	No	Partly	Yes, in full and updated
Does the SaaS provider use sub-vendors based outside of the EU?	I don't know	Yes		No

Sections 7.4 and 7.5 provide measures municipalities can use to increase their knowledge over sub-providers, including where they are located. Another example is the question on risk-assessments, shown in Table 5.

Table 5: Selection of the self-assessment tool regarding risk-assessment

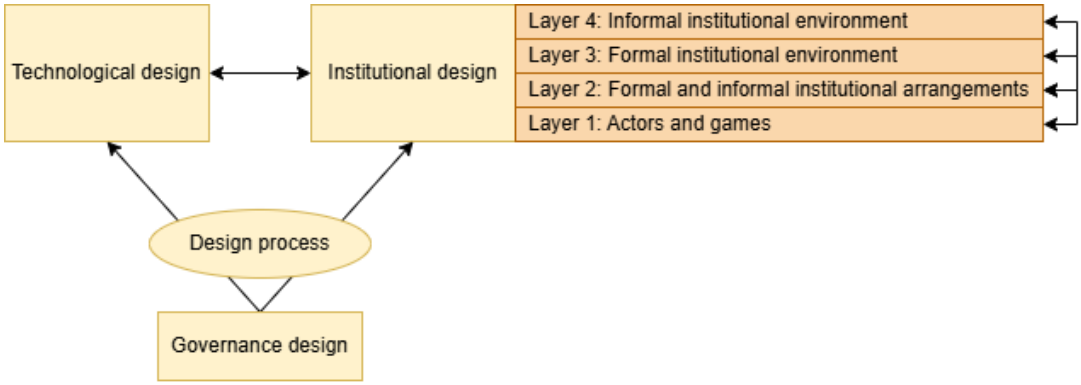
Has the municipality made a risk assessment (general, DPIA)?	I don't know	No	Yes

Section 7.4.2 explains how municipalities can use a DPIA to improve their control over SaaS-providers and increase their digital strategic autonomy. As we will show, the pooling of capacities and capabilities among multiple municipalities could enhance this approach, further indicating the need of other institutional measures.

7.2 An analytical framework for measures

Koppenjan and Groenewegen (2005) provide a comprehensive analytical framework for understanding and designing institutions in complex socio-technical systems. Their central argument is that technological systems, such as digital infrastructures, energy grids, or public service platforms, cannot be effectively designed or governed by focusing solely on their technical aspects. Instead, these systems require institutional arrangements to coordinate the actions and interactions of the multiple actors involved, which include both public and private parties, often with diverging interests and dependencies. The interaction and dependencies between the institutional and technological design is what renders these systems *complex*. Their framework distinguishes between three interrelated types of design, the *technological*, the *institutional* and the *governance* design, presented in Figure 11.

Figure 11: Framework for analysing and designing in socio-technical systems by Koppenjan and Groenewegen (2005)



The *technological design* is the substantive, technical solution or systems architecture. A large gap exists in this regard between the existing services and technologies provided by US hyperscalers, as highlighted in Chapter 5, and the services EU companies, governments and thereby municipalities can provide. Furthermore, there is a lack of interoperability and a *lock-in* effect is present. A concrete example of a technological design is the open source software on public space reports Signalen (*Signals*), which is developed by the city of Amsterdam and currently maintained by VNG. Municipalities can use this software (application layer) and host it themselves, or ask a private actor to provide it as SaaS (cloud to application layer). Other examples of technological design are encryption, developing technological standards or developing services for monitoring, authentication and databases, i.e. services which are applied on the higher steps of the cloud ladder.

The *institutional design* is the set of formal and informal rules, agreements and organizational arrangements that regulate actor positions, relations and behaviour. Koppenjan and Groenewegen introduce a four-layer model of institutional analysis and design, based on Williamson (1998), to specify this further. These layers are interdependent. Higher-level institutions constrain and shape lower-level arrangements, while changes at lower levels can, over time, influence higher-level norms and laws.[62] Effective institutions, therefore, requires attention to alignment and congruence across all layers. Layer 4 concerns the informal institutional environment: the culture, values, norms and

[62] Koppenjan and Groenewegen note that while institutions are robust and provide necessary stability, their evolution is slow, shaped by historical learning, power dynamics, and negotiation. Institutional (re)design must therefore proceed with caution, balancing the need for adaptability with the preservation of institutional capital, and recognizing the complex, multi-layered nature of institutional change in socio-technical systems.

attitudes of actors. Layers 3 concerns the formal institutional environment: laws and regulations. Layer 2 concerns the formal and informal institutional arrangements, e.g. contracts and alliances and informal rules, norms and relations. Layer 1 concerns the actors and games, referring to "actors/agents and their interactions aimed at creating and influencing (infrastructural) provisions, services, outcomes" (Koppenjan & Groenewegen, 2005, p. 247). For digital strategic autonomy, the institutional design or analysis can take place at all layers, as we will show in the next sections.

Lastly, *governance design* (Bharosa, 2022) is about designing the design process; it is the design of decision making processes. The governance design is about the scope of the design process, which actors are involved in which phase of the decision making, how are decision made and by whom and how can actors can leave and join this process. As such, the governance design determines how we get from a situation with a low level of digital strategic autonomy to a situation with a high level of digital strategic autonomy. The technological and institutional designs are the outcome of the design process, which is in turn determined by this governance design.

In the remaining sections, we suggest measures which can improve the digital strategic autonomy of municipalities. These measures already (partly) exist within the current technological, institutional and governance design or can be added. Our focus here is on measures within the institutional and governance design.

7.3 Current initiatives

Municipalities experience a severe lack of digital strategic autonomy. In this section we introduce initiatives that are currently carried out and contribute to the improvement of digital strategic autonomy, either by improving capabilities, capacities or controls.

7.3.1 VNG: determining a common position

The VNG has indicated that it is currently working on a position paper on the topic of digital strategic autonomy, describing the position of VNG on digital strategic autonomy, which is determined by its members as described in Section 6.1.1.[63] A common position can already help municipalities*:*

> "What [the VNG] can do is to support a municipality by taking a clear position, including an explanation of the problem and by offering support. Surely you want to be able to set an initial direction of: 'okay, why is it a problem? What do we think about it and then what impact does it have? And so this is our position and this is the line we take. That already helps a lot of municipalities" (GOV-VNG-1)

The position paper will also elaborate on the unique position of municipalities compared to, for examples, ministries. Municipalities implement national laws in the form of co-governance, as explained in Section 6.1. Because of this, they process a lot of sensitive data on citizens, compared to the ministries, whose main focus is policy making:

> "[The difference is indeed in particular regarding] personal data. Naturally apart from the implementing agencies.[64] There is a BSN [Citizen Service Number] in almost every application. And the difference is also in the amount of applications sitting at different municipalities. Each municipality has organised it in its own way. That would therefore have to be migrated separately by each municipality" (GOV-VNG-1).

The topic has been on the radar of the VNG for a longer time, as is clear from its *Digital Agenda Municipalities 2028*:

---

[63] Therefore, it is not a common position of all Dutch municipalities in a strict sense, unless all municipalities would vote in favour.
[64] In Dutch: "uitvoeringsorganisaties".

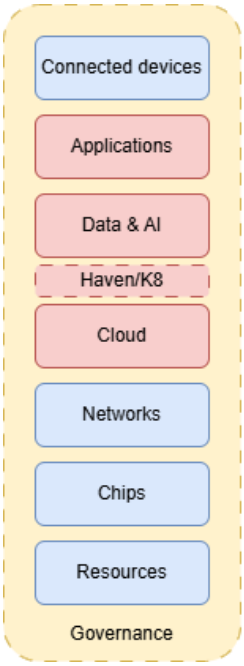
> “On many digital fronts, European, Dutch and local governments have become too dependent on non-European countries. To reduce that dependency, we need to increase our influence on the design and use of digital technologies and digital infrastructure. Digital independence thus involves several aspects: increasing democratic control, reducing strategic dependencies and thereby reducing vulnerabilities (including in the field of digital security)]” (Vereniging van Nederlandse Gemeenten [VNG], 2024, p. 24)

A common position can therefore explicate a norm and orientation which is present in the informal institutional environment.

7.3.2 Common Ground: Haven and Haven+

Haven is a VNG standard to achieve platform independent cloud hosting. Technically, it is a check-list with 16 mandatory and 2 suggested checks on the configuration of Kubernetes (or K8s) clusters, which is an open source system designed to automate (or ‘orchestrate’) the deployment, scaling and management of containerized applications. When this standard is followed, applications can be more easily migrated from one ‘Haven-compliant’ environment to another, regardless of the underlying cloud service provider. As such, it enables a functioning exit-strategy. Municipalities can use a standardized program of requirements to use in their contracts or procurement procedures (Haven, 2022). Figure 12 shows how following the Haven-standard functions as a layer at the top of the cloud layer. It effectively is a combination of a technological layer, namely the Kubernetes clusters, and part of the governance layer, as the standardised and agreed configuration of the technology. The haven standard itself is an example of a technological design. The adoption of the standard is, in turn, also determined by the institutional design.

Figure 12: The Haven orchestration layer



The Haven standard does however still allow for the use of cloud-specific services of US cloud service providers (developer.overheid, 2025), which diminished control and increased dependence, as discussed in Section 5.3. Haven+ aims to mitigate this. Haven+ is a project which develops cloud-agnostic services such as monitoring, authentication, databases, certificate management suitable for Haven environments (Haven, 2025). The use of these services and following its reference implementation in the technological design can reduce existing dependencies on the specific services of cloud service providers. Regarding the institutional design, in 2022, the VNG set Haven as an official standard according to the comply-or-explain level of commitment (Vereniging van Nederlandse Gemeenten, 2022). One of the interviewees mentioned, however, that such a standard is very soft, and any reason provided to deviate can suffice, hindering adoption (GOV-VNG-2).

7.3.3 GGI Cloud Centre of Expertise

In December 2023, the VNG launched the GGI (Municipal Common Infrastructure) cloud centre of expertise, based on needs from the municipalities. Its goal is to support municipalities in their transition to the cloud (GGI Cloud Expertisecentrum, n.d.-a). It focuses on developing strategic, legal (institutional), and technical resources, including the management of the GT Microsoft contract (see Section 7.3.4), cloud strategy guidelines and a risk-based implementation framework aligned with

national cloud policy.[65] It also advances a reference architecture for cloud infrastructure and data and develops standardized security frameworks for Microsoft Azure and 365. As such, the GGI Cloud Centre of Expertise contributes to the capacities and capabilities of municipalities by sharing and developing knowledge, and to the control by introducing security frameworks and managing the GT Microsoft contract.

Looking at the current activities of the centre, the focus lies mainly on improving the control of municipalities in their existing dependence on public cloud services from US cloud service providers, and less on supporting alternatives. This is understandable, as municipalities are highly dependent on e.g. Microsoft (see Section 6.2) and have asked for support in this context.

7.3.4 Framework agreements and standard configurations

GT(Gemeenschappelijke Telecommunicatie)-Microsoft is a framework agreement negotiated by the VNG with Microsoft. This is notably not a procurement process: municipalities would still have to buy or procure licenses. The framework agreement includes agreements on prices, its duration is until 2027. Until that time, municipalities can enter into the framework agreement. The joint negotiation of this agreement by the VNG is effectively a pooling of the capacities and capabilities of the municipalities, leading to a stronger negotiation position. Other GT framework agreements exist for i.a. printing services and mobile communication, but not for other cloud service providers (Vereniging van Nederlandse Gemeenten, 2025b). Next to framework agreements, the VNG (2023a) is working on standard configurations for cloud service providers. It states that

> "leading municipalities are willing to make these configurations available so that they can be elevated to 'municipal frameworks'. They see this last step as a task for VNG. This has also been offered for AWS. A framework for this platform is desirable to counter vendor dependence. However, only two municipalities are known to use AWS. Because of this, the investment is not considered reasonable for the time being." (p. 18)

One of the interviewees for this thesis also mentioned offering their BIO-compliancy template for Azure (ENG-SSC). This shows a clear tension relevant to the governance design design. The investment is currently not considered to be reasonable by the VNG, because of a lack of use by municipalities. However, a municipality would benefit from having these controls *before* they start using a cloud provider. Framework agreements and standard configuration can even stimulate adoption of cloud services that contribute to the digital strategic autonomy of a municipality. Therefore, even though framework agreements and standard configuration improve control, they can also further consolidate the use of large private non-EU cloud service providers, compared to service providers for which such frameworks do not exist (COM). An improved governance design could lead to framework agreements and standard configurations (institutional design) which better contribute to digital strategic autonomy.

7.4 General Data Protection Regulation

The General Data Protection Regulation (GDPR)[66] is an EU regulation, meaning that it is binding and directly applicable in all EU Member States, which includes the Netherlands. The regulation became effective on 25 May 2018. Its purpose is to regulate the protection of persons with regard to the

[65] The national cloud policy referred to does not sufficiently address digital strategic autonomy risks stemming from a lack of control as a result of foreign jurisdiction (Van der Wal, 2024).

[66] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation [GDPR]) (OJ 2016, L 119/1).

processing of their personal data and to protect their fundamental rights and freedoms.[67] The scope of the GDPR is in a large part determined by the definition of 'personal data', which refers to "any information relating to an identified or identifiable natural person (the 'data subject')".[68] In Section 7.3.1 we found that municipalities process a lot of personal data of citizens. As a result, a lot of their processing is governed by the GDPR.[69] We will first briefly introduce some important concepts, and then provide two examples of how municipalities (and/or the VNG) can use the GDPR to improve their control and as such their digital strategic autonomy. These measures highlights control possibilities present in the current institutional design.

Two important concepts in the GDPR for our purpose are the controller and the processor. The controller is the party that determines the purposes and means of the processing[70] of personal data.[71] The purposes and the means consider the *why* and the *how* of the personal data processing. The concept is functional, meaning that its application is based on a factual analysis of a case, not on a merely formal one (European Data Protection Board, 2021, para. 12). Municipalities are often the controller when using cloud services. A cloud service providers is often the processor, namely the party that processes personal data on behalf of the controller, i.e. the municipality.[72] As such, it is not allowed to process this data for its own purpose, as it would become a controller in respect of that processing and breach the GDPR (European Data Protection Board, 2021, para. 81).[73]

7.4.1 Obligations on sub-processors

SaaS-providers often use sub-vendors to provide their services, or in terms of the GDPR, they use sub-processors. An important prerequisite for municipalities in having control over the SaaS-provider is obtaining knowledge over these sub-vendors, not least because these sub-vendors themselves could be subject to foreign jurisdiction, as explained in Section 5.4. Having control over the use of these sub-processors by SaaS-providers would therefore increase the digital strategic autonomy of municipalities. The use of sub-processors is considered to be "essential means", on which the controller should decide (European Data Protection Board, 2021, para. 40, 2024, para. 152).

Article 28 GDPR establishes the legal framework governing the relationship between data controllers and processors, where a controller (such as a municipality) engages a processor (such as a SaaS provider) to process personal data on its behalf. This relationship must be governed by a written contract or other legal act (a 'processing agreement') that sets out the subject matter, duration, nature, and purpose of the processing, along with the types of personal data and categories of data subjects involved. It should also set out the agreements with regards to the use of sub-processors.[74] Article 28(2) GDPR specifies this further:

> "The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes."

---

[67] Article 1 GDPR

[68] Article 4(1) GDPR.

[69] Even more so because even for applications without personal data of citizens, municipality employees will often be logged-in, and all their actions on the cloud service have to be considered personal data, because this is data related to an identified person.

[70] 'Processing' is also broadly defined in Article 4(2) GDPR: *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*

[71] Article 4(7) GDPR.

[72] Article 4(8) GDPR.

[73] Article 28(10) GDPR.

[74] Article 28(3)(d) GDPR.

This provision effectively establishes a legal obligation for processors to identify their sub-processors and to obtain authorization from the controller before engaging them in processing operations. According to the EDPB, the primary difference between the specific authorisation and the general authorisation lies “in the meaning given to the controller’s silence” (European Data Protection Board, 2021, para. 157). With the specific authorization, a controller should authorize every change in the use of sub-processors before it is effectuated. Lack of authorization or absence of a response should be understood as a denial of the change request. When general authorization is in place, the processor must inform the controller of any intended changes in a timely manner and give the controller the opportunity to object. In this context, a lack of response should be interpreted as the controller not having any objections. A processor should provide information on the name, address and contact person of the sub-processor and provide a description of the intended processing activity.

The question then arises whether the whole processing chain, including sub-processors of sub-processors, should be identified. The EDPB answers this positively and states: “Although the chain [of processing] may be quite long, the controller retains its pivotal role in determining the purpose and means of processing” (2021, para. 152) and “The GDPR introduces specific obligations that are triggered when a (sub-)processor intends to engage another player, thereby adding another link to the chain, by entrusting to it activities requiring the processing of personal data.” (European Data Protection Board, 2021, para. 151). Since the controller must ultimately determine the purposes and means of processing, it should have full access to all information regarding all the processor’s sub-processors, i.e. the entire processing chain. Processors should therefore “proactively provide to the controller all information on the identity of all processors, sub-processors etc. processing on behalf of the controller, and should keep this information regarding all engaged sub-processors up to date at all times.” (European Data Protection Board, 2024, para. 32). Other legal reasons support this far-reaching interpretation. Data subjects have a right to specific and concrete information regarding all the recipients of their personal data[75] to exercise other GDPR rights (European Data Protection Board, 2024, Note 23). Data subjects need a full overview of all recipients, and hence sub-processors, to enable this.[76]

The controller has the right to audit all obligations arising from Article 28 GDPR, including the use of sub-processors.[77] It can e.g. request all the contracts between the initial processor and his sub-processors.

Municipalities could increase control over cloud service providers by ensuring that authorisation agreements are included in the contract and made effective, with reference to the legal obligations for both controllers and processors as stipulated in the GDPR. A joint approach with the VNG or the central government, whether or not in the form of standard contracts, could provide municipalities with more bargaining power in this regard. This could also increase its capabilities and capacities to e.g. perform audits and perform research on newly suggested sub-processors. Municipalities could also require such sub-processors authorisation procedures in its procurement processes. In practice, it can be hard for public bodies to meaningfully object, according to an investigation from the EDPB (2023):

> “Public bodies have highlighted difficulties in negotiating different rules on the identification/changes of sub-processors since most CSPs do not seem to be inclined to change their model considering that, in many cases, the CSPs claim that, it would not be possible for them to provide services in a different way.” (p. 16)

---

[75] Article 13(1)(e) jo. 14(1)(e) GDPR.
[76] See also CJEU Judgment of 12 January 2023, C-154/21 (*Österreichische Post*), para. 41-43.
[77] Article 28(3)(h) GDPR.

Next, we discuss a tool present in the current institutional design which municipalities can use to improve their ability to object to and effectively change current data processing by cloud service providers.

7.4.2 (Umbrella) Data Protection Impact Assessments

Under Article 35(1) GDPR, a controller has a legal obligation to carry out a data protection impact assessment (DPIA) prior to processing when the type of processing is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the processing. The Dutch Data Protection Authority has published a list of situations in which a DPIA is mandatory (Autoriteit Persoonsgegevens, 2019), but controllers can also voluntarily opt to perform one. Processors are obliged to assist the controller in its DPIA-obligations, and as such have to provide transparency about their data processing activities.[78] For municipalities processing extensive citizen data through cloud services, the GDPR creates an institutional environment in Layer 3 that enables more transparency and control in the Layer 1 negotiations which can result in institutional agreements, i.e. contracts, between municipalities and cloud service providers in Layer 2 which improve control and thereby digital strategic autonomy.

As part of their research project on the digital strategic autonomy of universities, the University of Amsterdam commissioned an expert memo on the use of DPIAs as a method to increase the control over the (personal) data processing by large commercial parties (Roosendaal, 2023).[79] The researchers (Meiring et al., 2023) conclude from this memo:

> "As practice has shown, a public document with legal technical findings on non-compliance with the GDPR can be used to force service providers to make the necessary changes, thus enhancing the position of buying organisations vis-à-vis powerful technology companies. In other words, a DPIA can serve as a 'sword' for universities to renegotiate contracts with commercial digital technology providers and regain independence." *(*p. 46)

Roosendaal (2023) describes how DPIAs can be used as such a 'sword' by universities. He argues that, in the context of his memo, universities should focus beyond the processing of 'content data' covered in Data Processing Addendums and also examine the processing of meta-data, i.e. diagnostic data, telemetry data, and logs. The processing of these data types is relevant to suppliers' commercial purposes. The scope of a DPIA should thus encompass the processing of all personal data generated from software usage, not just data processed by university employees in their research or educational activities. Organisations should perform a DPIA with a combination of legal and technical expertise: by using test accounts, by executing realistic usage scenarios, by intercepting data flows and by filing Data Subject Access Requests.[80] A DPIA assesses what the risks are for the rights and freedoms of data subjects, and whether these risks can be mitigated by measures. When a processor does not provide sufficient information on the data processing, this lack of transparency can result high risks for data subjects.[81] When DPIA results indicates a remaining high risk, a controller has to consult the supervisory authority, which in turn can prohibit the data processing when the intended processing would infringe the GPDR.[82]

---

[78] On the basis of Art. 28(3)(f) GDPR, the formulation of which shows how this is also supposed to counter any information asymmetry: *"taking into account the nature of processing and the information available to the processor"*. See also (Article 29 Working Party, 2017b, p. 15; European Data Protection Board, 2021, para. 137).

[79] The author of this thesis declares a professional relationship with Privacy Company as a working student. This expert memo is cited independently for its academic value in instrumentalising the GDPR, in particular DPIAs, to improve digital strategic autonomy.

[80] This is a right of data subject under Article 15 GDPR to i.a. receive a copy of all their personal data that is processed.

[81] One of the principles of the GDPR is that personal data shall be *"processed lawfully, fairly and in a transparent manner in relation to the data subject"* ex Article 5(1).

[82] Article 36 GDPR.

"The power is in the crowd" (Roosendaal, 2023, p. 15). Municipalities can improve their position by jointly commissioning or performing these DPIA's for the entire (local) public sector. These DPIAs are also called 'umbrella DPIAs'. Publishing these DPIAs in English and covering an entire sector can seriously impact the complete EU market for a cloud service provider, given that the GDPR is an EU-wide regulation. Public documentation of GDPR non-compliance, backed by a decision from a supervisory authority, can carry serious consequences, effectively prohibiting software use across the EU. Conversely, public documentation of GDPR compliance can be helpful for cloud service providers as it meets compliance requirements from customers.

This approach has proven useful in the past (Singer, 2023), with large and dominant service providers such as Microsoft, AWS and Google adjusting their services and contracts. For example, Dutch organizations representing the educational sector conducted a comprehensive DPIA that identified numerous high-risk data processing activities within Google's educational platform. The Dutch supervisory authority consequently argued that educational institution cannot (continue to) use the educational platform, unless the high risks would be mitigated. (Autoriteit Persoonsgegevens, 2021). According to Roosendaal: "the developments were closely followed by an international audience. The results were taken up internationally by governments and supervisory authorities" (2023, p. 16). Consequently, Google changed its approach and contractual, organizational and technical measures where introduces mitigated the high risks.

The VNG's position as coordinator could enable the umbrella DPIA approach that proved successful in the past for universities (via SURF, a Dutch cooperation of academia and research institutions) and the central government (via SLM Rijk, the strategic supplier management department of the central government). By pooling capacities and capabilities, municipalities can conduct the technical and legal research that they individually cannot afford. Currently, the VNG GGI Cloud Centre of Expertise does refer to the DPIAs performed by SLM Rijk on its website (GGI Cloud Expertisecentrum, n.d.-b) and to three VNG DPIAs that are currently being performed.

DPIAs can thus significantly improve municipalities' digital strategic autonomy by leveraging Article 28(3)(f) GDPR, which legally obligates processors to cooperate with controllers in fulfilling GDPR duties. This cooperation requirement transforms the power dynamic: suppliers cannot simply impose standardized terms but have to engage in substantive discussions about the data processing practices, where an entire sector is represented. Public documentation of GDPR compliance could enhance adoption. The VNG could therefore also choose to conduct DPIAs on currently less popular services which support digital strategic autonomy, e.g. because they do not fall under a foreign jurisdiction.

7.5 NIS 2 Directive and BIO

The Network and Information Systems Directive 2 (NIS 2) is an EU Directive, meaning that it is binding to the result to be achieved. Each Member State has to transpose a Directive into national legislation, the Netherlands will do so in the proposed Cyberbeveiligingswet (Cbw). The aim of the NIS 2 *is "to achieve a high common level of cybersecurity across the Union".*[83] The NIS 2 provides Member States the option to apply the directive to public administration at the local level.[84] The Dutch central government has used this option, and has appointed i.a. municipalities as 'essential entities'.[85] Digital strategic autonomy in the cloud layers and the layers on top is connected to cybersecurity, as

[83] Article 1(1) NIS 2.
[84] Article 2(5)(a) NIS 2.
[85] Article 8(1)(h) proposed Cyberbeveiligingswet.

indicated in Section 5.4. As such, the Cbw as part of the current institution design can provide municipalities with tools (and obligations) to improve their control.

The Cbw introduces certain specific obligations for essential entities, among which is a 'duty of care'.[86] The duty of care for municipalities will be specified by a governmental decree (Ministry of Justice and Security, 2024), specifically the Baseline Informatiebeveiliging Overheid (Baseline Information security Government, BIO.[87]

The previous version of the BIO was a form of self-regulation not grounded in law (Ministry of the Interior and Kingdom Relations, 2019, 2020). Apart from this, a wide range of sector-specific laws and regulations also contain information security requirements, often overlapping with the BIO. The Ministry of Justice and Security argues that this results from a lack of a formal legal status of the BIO. The central government has previously expressed the ambition to harmonize information security regulations across all levels of government and to give the BIO this formal legal status (Rijksoverheid, 2022, p. 35). The BIO is based on the NEN-EN-ISO norms 27001 27002 together with a list of measures for government organisations. The proposed new version of the BIO prescribes certain measures that could contribute to the digital strategic autonomy of municipalities, more specifically:

Table 6: A selection of BIO measures which can improve digital strategic autonomy (Ministry of the Interior and Kingdom Relations, 2025).

#	Measure
5.21.02	Prior to entering into the agreement, the supplier provides insight into the supply chain and any risks therein. The government organisation assesses whether the risks are acceptable.
5.21.04	During the contract term, the supplier communicates changes in the supply chain, including risks therein. At a minimum, this includes vulnerabilities and information security incidents that may affect the provision of services to the government organisation
5.23.01	Establish policies that oversee the inventory, classification, selection, assessment and management of Cloud Service Providers (CSP) and the termination of services by CSPs • Implement the policy. • Review this policy at least once every three years. • Include in contracts which situations can be grounds for contract termination. • When significant supplier changes occur, assess their risks and take appropriate action.

The measures prescribed in 5.21.02 and 5.21.04 correspond roughly to the obligations for processors described in Section 7.4.1. The difference is that this obligation applies to any ICT service-provider, regardless of the procession of personal data. Compliance with these BIO-measures ensures that municipalities are aware of all parties in the supply chain and can better assess the digital strategic autonomy related risks. Measure 5.23.01 specifically prescribes the creation of policies on the use of

[86] Article 21 proposed Cyberbeveiligingswet, which implements Article 21 NIS 2: *"[A duty of care to] take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services."*

[87] Article 21(5) proposed Cyberbeveiligingswet and

cloud service providers. Contracts should contain the grounds for contract termination. This can be used to include digital strategic autonomy related provision in the contract. For example, a contract could contain a provision for termination when a sub-vendor is used that falls under foreign jurisdiction, or when the contracting party is acquired by a foreign party. Including this in the contract, the second layer of the institutional design, would increase the control of municipalities.

7.6 Digital Government Act

With the Wet digitale overheid (Wdo, *Digital Government Act*), the central government has created a legal basis to make the use of certain standards mandatory for administrative bodies. The relation between the (mandatory) use of standards and independence from IT-providers is explicitly mentioned in the explanatory memorandum to the law: *"*The consequences of not adopting a particular standard may be too severe. This occurs when the lack of pace in adopting certain standards harms the public interest, for example, because […] vendor independence […] is at stake." (Ministry of the Interior and Kingdom Relations, 2018, p. 7). Applying open standards, part of the technological design, leads to less dependence of the application and data layers on the cloud layers, because it enables migration to other cloud service providers functioning according to the same standards. Section 7.3.2 explains this mechanism for Haven and Haven+.

Currently, the Forum Standaardisatie (the Standardisation Forum) controls a list with 'comply-or-explain' standards, to which municipalities have committed themselves via a system of self-governance, e.g. the administrative agreements between VNG and the central government (Vereniging van Nederlandse Gemeenten et al., 2011) and target agreements (Standardisation Forum, 2024). However, the adoption of open standards has stayed low, and it is rarely explained why an organization does not follow a standard (Ministry of the Interior and Kingdom Relations, 2018).[88] Multiple advisory reports have advocated for a more stringent system of open standards (Netherlands Court of Audit, 2011; Commissie Elias, 2014). Forum Standaardisatie has furthermore called for more standards focussing on digital strategic autonomy and for mandatory standards on cloud interoperability (Brienen & Ruig, 2024, para. 3.4 and 3.6).

Specifically, the Minister of the Interior and Kingdom relations can now, by a governmental decree (Algemene maatregel van bestuur), set a standard for municipalities if it satisfies three conditions.[89] Firstly, the designation of the standard must be necessary and proportionate in light of the proper functioning, safety, reliability, sustainable accessibility, or efficiency of electronic communications, or must be required for the implementation of international treaties or binding decisions of international organizations. Secondly, the standard must have been developed through a procedure that is open and accessible to all. Thirdly, the standard must be publicly accessible and free to use, with its specifications either permanently available free of charge or obtainable for a reasonable fee. The Minister can impose additional obligations on municipalities which 'adopt a course of action that conflicts with a designated standard'.[90] The Wdo has therefore impacted the governance design, and provides the central government with a decision making capacity to require municipalities to implement certain standards.

[88] This was confirmed by interviewee GOV-VNG-2.
[89] Article 3(2) Wdo.
[90] Article 3(5) Wdo.

7.7 Encryption

Encryption is often mentioned as a technical solution to improve control. As such, it is part of the technological design. As discussed in Section 5.4, encryption could prevent the application of US legislation impacting the confidentiality of municipal data, such as the CLOUD Act and FISA Section 702. However, this mitigating measure only addresses the concerns stemming from the risk to confidentiality of content data. It does not address the availability of data or other layers in the stack, it does not address the confidentiality of meta-data which cannot be encrypted, nor does it address the power cloud service providers have in shaping and determining their specific service provisioning in the public/private dimension, discussed in Section 5.5. As one of the interviewees noted:

> "It is such a significant challenge to protect your data in a way that the hosting provider cannot access it in any way, that in practice the actual level of protection will likely be disappointing. And this still only concerns confidentiality, not availability" (POL-NAT).

Encryption, or two-way cryptography, is the processes of encoding content data (plain text) to unreadable data (ciphertext). With asymmetric cryptography, this is achieved by the generation of keypairs of a public and a private key. The keys enable the encryption and decryption of the data. The sender of data encrypts the data using the recipient's public key. The data can then be decrypted by the recipients private key. As such, an important element of encryption with cloud services is determined by control over the private key of the customer, i.e. the municipality. Three types of encryption can be distinguished based on three states data can have: at-rest, in-transit and in-use. Encrypting data at rest refers to the encryption of stored data. Encrypting data in-transit refers to encrypting data that is transmitted over a network. Encryption of data in-use can sometimes be achieved by the application of certain types of privacy enhancing technologies, namely confidential computing. Relevant technologies here are multiparty computation, federated learning, homomorphic encryption, zero-knowledge proof and functional encryption (Veale, 2023). However, specifically for SaaS-functionalities to work, the cloud service needs access to the encryption keys to be able to perform operations on the data needed to provide a service (Hon et al., 2022). In the context of Microsoft for example:

> "Service encryption isn't meant to prevent Microsoft personnel from accessing your data. Instead, Customer Key helps you meet regulatory or compliance obligations for controlling root keys. You explicitly authorize Microsoft 365 services to use your encryption keys to provide value added cloud services, such as eDiscovery, anti-malware, anti-spam, search indexing, and so on." (Microsoft, 2025a).

Applying encryption fully to content-data, with the keys solely under control of the customer, requires capacities and capabilities, but is possible in some specific circumstances. This does however lead to loss of cloud functionalities and is often not suitable for all the data of a customer (Hubert, 2025c; Microsoft, 2024). As one of the interviewees noted:

> "We encrypt everything with our own keys. And I mean truly with double key encryption, confidential computing, and all the bells and whistles. So everything is managed in-house. Of course, on the one hand, that makes it a lot riskier, because there's nothing to fall back on. But it does ensure […] that you are the only one with access to the data. We've taken that quite far." (ENG-SCC)

One respondent furthermore noted a tension between *requiring* certain types of encryption, e.g. by means of the BIO (discussed in Section 7.5) or mandatory standards. Such a requirement could effectively exclude clouds service providers that better meet digital strategic autonomy wishes in other areas, e.g. because they do not fall under foreign jurisdictions, while entrenching the dominance of US hyperscalers, because of their extensive encryption solutions that could meet such

requirements. This clearly shows the relation with the institutional design with the technological design.

As such, encryption is no ‘silver bullet’ in achieving digital strategic autonomy for municipalities. Municipalities still depend on the cloud service provider to implement encryption solutions, which could be changed by the cloud service provider in the future.[91] Furthermore, encryption does not mitigate the broader availability dependency in any way. Encryption can, however, contribute to control and better protect the confidentiality of data vis-à-vis cloud service providers and foreign governments. Managing your own keys, and keeping these out of reach for third parties, requires specific capacities and capabilities on the side of the customer, e.g. to manage a self-hosted Hardware Security Modules (HSMs) to create and manages keys. The full responsibility for key management also creates a new risk: the loss of keys leads to the loss of data. Municipalities could choose to centrally manager customer keys, e.g. by having VNG or another organisation managing these. Justid provides a similar service on the level of the central government (Ministry of Justice and Security, 2025).

7.8 Subconclusion

In this chapter, we partly applied the self-assessment tool and presented several governance, institutional and technological measures which municipalities, on their own or together with others, can take to improve their digital strategic autonomy. Applying the framework of Koppenjan & Groenewegen (2005), resulted in the identification of technological measures such as the Haven and Haven+ standards and encryption. We identified the institutions and institutional solutions mentioned in Table 6.

Table 7: Initiatives per institutional layer

Institutional layer	Initiatives
4 - Informal institutional environment	• Common position VNG
3 - Formal institutional environment	• GDPR • NIS 2 and BIO • Wet digitale overheid
2 - Formal and informal institutional arrangements	• Standards setting: Haven and Haven+, encryption • Framework agreements: GT-Microsoft • Contracts with cloud service providers • VNG statutes
1 - Actors and games	• Contract negotiations with cloud service providers • Performing a Data Protection Impact Assessment

Municipalities can already improve their digital strategic autonomy by harnessing the control provided by legislation such as the GDPR, both via DPIAs and via obligations on transparency on sub-processors, and NIS 2 together with the BIO. Both laws enhances the position of municipalities in contract negotiations with SaaS-providers. Furthermore, municipalities can use encryption and follow the Haven and Haven+ standards in the technological design to increase digital strategic autonomy by improving control. However, proper key management requires capacities and capabilities on the

[91] A similar conclusion is drawn in a report commissioned by SLM Rijk (2021) on a specific cloud double key encryption solution.

side of municipalities, which could be improved by pooling resources via e.g. the VNG. The same goes for other technological capabilities and capacities of municipalities. There is a lack of supply in the EU concerning cloud native services, such as integrated databases and identity and access management. The Signalen project en Haven+ show that open source service development can contribute to this technological dimension.

The VNG already contributes to the digital strategic autonomy of municipalities. They do so by developing a common position on digital strategic autonomy, expressing a norm in the highest institutional layer, the development of standards like Haven and Haven+, the GGI Cloud Centre of Expertise and framework agreements. The VNG could furthermore perform umbrella DPIAs to improve control, and conclude more framework agreements with cloud service providers not falling under foreign jurisdiction, which could support both adoption and control. The VNG could also introduce more mandatory standards. However, as shown in Section 6.1.1, the VNG is not a governing body, but a private law association. It can ultimately not determine the actions municipalities take to improve their digital strategic autonomy. The Wet digitale overheid shows in this regard the influence the central government has in the governance design. It can impose mandatory standards on municipalities. Depending on the specific standards, this could enhance digital strategic autonomy.

8 Conclusion and discussion

This Chapter provides the research findings in Section 8.1, answering the research questions. Section 8.2 discusses research limitations. Lastly, Section 8.3 provides both practical recommendations and suggestions for future research.

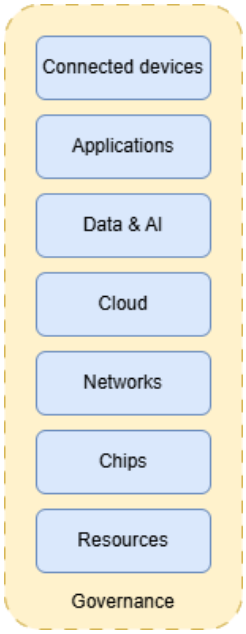
8.1 Research findings

In this thesis, we addressed the following main research question: *What self-assessment tool will support Dutch municipalities in systematically assessing and improving their digital strategic autonomy?* We provide the answer to this question by answering the following three sub-questions.

RQ 1: What is digital strategic autonomy?

This thesis defines digital strategic autonomy as "*the capabilities, capacities, and control to decide and act autonomously on essential digital aspects of our economy, society and democracy*". Capabilities refer to the knowledge, skills and tools and capacity refers to the amount of resources available. Control refers to the influence over capabilities, capacities, decisions and actions. Digital strategic autonomy serves as a more precise and actionable concept compared to digital sovereignty, which is prevalent in policy debates. Digital strategic autonomy better captures the ability of an actor to independently decide and act on essential digital aspects of its economy, society, and democracy by having sufficient capabilities, capacities, and control. The definition acknowledges that, unlike the binary and territorially anchored notion of sovereignty, digital strategic autonomy is context-dependent, more operationalizable, and better suited to address power differences, including those arising from direct reliance on large private actors. A synthesis of different stacks resembling the 'digital' in the definition leads to the stack presented in Figure 13. This conceptualisation of digital strategic autonomy serves allows for the analysis of every layer of an organisation in terms of its capacities, capabilities and control: its digital strategic autonomy. As such, this is the analytic theory developed in this thesis and contributes to the current literature on digital strategic autonomy. The layers are in reality not strictly separated, but serve the analytical function. Furthermore, the layers are interdependent. A lack of digital strategic autonomy on a layer lower in the stack can result in a lack of digital strategic autonomy on a layer higher in the stack. The working stack is mainly based on Sheikh (2022) and Bria et al. (2025). Their division of seven layers strikes a balance between a framework that gets complicatedly large and frameworks that are too small. Furthermore, the Eurostack report of Bria et al. has generated support from a variety of European businesses and both the German and French government, the former even mentioned it explicitly in the coalition agreement. We positioned the connected devices layer at the top, adhering to the principle that the highest layer in the stack is closest to the end users.

Figure 13: Digital Strategic Autonomy Stack



RQ 2: What are indicators of the digital strategic autonomy of Dutch municipalities on the cloud, data & AI and application layer?

In order to answer the second question, we focused on the Cloud, Data & AI and Applications layers in the stack. A lack of digital strategic autonomy on especially the Cloud layer has an uniquely large influence on the digital strategic autonomy on the layers above. We elaborated on the technical definition of cloud computing and the different cloud service models, covering the three layers mentioned in the form of SaaS. US cloud service providers dominate the EU and Dutch cloud market for government organisations. This is partly because of their integrated offerings on all the three stack layers. The specific type of cloud use impacts the level of control of an organisation. As an organization uses functions more specific to the cloud service provider, i.e. database functionalities, it has less direct control, depends more on these provider('s specific services), and requires less technical knowledge and expertise, leading to fewer in-house capacities and capabilities.

Both a geopolitical and a public/private dimension to digital strategic autonomy exist. The geopolitical dimension highlights the lack of control an organisation has as a result of foreign jurisdiction over de cloud service provider, i.e. US jurisdiction. With legislation such as the FISA Section 702 and sanctions, a foreign country can impact the confidentiality and availability of clouds service used for public service provisioning. Following Farrell and Newman (2019), we refer to this as respectively the panopticon and the chokepoint effect. The public/private dimension highlights how a lack of digital strategic autonomy leads to private values, determined by economic authority instead of political authority, impact public processes. This analysis of digital strategic autonomy in three specific layers of the stack provides indicators of the digital strategic autonomy of municipalities by unpacking the control, capabilities and capacities.

RQ 3: To what extent does the prototype self-assessment tool support Dutch municipalities in assessing and improving their digital strategic autonomy in the use of cloud services?
Chapter 6 presents the artefact developed in this thesis, a self-assessment tool for municipalities to assess their digital strategic autonomy on a process supported by SaaS, which again covers the Cloud, Data & AI and Applications layers. We partly applied the self-assessment tool and presented several institutional and technical measures which municipalities, on their own or together with others, can take to improve their digital strategic autonomy. In answering the previous research question, and as specifically mentioned by interviewees, municipalities themselves cannot take all the measures needed to improve their digital strategic autonomy. As such, the prototype self-assessment tool is more effective at evaluating digital strategic autonomy than at facilitating its improvement. Therefore, in answer to this research question, other solutions in the technological, institutional and governance design are relevant.

Municipalities can already improve their digital strategic autonomy by harnessing the control provided by legislation such as the GDPR and NIS 2 together with the BIO. Both laws provides enhances the position of municipalities in contract negotiations with SaaS-providers. Furthermore, municipalities can use encryption and (require SaaS-providers to) apply the Haven and Haven+ standards as a technical measure to increase digital strategic autonomy by improving control. Proper key management for encryption requires capacities and capabilities on the side of municipalities, which could be improved by pooling resources via e.g. the VNG.

The VNG already contributes to the digital strategic autonomy of municipalities. They do so by developing a common position on digital strategic autonomy, expressing a norm in the highest institutional layer, the development of standards like Haven and Haven+, the GGI Cloud Centre of Expertise and framework agreements. The VNG could furthermore perform umbrella DPIAs to improve control, and conclude more framework agreements with cloud service providers not falling under foreign jurisdiction, which could support both adoption and control. The VNG could also introduce more mandatory standards. However the VNG is not a governing body, but a private law

association. It can ultimately not determine the actions municipalities take to improve their digital strategic autonomy. The Wet digitale overheid shows in this regard the influence the central government has in the governance design. It can impose mandatory standards on municipalities contributing to digital strategic autonomy.

8.2 Limitations and future research

8.2.1 Arising from methodologies

While the methodologies employed in this thesis, i.e. the use of literature, semi-structured interviews, coding of transcripts, actor analysis and legal doctrinal research, provided valuable insights and supported the relevance cycle, several limitations should be acknowledged. These limitations may influence the interpretation and generalizability of the findings. Future research can improve this.

We held nine interviews with in total twelve persons. This is a limited amount of interviews, which fits the scope of the thesis. However, this could have led to biases. We accounted for this by inviting interviewees from different sectors and by comparing statements with the literature. However, future research could include more interviewees, especially from the private sector in general and US cloud service providers themselves. These perspectives might have been underrepresented. Furthermore, the coding of interviews is an interpretative act, as stated in Section 2.4.2. We accounted for this by providing transparency via the interview questions in Appendix C and the codes and their groundedness in Appendix D. However, future research could improve coding by introducing more coding cycles and by including more than one coder, subsequently comparing codes and reporting on inter-coder reliability.

Regarding the design science research approach, we did not include people in the environment, with their specific roles, capabilities and characteristics. This is contrary to Hevner et al. (2004). Future research could focus more on individuals working in municipalities which determine choices relevant to digital strategic autonomy. Gomes and Okano-Heijmans (2024, p. 11) indicate that this could be a relevant perspective: they argue that the distance between IT staff and policy makers poses a challenge. Another perspective could be to research the willingness of end-users, i.e. municipal employees to use other applications and how to influence this, which could be a decisive condition for successful migration.

Another limitation arises from the lack of evaluation in the application of the design science research methodology. This results in a self-assessment tool that is grounded in the analytic theory and developed in connection with the environment, but not tested in practice. Future research could account for this by evaluating both the working stack presented in this thesis and the self-assessment tool. Regarding the actor analysis, Enserink et al. (2022) note, with reference to van Eeten (2006), that an actor analysis can function as a ‘self-fulfilling prophecy’, limiting the view on other potential positions of actors. We accounted for this partly by having the interviews serve as input for the actor analysis, but future research could explore other actor perspectives, such a perspective based on trust in line with Blancato and Carr (2024).

For the analysis of US legislation by legal doctrinal research, we mainly used secondary literature. Future research could add a more substantive analysis of the legislation, for example by further analysing the possible sanctions the US can and cannot impose with impact on service provisioning to municipalities.

We presented the different measures in Chapter 7 using the framework of Koppenjan and Groenewegen (2005). Our focus was mainly on the institutional and governance measures, applying the 4-layer model of Williamson. We did present some technological measures, but these were less specific. The reason for this is partly the large scope of the measures, as these concern the digital

strategic autonomy of municipalities in a general sense. Improving digital strategic autonomy is dependent on a corresponding technological, institutional and governance design. Future research could therefore first zoom in on a specific process of a municipality with a low digital strategic autonomy, e.g. based on the outcome of the self-assessment tool, and analyse the more specific technological and institutional design, together with the governance design on how to get from the current to the desired situation.

8.2.2 Arising from scope

Other limitations arise from the scope of the thesis. First of all, we mainly draw attention to US hyperscalers falling under foreign jurisdiction. We also have essentially assumed that cloud service providers in the EU are equal, without focussing on EU-country specific laws regarding foreign government access to data an influence availability of services. This is justified in our view, as the EU is a separate legal order to which its Member States are part,[92] but future research could further identify the differences in legislation between EU countries to better assess this digital strategic autonomy dimension.

Next to this, specific providers focusing on the Dutch municipal market were not the focus of this thesis. Nonetheless, a lock-in effect with these providers does exist. Future research could explore these actors in more detail and assess their impact. Conversely, the focus on the EU or the central government was limited, even though these actors could indirectly contribute to the digital strategic autonomy of municipalities. For example by policy and legislation impacting the economic playing field, leading to more alternative cloud service providers based in the EU.

Future research could also pay more attention to procurement law, as it plays an important role in determining the level of control municipalities have. Other existing relevant (EU) legislation, such as provisions from the Data Act or other provision from NIS 2, may also affect digital strategic autonomy and should be considered.

Limitations furthermore arise from the restricted selection of stack layers. As a result, we excluded layers such as Connected Devices, Networks, Chips, and Resources excluded. Future work could include these layers and aim to define indicators for capacities, capabilities, and control. However, this may require a more national or EU-level approach.

Regarding the Cloud layer, future research could focus more on cloud deployment models and their impact on digital strategic autonomy: private cloud, community cloud, public cloud and hybrid- or multi-cloud (Mell & Grance, 2011). Hybrid-cloud solutions can combine a cloud service from US hyperscalers and EU service providers. The question remains to which extend this improves the digital strategic autonomy of municipalities, especially with regards to how this fits into the business model of these US hyperscalers and who has control over the technology enabling data and application portability between these two cloud services (see e.g. Rikap, 2025).

It is important to note that US hyperscalers find themselves in multiple jurisdictions, for which they themselves propose measures. We have discussed encryption, but US hyperscalers all have proposed multiple solutions to improve the digital strategic autonomy of their customer. As we have argued in this thesis, the geopolitical dimension of digital strategic autonomy is determined by US jurisdiction of US cloud service providers, raising questions over these solutions. Future research could address this question in the form of case studies on specific solutions, e.g. in line with the analysis of Blancato and Carr (2024).

A factual gap analysis, based on empirical data of specific cloud service used by municipalities could provide a more nuanced picture of existing dependencies and factual gap

[92] See also the famous case CJEU Judgment of 5 February 1963, Case 26/62 (*Van Gend & Loos*), ECLI:EU:C:1963:1, para. 3.

analysis between EU and non-EU cloud service offerings. A financial gap analysis, showing the cloud services costs of municipalities should be part of this analysis. This gap analysis is highly relevant for deciding how to move forward with digital strategic autonomy, specifically in determining the *strategy*. Dependencies are high as we highlighted in this thesis, and complete autonomy (autarky) is practically infeasible and undesirable. Many sub-vendors from EU service providers can be non-EU service providers. This entanglement renders the shift towards more digital strategic autonomy highly difficult. Current non-EU cloud service offerings can furthermore provide a high level of security and a high integration level of different services. As such, any strategy comes at a cost, whether it is financially or in the lower ease of use of alternatives.

We did not take into the Dutch Digitalisation Strategy (NDS), because the Dutch central government did not yet present it during our research. One of the principles of this strategy is a 'one-government' approach. As such, it is to be seen to which extent this strategy can contribute to the digital strategic autonomy of municipalities.

Lastly, future research could examine how municipalities and other governments themselves can be properly held accountable within the context of digital strategic autonomy, by focussing not only on control but on *legitimate* control. This is an underdeveloped perspective according to multiple authors (Maciel, 2025; Pohle et al., 2024; Roberts, 2024), and was out of scope in this thesis.

8.3 Recommendations

This sections presents specific recommendations to improve the digitals strategic autonomy of municipalities, based on the findings of this thesis. This can be summarized with **think big, act now, together.**

Think big

The EU is especially lagging behind on providing cloud services and applications. Currently, the default choice is to use US cloud service providers, whether or not as a sub-vendor of another SaaS-provider. Given the size of the problem, the EU and the central government need to act. Here, think big refers to the need to prioritize digital strategic autonomy within municipalities as well. A common position of the VNG can contribute to this prioritization. However, municipalities themselves also need to act if they want to improve their digital strategic autonomy. This is arguably a political choice. Expressing digital strategic autonomy as a norm can impact other institutional layers, such as contract negotiations and procurement decisions. As such, municipalities could mark 'a spot on the horizon'. The Dutch central government recently adopted a motion expressing that "by 2029, at least 30% of all cloud storage services and applications used by the central government will originate from Dutch-European providers, and to provide annual insight into progress on this objective" (Thijssen & Bruyning, 2025a). The city council of Amsterdam has expressed the same goal (IJmker et al., 2025). Other targets should be defined, e.g. 50% Dutch-European providers in 2034 or fully migrating away from a dominant supplier such as Microsoft, following government organisations in Denmark (Hartholt, 2025b; Hupkens, 2025). Furthermore, municipalities should determine which processes should never be dependent on non-EU cloud service providers, such as citizen registries and the identity & access management of municipalities.

Act now

The dependency of municipalities on US cloud service providers is large. However, municipalities can already take actions to improve their digital strategic autonomy, either by increasing their capacities, capabilities or control. Municipalities can already identify their most critical process with the self-

assessment tool, and use measures suggested in Chapter 7, such as following the Haven and Haven+ standards. In order to better protect the confidentiality of data, municipalities can use encryption. As indicated in the self-assessment tool, municipalities can inventorize possible exit strategies or fall-back options. Municipalities can also start pilots for certain processes, or experiment with less critical processes to enhance internal capabilities and capacities. By assessing the digital strategic autonomy on different processes now, municipalities can prepare for the next procurement cycle when current contracts end. As such, digital strategic autonomy can better serve as a guidance during procurement. Furthermore, acting now will result in a better negotiation position when the current VNG GT-Microsoft framework agreement expires in 2027.

Together

Digital strategic autonomy consists of capabilities, capacities and control. These can be pooled, as we showed in this thesis. For example, municipalities could together perform umbrella DPIAs to improve control. Furthermore, municipalities could cooperate within shared service centres to pool capabilities and capacities in providing cloud services themselves. Capabilities could furthermore be increased by sharing knowledge, as is already happening with the GGI Cloud Centre of Expertise of the VNG and the Centre of Competence on Digital Autonomy. Collaboration with the central government is also advised. Representing the entire government during contract negotiations and umbrella DPIAs can further increase the bargaining power against larger cloud service providers. Jointly performing general risk assessments is furthermore a more efficient use of capabilities and capacities and prevents duplication of work. A specific recommendation is a partnership between municipalities and Strategic Supplier Management on the level of central government. Although SLM (Strategic Supplier Management) Rijk mainly focuses on agreements with US cloud service providers, the parliament adopted a motion requesting the government to create a ‘SLM Autonomous Cloud’ (Thijssen & Bruyning, 2025b). Collaboration with the national government also allows for more direction and central control, as the VNG is an association dependent on 342 different municipalities, with limited influence on the actions of individual municipalities. Lastly, the lack of digital strategic autonomy of municipalities is not solely a Dutch problem. Recently, two Danish municipalities chose to replace all Microsoft services (Hartholt, 2025b). As such, this provides an opportunity for knowledge sharing and improving capabilities.

Bibliography

Abraha, H. H. (2020). Regulating law enforcement access to electronic evidence across borders: The United States approach. *Information & Communications Technology Law*, *29*(3), 324–353. https://doi.org/10.1080/13600834.2020.1794617

Adams, W. C. (2015). Conducting Semi-Structured Interviews. In K. E. Newcomer, H. P. Hatry, & J. S. Wholey (Eds.), *Handbook of Practical Program Evaluation* (1st ed., pp. 492–505). Wiley. https://doi.org/10.1002/9781119171386.ch19

Aldrich, R. J., & Karatzogianni, A. (2020). Postdigital war beneath the sea? The Stack's underwater cable insecurity. *Digital War*, *1*(1), 29–35. https://doi.org/10.1057/s42984-020-00014-x

AMS Institute. (2024). Beta procurement tool for cities to safeguard autonomy. *Responsible Sensing Lab*. https://responsiblesensinglab.org/projects/beta-procurement-tool-for-cities-to-safeguard-autonomy

Applegate, L. M. (1999). Rigor and Relevance in MIS Research. *MANAGEMENT INFORMATION SYSTEMS QUARTERLY*, *23*(1), 1–2.

Archer, L. B. (1984). Systematic method for designers. In N. Cross (Ed.), *Developments in Design Methodology* (pp. 57–82). John Wiley.

Article 29 Working Party. (2017a). *Data protection and privacy aspects of cross-border access to electronic evidence* [Statement]. Article 29 Working Party of the European Data Protection Authorities.

Article 29 Working Party. (2017b, October). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/611236/en

Autoriteit Consument en Markt. (2022). *Marktstudie Clouddiensten*. Autoriteit Consument en Markt. https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf

Autoriteit Persoonsgegevens. (2019, November). *Besluit lijst verwerkingen persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is*. https://wetten.overheid.nl/BWBR0042812/2019-11-27

Autoriteit Persoonsgegevens. (2021). *Advies: Google G Suite for Education* (Adviesrapport z2021-08230). Autoriteit Persoonsgegevens. https://open.overheid.nl/documenten/ronl-fc5fa700-2b23-4293-8f48-360b71233ee7/pdf

Balayn, A., & Gürses, S. (2024). Misguided: AI regulation needs a shift in focus. *Internet Policy Review*, *13*(3). https://doi.org/10.14763/2024.3.1796

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Benbasat, I., & Zmud, R. W. (1999). Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly*, *23*(1), 3–16. https://doi.org/10.2307/249403

Bendiek, A. (2018, November 28). No New Cold War: Give Strategic Interdependence a Chance. *Stiftung Wissenschaft und Politik (SWP)*. https://www.swp-berlin.org/publikation/no-new-cold-war-give-strategic-interdependence-a-chance-1

Bharosa, N. (2022). The rise of GovTech: Trojan horse or blessing in disguise? A research agenda. *Government Information Quarterly*, *39*(3), 101692. https://doi.org/10.1016/j.giq.2022.101692

Blancato, F. G. (2024). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet*, *16*(1), 12–32. https://doi.org/10.1002/poi3.358

Blancato, F. G., & Carr, M. (2024). The trust deficit. EU bargaining for access and control over cloud infrastructures. *Journal of European Public Policy*, 1–32. https://doi.org/10.1080/13501763.2024.2441418

Bozeman, B., & Bretschneider, S. (1994). The 'Publicness Puzzle' in Organization Theory: A Test of Alternative Explanations of Differences between Public and Private Organizations. *Journal of Public Administration Research and Theory: J-PART*, *4*(2), 197–223. https://www.jstor.org/stable/1181777

Bratton, B. H. (2015). *The stack: On software and sovereignty*. MIT Press.

Bria, F., Timmers, P., & Gernone, F. (2025). *EuroStack – A European Alternative for Digital Sovereignty*. Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/doi/10.11586/2025006

Brienen, A., & Ruig, J. de. (2024). *Standards and standardisation activities for cloud services*. Standardisation Forum. https://www.forumstandaardisatie.nl/sites/default/files/bestanden/website/Cloudonderzoek-FS-ENG.html

Brier, T. F., Jr. (2017). Defining the Limits of Governmental Access to Personal Data Stored in the Cloud: An Analysis and Critique of Microsoft Ireland. *Journal of Information Policy*, *7*, 327–371. https://doi.org/10.5325/jinfopoli.7.2017.0327

Broeksteeg, J. L. W. (2021). *Gemeenterecht* (1st ed.). Wolters Kluwer.

Burt, T. (2021, June). The Need for Legislative Reform on Secrecy Orders. *Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2021/06/30/the-need-for-legislative-reform-on-secrecy-orders/

Calderaro, A., & and Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, *31*(3), 415–434. https://doi.org/10.1080/09662839.2022.2101885

Carlson, J. (2025, April 3). *Licensing and pricing updates for on-premises server products coming July 2025*. https://techcommunity.microsoft.com/blog/microsoft_365blog/licensing-and-pricing-updates-for-on-premises-server-products-coming-july-2025/4400174?WT.mc_id=M365-MVP-9501

Česnakas, G., & Juozaitis, J. (2023). *European strategic autonomy and small states' security: In the shadow of power*. Routledge, Taylor & Francis group.

Chander, A., & Sun, H. (2021). Sovereignty 2.0. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3904949

Commissie Elias. (2014). *Parlementair onderzoek naar ICT-projecten bij de overheid: Eindrapport* (Kamerstuk 33326–5). Tweede Kamer der Staten-Generaal. https://zoek.officielebekendmakingen.nl/kst-33326-5.html

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Crul, S. (2022, March 29). *An introduction to the Stack*. Freedomlab.Com. https://www.freedomlab.com/posts/an-introduction-to-the-stack

Cyber Security Raad. (2021). *Nederlandse Digitale Autonomie en Cybersecurity'* [Beleidsnota]. Cyber Security Raad. https://www.cybersecurityraad.nl/documenten/adviezen/2021/05/14/csr-advies-nederlandse-digitale-autonomie-en-cybersecurity---csr-advies-2021-nr.-3

Czerwonka, P. (2024). Key Factors Influencing the Adoption of SaaS: A Case Study of Microsoft Exchange Online. *European Research Studies*, *XXVII*(Special A), 240–251. https://ersj.eu/journal/3648

De Vries, L. (2022). *Kanttekeningen bij de digitale stad: Gelijkheid, democratische controle en digitale autonomie in Nederlandse gemeenten*. Mr. Hans van Mierlo Stichting (VMS). https://d66.nl/vanmierlostichting/wp-content/uploads/sites/4/2022/04/Kanttekeningen-bij-de-digitale-stad_VMS_Laura-de-Vries_.pdf

developer.overheid. (2025). *Haven (Kubernetes)*. https://developer.overheid.nl/kennisbank/infra/standaarden/haven/

Duan, Y., Fu, G., Zhou, N., Sun, X., Narendra, N. C., & Hu, B. (2015). Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends. *2015 IEEE 8th International Conference on Cloud Computing*, 621–628. https://doi.org/10.1109/CLOUD.2015.88

Dutch Council of State. (2018). *Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen* (Ongevraagd advies W04.18.0230/I). Dutch Council of State. https://www.raadvanstate.nl/adviezen/@112661/w04-18-0230/

Eekels, J., & Roozenburg, N. F. M. (1991). A methodological comparison of the structures of scientific research and engineering design: Their similarities and differences. *Design Studies*, *12*(4), 197–203. https://doi.org/10.1016/0142-694X(91)90031-8

Elzinga, D. J. (2023, April). Decentrale autonomie als sterk verwaarloosd fenomeen | VNG. *Decentrale autonomie als sterk verwaarloosd fenomeen*. https://vng.nl/artikelen/decentrale-autonomie-als-sterk-verwaarloosd-fenomeen

Enserink, B., Bots, P., Van Daalen, E., Hermans, L., Koppenjan, J., Kortmann, R., Kwakkel, J., Slinger, J., Ruijgh Van Der Ploeg, T., & Thissen, W. (2022). *Policy Analysis of Multi-Actor Systems*. TU Delft OPEN Publishing. https://doi.org/10.5074/T.2022.004

European Data Protection Board. (2021). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (Guidelines 07/2020; Version 2.1). European Data Protection Board.

https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

European Data Protection Board. (2023). *2022 Coordinated Enforcement Action: Use of Cloud-Based Services by the Public Sector*. European Data Protection Board. https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf

European Data Protection Board. (2024). *Opinion 22/2024 on the reliance on processors and sub-processors for the provision of services by European Union institutions, bodies, offices and agencies*. https://www.edpb.europa.eu/system/files/2024-10/edpb_opinion_202422_relianceonprocessors-sub-processors_en.pdf

European Data Protection Supervisor. (2024). *EDPS Investigation into Use of Microsoft 365 by the European Commission*. European Data Protection Supervisor. https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf

European Political Strategy Centre. (2019). *Rethinking strategic autonomy in the digital age.* (EPSC Strategic Notes 30). Publications Office. https://data.europa.eu/doi/10.2872/231231

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty—Rhetoric and reality. *Journal of European Public Policy*, *31*(8), 2099–2120. https://doi.org/10.1080/13501763.2024.2358984

Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Floridi, L. (2014). *The fourth revolution how the infosphere is reshaping human reality*. Oxford university press.

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Foran, C., & Barrett, T. (2024, April 19). Senate passes surveillance bill despite contentious debate over privacy concerns. *CNN*. https://www.cnn.com/2024/04/19/politics/fisa-senate-negotiations

Galbraith, J. (2025). U.S. Sanctions on the International Criminal Court. *Verfassungsblog*. https://doi.org/10.59704/2fc624d0e6e15bd3

Ganz, A., Camellini, M., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Submarine Cables and the Risks to Digital Sovereignty. *Minds and Machines*, *34*(3), 1–23. https://doi.org/10.1007/s11023-024-09683-z

GGI Cloud Expertisecentrum. (n.d.-a). Over GGI-Cloud Expertisecentrum. *GGI Cloud Expertisecentrum*. Retrieved 16 May 2025, from https://gce.scgemeenten.nl/over-ons/

GGI Cloud Expertisecentrum. (n.d.-b). Overzicht generieke DPIA's voor cloud service providers. *GGI Cloud Expertisecentrum*. Retrieved 9 June 2025, from https://gce.scgemeenten.nl/project/overzicht-generieke-dpias-voor-cloud-service-providers/

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2023). Contested Spatialities of Digital Sovereignty. *Geopolitics*, *28*(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070

Gomes, A., & Okano-Heijmans, M. (2024). *Too late to act? Europe's quest for cloud sovereignty* [Policy Brief]. Clingendael Institute. https://www.clingendael.org/sites/default/files/2024-02/Policy_brief_Cloud_sovereignty.pdf

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611. https://doi.org/10.2307/25148742

Groeneveld, K., & Timmermans, H. (2021). *Reset de gemeentelijke ICT: Op zoek naar een evenwicht tussen zelf doen en uitbesteden*. Haystack. https://haystack.nl/product/reset-de-gemeentelijke-ict/

Grohmann, R., & Alexandre Costa Barbosa. (2024). BIG TECH SOVEREIGNTY: PLATFORMS AND DISCOURSE OF SOVEREIGNTY-AS-A-SERVICE. *AoIR Selected Papers of Internet Research*. https://doi.org/10.5210/spir.v2024i0.13948

Gürses, S., & van Hoboken, J. (2018). Privacy after the Agile Turn. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (pp. 579–601). Cambridge University Press. https://doi.org/10.1017/9781316831960.032

Hartholt, S. (2022, September 9). *Waarom toestaan van commerciële clouds bij de overheid géén goed idee is*. AG Connect. https://www.agconnect.nl/business/security/waarom-toestaan-van-commerciele-clouds-bij-de-overheid-geen-goed-idee-is

Hartholt, S. (2025a, February 13). Vastgeplakt aan Microsoft. *Binnenlands Bestuur*, *3*, 14–17. https://onlinetouch.nl/binnenlandsbestuur/bb-03-2025?timeout=1746617483&Signature=s1TmMlJe9wFbEzilCNju36Bno6t%2B0%3D&html=true#/14/

Hartholt, S. (2025b, June 6). Deense gemeenten beëindigen samenwerking met Microsoft. *iBestuur*. https://ibestuur.nl/artikel/deense-gemeenten-beeindigen-samenwerking-met-microsoft/

Harvey, C. J., & Moore, C. L. (2023). The client net state: Trajectories of state control over cyberspace. *Policy & Internet*, *15*(1), 133–151. https://doi.org/10.1002/poi3.334

Haven. (2022, August 18). *Haven—Techniek—Inkoop*. https://haven.commonground.nl/techniek/inkoop

Haven. (2025). *Haven+: Cloud-agnostische services*. https://gitlab.com/commonground/haven/havenplus/

Hemmings, J., Srinivasan, S., & Swire, P. (2020). Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the CLOUD Act. *Journal of National Security Law and Policy*, *10*, 631–677. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3469808

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). *Design Science in Information Systems Research*. *28*(1), 75–105.

Hirsch, P. M., & Levin, D. Z. (1999). Umbrella Advocates Versus Validity Police: A Life-Cycle Model. *Organization Science*, *10*(2), 199–212. https://doi.org/10.1287/orsc.10.2.199

Hoeksema, B. (2024). Digital Sovereignty, the Private Sector, and a Social Republican Alternative. *Digital Society*, *3*(3), 1–26. https://doi.org/10.1007/s44206-024-00140-z

Hoepman, J.-H. (2025, June 18). Sovereignty-washing. *Blog.Xot*. https://blog.xot.nl/2025/06/18/sovereignty-washing/index.html

Hon, W. K., Millard, C., & Singh, J. (2022). *Cloud Computing Demystified (Part 2): Control, Security, and Risk in the Cloud* (SSRN Scholarly Paper 4030114). https://doi.org/10.2139/ssrn.4030114

Hubert, B. (2024, May 31). De hele overheid naar de cloud? Dat is een politiek besluit. *Bert Hubert's Writings*. https://berthub.eu/articles/posts/de-hele-overheid-naar-de-cloud-dat-is-een-politiek-besluit/

Hubert, B. (2025a, March 14). The (European) cloud ladder: From virtual server to MS 365. *Bert Hubert's Writings*. https://berthub.eu/articles/posts/the-european-cloud-ladder/

Hubert, B. (2025b, April 27). 'The cloud' is not just servers. 'Going to the cloud' could also mean locking into a forever sub-contractor. *Bert Hubert's Writings*. https://berthub.eu/articles/posts/beware-cloud-is-part-of-the-software/

Hubert, B. (2025c, June 7). Demissionair de cloud in Denderen: Doe het niet. *Bert Hubert's Writings*. https://berthub.eu/articles/posts/demissionair-de-cloud-in-denderen/

Human Rights First. (2025, February 10). What's Different about the new ICC Sanctions? Still Appalling, Not Much Narrower. *Human Rights First*. https://humanrightsfirst.org/library/whats-different-about-new-icc-sanctions/

Hupkens, H. (2025, June 11). Deens ministerie van Digitalisering wil gebruik Microsoft uitfaseren. *iBestuur*. https://ibestuur.nl/artikel/deens-ministerie-van-digitalisering-wil-gebruik-microsoft-uitfaseren/

IJmker, E. C., Garmy, I. G., & Belkasmi, M. (2025). *Motie Maak digitale autonomie concreet*. https://amsterdam.raadsinformatie.nl/document/15621840/1/158_25+Motie++IJmker+c_s_+maak+digitale+autonomie+concreet?connection_type=17&connection_id=11937307

International Organization for Standardization. (1994). *Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model* (Standard ISO/IEC 7498-1:1994). International Organization for Standardization.

International Organization for Standardization. (2023). *Information technology—Cloud computing—Part 1: Vocabulary* (Standard ISO/IEC 22123-1:2023). International Organization for Standardization.

Irion, K. (2012). Government Cloud Computing and National Data Sovereignty. *Policy & Internet*, *4*(3–4), 40–71. https://doi.org/10.1002/poi3.10

Jak, N. (2011). Annotatie bij ABRvS 25 mei 2011, ECLI:NL:RVS:2011:BQ5933 (VNG is geen bestuursorgaan). *Gemeentestem (Gst.)*, *2011*(121). https://www.inview.nl/document/id6b4b63d4362843138850e21998e0aaea

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science*. Springer International Publishing. https://doi.org/10.1007/978-3-319-10632-8

Jongen, H., Ramos, G., & van Wengen, W. (2022). *Number of CLOUD Act requests* [Memorandum to the Dutch Ministry of Justice and Security—NCSC]. Greenberg Traurig LLP.

Kagermann, H., Streibich, K.-H., & Suder, K. (2021). *Digital Sovereignty: Status Quo and Perspectives*. acatech – National Academy of Science and Engineering. https://www.acatech.de

Kersten, M. (2025, February 12). It's all about control: U.S. sanctions against the International Criminal Court and navigating a path forward. *Justice in Conflict*. https://justiceinconflict.org/2025/02/12/its-all-about-control-u-s-sanction-on-the-international-criminal-court-and-navigating-a-path-forward/

Koning, M. de. (2024, October 21). DNB: Burgers moeten beseffen dat financiële dienstverlening uit kan vallen. *NRC*. https://www.nrc.nl/nieuws/2024/10/21/dnb-burgers-moeten-beseffen-dat-financiele-dienstverlening-uit-kan-vallen-a4870084

Koningsveld, H. (2006). *Het verschijnsel wetenschap*. Boom.

Koppenjan, J., & Groenewegen, J. (2005). Institutional design for complex technological systems. *International Journal of Technology, Policy and Management*, *5*(3), 240. https://doi.org/10.1504/IJTPM.2005.008406

Kotulski, Z., Nowak, T., Sepczuk, M., Bocianiak, K., Pawlikowski, T., Podlasek, A., & Wary, J.-P. (2024). Keeping Verticals' Sovereignty During Application Migration in Continuum. *Journal of Network and Systems Management*, *32*(4), 1–46. https://doi.org/10.1007/s10922-024-09843-7

Krikke, J. (2022). Opinie—Kamerbrief Rijksbreed cloudbeleid 2022. *Tijdschrift Voor Internetrecht*, *5*, 187–188. https://denhollander.info/artikel/17482

Kroll, H. (2024). *Assessing open strategic autonomy*. (JRC136359). Publications Office of the European Union. https://data.europa.eu/doi/10.2760/767279

Lambach, D., & Oppermann, K. (2023). Narratives of digital sovereignty in German political discourse. *Governance*, *36*(3), 693–709. https://doi.org/10.1111/gove.12690

Lee, A. (1999). Inaugural Editor's Comments. *MIS Quarterly*, *23*(1), v–xi. https://www.jstor.org/stable/249400

Lovink, G. (2020). Principles of Stacktivism. *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, 716–724. https://doi.org/10.31269/triplec.v18i2.1231

Lynn, T., Van Der Werff, L., & Fox, G. (2021). Understanding Trust and Cloud Computing: An Integrated Framework for Assurance and Accountability in the Cloud. In T. Lynn, J. G. Mooney, L. Van Der Werff, & G. Fox (Eds.), *Data Privacy and Trust in Cloud Computing* (pp. 1–20). Springer International Publishing. https://doi.org/10.1007/978-3-030-54660-1_1

Maciel, M. (2025, April 3). *Digital sovereignty: The end of the open internet as we know it?* https://www.diplomacy.edu/blog/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/

Meiring, A., Yakovleva, S., Irion, K., van Hoboken, J., & van Eechoud, M. (2023). *Information Law and the Digital Transformation of the University: Part I - Digital Sovereignty*. Institute for

Information Law. https://www.uva.nl/binaries/content/assets/uva/nl/over-de-uva/over-de-uva/beleid-en-financien/digitale-agenda/part-i-digital-sovereignty.pdf

Mell, P. M., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST SP 800-145; 0 ed., p. NIST SP 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Michels, J. D. (2025a, maart). *Europeans, forget the US Cloud Act… worry about FISA instead (!)*. https://www.linkedin.com/pulse/europeans-forget-us-cloud-act-worry-fisa-instead-dave-michels-anjze/

Michels, J. D. (2025b). Sovereign Cloud for Europe. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5146122

Michels, J. D., Millard, C., & Walden, I. (2023). *On Cloud Sovereignty: Should European Policy Favour European Clouds?* (SSRN Scholarly Paper 4619918). https://doi.org/10.2139/ssrn.4619918

Michels, J. D., Walden, I., & Millard, C. (2025). *Storm Clouds are Building: Surveillance, Sovereignty, and State Interests* (SSRN Scholarly Paper 5159829). Social Science Research Network. https://doi.org/10.2139/ssrn.5159829

Microsoft. (2022, mei). Wigo4it: How a public-sector organization is modernizing critical services with cloud technology. *Microsoft Customer Stories*. https://www.microsoft.com/en/customers/story/1505961706126415574-wigo4it-national-government-azure-en-netherlands

Microsoft. (2024, July 19). *Double Key Encryption (DKE)*. https://learn.microsoft.com/en-us/purview/double-key-encryption

Microsoft. (2025a, April 2). *Overview of Customer Key—Microsoft Purview*. https://learn.microsoft.com/en-us/purview/customer-key-overview

Microsoft. (2025b, April 15). *Microsoft 365-roadmap | Microsoft 365*. https://www.microsoft.com/nl-nl/microsoft-365/roadmap

Ministry of Foreign Affairs. (2022, November 8). *Kamerbrief Open Strategische Autonomie* [Kamerbrief]. https://open.overheid.nl/documenten/ronl-5b134a1ba15379fdfc6ecb0b6dcc431843087193/pdf

Ministry of Justice and Security. (2024, December 16). *Memorie van Toelichting—Cyberbeveiligingswet*. https://open.overheid.nl/documenten/81b4227e-7375-45fa-a8f7-eb2d763698dc/file

Ministry of Justice and Security. (2025). *Beheer Public Key Infrastructure (PKI) – Hardware Security Modules (HSM)*. Justitiële Informatiedienst. https://www.justid.nl/producten-en-dienstencatalogus/digitale-veiligheid-betrouwbaarheid-authenticatie/pki---hsm

Ministry of the Interior and Kingdom Relations. (2018, June 19). *Memorie van Toelichting—Wet digitale overheid*. https://zoek.officielebekendmakingen.nl/kst-34972-3.html

Ministry of the Interior and Kingdom Relations. (2019, April 16). *Toepassen van de Baseline Informatiebeveiliging Overheid in het digitale verkeer met het Rijk [Circulaire]*. https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html

Ministry of the Interior and Kingdom Relations. (2020, February 17). *Toepassen van de Baseline Informatiebeveiliging Overheid versie 1.04 in het digitale verkeer met het Rijk [Circulaire]*. https://zoek.officielebekendmakingen.nl/stcrt-2020-7857.html

Ministry of the Interior and Kingdom Relations. (2022, August 29). *Rijksbreed Cloudbeleid 2022*. https://open.overheid.nl/documenten/ronl-a79331dc7c088f2cb6259f591c3b4f2fbcc9b5f1/pdf

Ministry of the Interior and Kingdom Relations. (2025). *Verplichte overheidsmaatregelen, Baseline Informatiebeveiliging Overheid 2 (BIO2), versie 1.1*. https://minbzk.github.io/Baseline-Informatiebeveiliging-Overheid/maatregelen/

M&I/Partners. (2023). *Analyse cloud-ontwikkelingen gemeenten*. https://gce.scgemeenten.nl/wp-content/uploads/sites/2/2024/09/Bijlage-Rapportage-MI-Analyse-cloud-ontwikkelingen-gemeenten-v1.0-003.pdf

Moerel, L., & Timmers, P. (2021). *Reflections on Digital Sovereignty* (SSRN Scholarly Paper 3772777). https://papers.ssrn.com/abstract=3772777

Monterie, A. (2024, November 15). DNB waarschuwt voor te grote macht Big Tech. *Computable.nl*. https://www.computable.nl/2024/11/15/dnb-waarschuwt-voor-te-grote-macht-big-tech/

Netherlands Court of Audit. (2011). *Open standaarden en opensourcesoftware bij de rijksoverheid* [Report]. Netherlands Court of Audit. https://www.rekenkamer.nl/publicaties/rapporten/2011/03/15/open-standaarden-en-opensourcesoftware-bij-de-rijksoverheid

Netherlands Court of Audit. (2025). *Dutch central government in the cloud: Dark clouds looming*. Netherlands Court of Audit. https://english.rekenkamer.nl/publications/reports/2025/01/15/dutch-central-government-in-the-cloud

Nunamaker, J. F., Chen, M., & Purdin, T. D. M. (1990). Systems development in information systems research. *Journal of Management Information Systems*, *7*(3), 89–106. https://doi.org/10.1080/07421222.1990.11517898

Okano-Heijmans, M. (2023). *Open strategic autonomy: The digital dimension*. Clingendael.

Opara-Martins, J. (2017). *A decision framework to mitigate vendor lock-in risks in cloud (SaaS category) migration* [Doctoral Thesis]. Bournemouth University.

Passanti, C., & Pommerolle, M.-E. (2022). The (un)making of electoral transparency through technology: The 2017 Kenyan presidential election controversy. *Social Studies of Science*, *52*(6), 928–953. https://doi.org/10.1177/03063127221124007

Passchier, R. (2021). *Artificiële intelligentie en de rechtsstaat: Over verschuivende overheidsmacht, Big Tech en de noodzaak van constitutioneel onderhoud*. Boom Juridisch. https://www.boomdenhaag.nl/webshop/artificiele-intelligentie-en-de-rechtsstaat

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Peters, H. (2011). Annotatie bij ABRvS 25 mei 2011, ECLI:NL:RVS:2011:BQ5933 (VNG is geen bestuursorgaan). *AB Rechtspraak Bestuursrecht*, *2011*(233). https://www.inview.nl/document/ide65e251d638644e9b1cc7d86832ce782

Platform voor de InformatieSamenleving & AMS-IX. (2025). *Argumentenkaart Cloud*. https://ecp.nl/wp-content/uploads/2025/02/Argumentenkaart-cloud.pdf

Pohle, J. (2023). The European Strive for Digital Sovereignty: Have We Lost Our Belief in the Global Promises of the 'Free and Open Internet'? *Weizenbaum Journal of the Digital Society*, *3*(2). https://doi.org/10.34669/WI.WJDS/3.2.6

Pohle, J., Nanni, R., & Santaniello, M. (2024). Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. *Policy & Internet*, *16*(4), 666–671. https://doi.org/10.1002/poi3.437

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://policyreview.info/concepts/digital-sovereignty

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. *Policy & Internet*, *14*(1), 13–27. https://doi.org/10.1002/poi3.296

Politie Noord-Holland. (2024, November 4). *Politie Noord-Holland start met aangifte doen via videobellen*. https://www.politie.nl/nieuws/2024/november/4/04-politie-noord-holland-start-met-aangifte-doen-via-videobellen.html

President's Intelligence Advisory Board and Intelligence Oversight Board. (2023). *Review of FISA Section 702 and Recommendations for Reauthorization*. Executive Office of the President of the United States. https://int.nyt.com/data/documenttools/presidents-intelligence-advisory-board-and-intelligence-oversight-board-review-of-fisa-section-702-and-recommendations-for-reauthorization/4d2d3218303fc702/full.pdf

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting and Management*, *8*(3), 238–264. https://doi.org/10.1108/11766091111162070

Quell, M. (2025). Trump's sanctions on ICC prosecutor have halted tribunal's work. *AP News*. https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3

Ramos, G., Maciejewski, A., & Jongen, H. (2022). *Application of the CLOUD Act to EU Entities* [Memorandum to the Dutch Ministry of Justice and Security—NCSC]. Greenberg Traurig LLP. https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo

Rensen, F. (2024, December 2). Staatssecretaris zet verhuizing van overheidsgegevens naar de cloud voorlopig stil. 'Dit gaat om de Nederlandse veiligheid'. *de Volkskrant*. https://www.volkskrant.nl/tech/staatssecretaris-zet-verhuizing-van-overheidsgegevens-naar-de-cloud-voorlopig-stil-dit-gaat-om-de-nederlandse-veiligheid~bf8d9544/

Reuters. (2015a, June 30). NSA wiretapped two French finance ministers, WikiLeaks says. *The Guardian*. https://www.theguardian.com/world/2015/jun/30/nsa-wiretapped-two-french-finance-ministers-wikileaks-says

Reuters. (2015b, July 8). NSA tapped German Chancellery for decades, WikiLeaks claims. *The Guardian*. https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel

Richards, D. (1996). Elite Interviewing: Approaches and Pitfalls. *Politics*, *16*(3), 199–204. https://doi.org/10.1111/j.1467-9256.1996.tb00039.x

Ridgway, W. (2018, December 13). Understanding The CLOUD Act's Expansive Reach. *Mondaq*. https://www.mondaq.com/unitedstates/privacy-protection/763706/understanding-the-cloud-acts-expansive-reach

Rijksoverheid. (2022, November). *Werkagenda Waardengedreven Digitaliseren*. https://zoek.officielebekendmakingen.nl/blg-1062267.pdf

Rikap, C. (2025, June 16). How Big Tech Turns Knowledge into Power. *Critical Takes*. https://criticaltakes.org/the-corporation/how-big-tech-turns-knowledge-into-power/

Roberts, H. (2024). Digital sovereignty and artificial intelligence: A normative approach. *Ethics and Information Technology*, *26*(4), 1–10. https://doi.org/10.1007/s10676-024-09810-5

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies* (SSRN Scholarly Paper 3937345). https://doi.org/10.2139/ssrn.3937345

Rone, J. (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

Roosendaal, A. (2023). *The GDPR as a means to protect Digital sovereignty of universities*.

Rosenthal, D. (2025). *Frequently Asked Questions (FAQ) on the Risk of Foreign Lawful Access and the Statistical 'Rosenthal' Method for Assessing It*. https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf

Rossi, M., & Sein, M. K. (2003, August). Design research workshop: A proactive research approach. *Proceedings of the Twenty-Sixth Information Systems Research Seminar in Scandinavia (IRIS 26)*.

Saldana, J. (2009). *The Coding Manual for Qualitative Researchers* (1–1 online resource.). Sage.

Satariano, A., & Smialek, J. (2025, June 20). Europe's Growing Fear: How Trump Might Use U.S. Tech Dominance Against It. *The New York Times*. https://www.nytimes.com/2025/06/20/technology/us-tech-europe-microsoft-trump-icc.html

Schaake, M. (2024). *The tech coup: How to save democracy from Silicon Valley*. Princeton University Press.

Sharon, T., & Gellert, R. (2024). Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy. *Information, Communication & Society*, *27*(15), 2651–2668. https://doi.org/10.1080/1369118X.2023.2246526

Sheikh, H. (2022). European Digital Sovereignty: A Layered Approach. *Digital Society*, *1*(3), 25. https://doi.org/10.1007/s44206-022-00025-z

Sheikh, H. (2024). *Atlas van de digitale wereld: Richting Europese digitale soevereiniteit*. Boom.

Simmon, E. (2018). *Evaluation of cloud computing services based on NIST SP 800-145* (NIST SP 500-322; p. NIST SP 500-322). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.500-322

Singer, N. (2023). How The Netherlands is taming Big Tech. *The New York Times*. https://www.nytimes.com/2023/01/18/technology/dutch-school-privacy-google-microsoft-zoom.html

Sipe, L. R., & Ghiso, M. P. (2004). Developing Conceptual Categories in Classroom Descriptive Research: Some Problems and Possibilities. *Anthropology & Education Quarterly*, *35*(4), 472–485. https://www.jstor.org/stable/3651350

SLM Rijk. (2021). *Analyse Microsoft Double Key Encryption (DKE)* (Technical Report SLM-DKE-2021-01). Privacy Company. https://slmmicrosoftrijk.nl/wp-content/uploads/2021/02/Analyse-Microsoft-DKE-13-jan-2021.pdf

Snijders, P., & Wever, R. (2024, September 30). *Gezamenlijke prioriteitstelling Huis van Thorbecke [U202400491]*. https://vng.nl/sites/default/files/2024-10/20240930-brief-kabinet-gezamenlijke-prioriteitstelling-huis-van-thorbecke.pdf

Solarino, A. M., & Aguinis, H. (2021). Challenges and Best-practice Recommendations for Designing and Conducting Interviews with Elite Informants. *Journal of Management Studies*, *58*(3), 649–672. https://doi.org/10.1111/joms.12620

Sonnenberg, C., & vom Brocke, J. (2012). Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research. In K. Peffers, M. Rothenberger, & B. Kuechler (Eds.), *Design Science Research in Information Systems. Advances in Theory and Practice* (pp. 381–397). Springer. https://doi.org/10.1007/978-3-642-29863-9_28

Speed, R. (2025). Why is Big Tech hellbent on making AI opt-out? *The Register*. https://www.theregister.com/2025/01/23/why_is_ai_optout/

Standardisation Forum. (2024). *Streefbeeldafspraken informatieveiligheid*. Standardisation Forum. https://www.forumstandaardisatie.nl/onderwerpen/veilig-internet/streefbeeldafspraken

Stolwijk, C., Punter, L. M., Timan, T., Berkers, F. T. H. M., Georgieva, I. N., Gilsing, R. A. M., Bastiaansen, H. J. M., Hoekstra, M., Yagafarova, A. Y., Mulder, W., Dalmolen, S., & Joosten, H. J. M. (2022). *Bridging the Dutch and European Digital Sovereignty gap* (R10507). TNO. https://resolver.tno.nl/uuid:588a42c3-9369-4c18-8163-e7b5dc183aff

Stolwijk, C., Punter, M., Timmers, P., Rabbie, J., Regeczi, D., & Dalmolen, S. (2024). *Towards a sovereign digital future – the Netherlands in Europe* (060.55452/01.01). TNO. https://publications.tno.nl/publication/34642268/o5remY/TNO-2024-R10300.pdf

Svantesson, D. (2023). A Starting Point for Re-thinking 'Sovereignty' for the Online Environment. In A. Chander & H. Sun (Eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (pp. 49–71). Oxford University Press. https://doi.org/10.1093/oso/9780197582794.003.0003

Svantesson, D., Haataja, S., Ireland-Piper, D., & Chen, K.-W. (David). (2023). On sovereignty. *Masaryk University Journal of Law and Technology*, *17*(1), 33–85. https://doi.org/10.5817/mujlt2023-1-2

Takeda, H., Veerkamp, P., Tomiyama, T., & Yoshikawa, H. (1990). Modeling design processes. *AI Magazine*, *11*(4), 37–48.

Taylor, J. (2025, May 20). NSW education department caught unaware after Microsoft Teams began collecting students' biometric data. *The Guardian*. https://www.theguardian.com/australia-news/2025/may/19/nsw-education-department-caught-unaware-after-microsoft-teams-began-collecting-students-biometric-data

The Exchange Team. (2024, September 10). *Upgrading your organization from current versions to Exchange Server SE*. https://techcommunity.microsoft.com/blog/exchange/upgrading-your-organization-from-current-versions-to-exchange-server-se/4241305

The Exchange Team. (2025, April 14). *T-6 months: Exchange Server 2016 and Exchange Server 2019 End of Support*. https://techcommunity.microsoft.com/blog/exchange/t-6-months-exchange-server-2016-and-exchange-server-2019-end-of-support/4403017

Thijssen & Bruyning. (2025a, June). *Motie van de leden Thijssen en Bruyning over digitale autonomie en cloudopslag (Motie nr. 5 bij initiatiefnota «Wolken aan de horizon»)*. https://berthub.eu/tkconv/document.html?nummer=2025D25466

Thijssen & Bruyning. (2025b, June). *Motie van de leden Thijssen en Bruyning over Strategisch Leveranciersmanagement Autonome Cloud (Motie nr. 7 bij initiatiefnota «Wolken aan de horizon»)*. https://berthub.eu/tkconv/getraw/2025D25469

Thorne, B. (2025, February 25). Artificial Sanctions: Potential Implications of US Sanctions on the ICC's use of AI and Digital Evidence. *Opinio Juris*. https://opiniojuris.org/2025/02/25/artificial-sanctions-potential-implications-of-us-sanctions-on-the-iccs-use-of-ai-and-digital-evidence/

Timmers, P. (2019a). Challenged by "Digital Sovereignty". *Journal of Internet Law*, *23*(6), 12–20.

Timmers, P. (2019b). *Strategic autonomy and cybersecurity* (Policy in Focus). EU Institute of Security Studies. https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/RFt_Rvhh/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf

Timmers, P. (2021, July 23). Debunking Strategic Autonomy. *Directions Blog*. https://directionsblog.eu/debunking-strategic-autonomy/

Timmers, P. (2022, August 9). How Europe aims to achieve strategic autonomy for semiconductors. *Brookings*. https://www.brookings.edu/articles/how-europe-aims-to-achieve-strategic-autonomy-for-semiconductors/

Timmers, P. (2024). Sovereignty in the Digital Age. In H. Werthner, C. Ghezzi, J. Kramer, J. Nida-Rümelin, B. Nuseibeh, E. Prem, & A. Stanger (Eds.), *Introduction to Digital Humanism: A Textbook* (pp. 571–592). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45304-5_36

Tjong Tjin Tai, E., & Verbruggen, P. (2022). Onderzoeksmethoden in de rechtswetenschap: Over pluraliteit en vernieuwing. *Nederlands Juristenblad*, *2022*(1), 4–12.

Tretter, M. (2023). Sovereignty in the Digital and Contact Tracing Apps. *Digital Society*, *2*(1), 1–28. https://doi.org/10.1007/s44206-022-00030-2

Trigt, M. van. (2025). Microsoft bevestigt loskoppeling ICC-hoofdaanklager van diensten. *iBestuur*. https://ibestuur.nl/artikel/microsoft-bevestigt-loskoppeling-icc-hoofdaanklager-van-diensten/

U.S. Department of Justice. (2019). *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*. U.S. Department of Justice. https://www.justice.gov/criminal/media/999601/dl?inline

U.S. Department of State. (2025, June). *Imposing Sanctions in Response to the ICC's Illegitimate Actions Targeting the United States and Israel*. https://www.state.gov/releases/office-of-the-spokesperson/2025/06/imposing-sanctions-in-response-to-the-iccs-illegitimate-actions-targeting-the-united-states-and-israel/

van der Waal, S., Stikker, M., Kortlander, M., Van Eeden, Q., Demeyer, T., & Bocconi, S. (2021). *Digital European Public Spaces*. Waag. https://waag.org/sites/waag/files/2021-04/Waag%20Report%20on%20Digital%20European%20Public%20Spaces.pdf

Van der Wal, M. (2024). *On the Sovereignty of Dutch Government Data: How the National Cloud Policy Falls Short of Protecting Government Data Against Risks From Third Countries' Jurisdiction and Why This Matters* [Master Thesis, University of Amsterdam]. https://scripties.uba.uva.nl/search?id=c11345955

Van Dijck, J. (2021). Seeing the forest for the trees: Visualizing platformization and its governance. *New Media & Society*, *23*(9), 2801–2819. https://doi.org/10.1177/1461444820940293

van Dijck, J., & Jacobs, B. (2022, September 21). Opinie: Onze overheid moet haar kostbare data niet klakkeloos uitleveren aan Google en Amazon. *de Volkskrant*. https://www.volkskrant.nl/columns-opinie/opinie-onze-overheid-moet-haar-kostbare-data-niet-klakkeloos-uitleveren-aan-google-en-amazon~b57cb834/

van Dijck, J., Poell, T., & de Waal, M. (2016). *De Platformsamenleving: Strijd om publieke waarden in een online wereld*. AmsterdamAmsterdam University Press. https://dare.uva.nl/search?identifier=fa8f9dfa-3b16-41ef-b923-1acc74d769d5

van Eeten, M. J. G. van. (2006). Narrative Policy Analysis. In F. Fischer, G. J. Miller, & M. S. Sidney (Eds.), *Handbook of Public Policy Analysis: Theory, Methods, and Politics* (pp. 251–269). Taylor & Francis CRC Press.

van Hoboken, J., Arnbak, A., & van Eijk, N. a. N. M. (2013). *Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad* (SSRN Scholarly Paper 2276103). Social Science Research Network. https://doi.org/10.2139/ssrn.2276103

Van Trigt, M. (2024, March 28). Amsterdam wil onderzoek naar digitale onafhankelijkheid. *iBestuur*. https://ibestuur.nl/artikel/amsterdam-wil-onderzoek-naar-digitale-onafhankelijkheid/

Veale, M. (2023). *Denied by Design? Data Access Rights in Encrypted Infrastructures*. https://doi.org/10.31235/osf.io/94y6r

Vereniging van Nederlandse Gemeenten. (2017). *Local Government in the Netherlands*. https://www.vng-international.nl/sites/default/files/Local-Government_20170823.pdf

Vereniging van Nederlandse Gemeenten. (2020, November). *Statuten van de Vereniging van Nederlandse Gemeenten*. https://vng.nl/sites/default/files/2020-11/vng-statuten_20201111.pdf

Vereniging van Nederlandse Gemeenten. (2022, August 25). *Standaardisatie Haven en Haal Centraal-specificaties*. https://vng.nl/nieuws/bestuur-vng-verklaart-haven-tot-standaard

Vereniging van Nederlandse Gemeenten. (2023a). *Eindrapportage onderzoek Behoefte gemeentelijke cloudondersteuning*. VNG. https://vng.nl/sites/default/files/2023-12/eindrapportage-cbi-fase1-publicatie.pdf

Vereniging van Nederlandse Gemeenten. (2023b). *Rapportage behoefteonderzoek cloudondersteuning*. https://gce.scgemeenten.nl/wp-content/uploads/sites/2/2024/09/Bijlage-Rapportage-behoefteonderzoek-cloudondersteuning-Enquete.pdf

Vereniging van Nederlandse Gemeenten. (2024a). *Digitale Agenda Gemeenten 2028*. https://vng.nl/sites/default/files/2024-09/vng-digitale-agenda-gemeenten-2028.pdf

Vereniging van Nederlandse Gemeenten. (2024b, April). *Financieel Jaarverslag 2023*. Vereniging van Nederlandse Gemeenten. https://vng.nl/artikelen/financieel-jaarverslag-2023

Vereniging van Nederlandse Gemeenten. (2025a). *Rondetafelgesprek Digitale Afhankelijkheid*. https://gce.scgemeenten.nl/nieuws/vng-in-gesprek-met-tweede-kamer-over-digitale-soevereiniteit/

Vereniging van Nederlandse Gemeenten. (2025b, January 27). *GT en collectieve inkoop*. https://vng.nl/artikelen/gt-en-collectieve-inkoop

Vereniging van Nederlandse Gemeenten, Interprovinciaal Overleg, Unie van Waterschappen, & Rijksoverheid. (2011). *Bestuursakkoord 2011–2015*. Tweede Kamer der Staten-Generaal. https://zoek.officielebekendmakingen.nl/blg-110123.pdf

VNG Realisatie (Director). (2024, November 18). *Digitale Autonomie, een Duivels Dilemma—Uitvoeringscongres 2024* [Video recording]. https://www.youtube.com/watch?v=nmUIykem6jk

Vom Brocke, J., Hevner, A., & Maedche, A. (2020). Introduction to Design Science Research. In J. Vom Brocke, A. Hevner, & A. Maedche (Eds.), *Design Science Research. Cases* (pp. 1–13). Springer International Publishing. https://doi.org/10.1007/978-3-030-46781-4_1

Vonk, G. (Ed.) (with Klingenberg, A., Munneke, S., Tollenaar, A., & Vonk, Gijsbert). (2016). *Rechtsstatelijke aspecten van de decentralisaties in het sociale domein*. Rijksuniversiteit Groningen, Vakgroep Bestuursrecht & Bestuurskunde. https://pure.rug.nl/ws/portalfiles/portal/32021268/2016_decentralisaties_in_het_sociale_domein_full_text.pdf

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. *Information Systems Research*, *3*(1), 36–59. https://doi.org/10.1287/isre.3.1.36

Warren, T. (2024, January 12). Microsoft wants to automatically launch its Copilot AI on some Windows 11 devices. *The Verge*. https://www.theverge.com/2024/1/12/24035637/microsoft-windows-11-copilot-ai-chatbot-automatically-open-boot-startup

Williamson, O. E. (1998). Transaction Cost Economics: How It Works; Where It is Headed. *De Economist*, *146*(1), 23–58. https://doi.org/10.1023/A:1003263908567

Zijlstra, S. E. (2019). *Bestuurlijk organisatierecht* (2nd ed.). Wolters Kluwer. https://shop.wolterskluwer.nl/shop/boeken/bestuurlijk-organisatierecht-9789013130614

Appendix A: Interviewees

Table 8 characterizes the nine interviewees who participated in this research. Two interviewees are politicians and as such public figures. They explicitly agreed to having their name mentioned.

Table 8: List of interviewees

Interviewee	Relevance	Code
Member of the Dutch Parliament	Jesse Six Dijkstra is co-initiator of a parliamentary policy proposal on digital strategic autonomy of the central government. As such he possesses direct, knowledge of the motivations, arguments, and intended policy outcomes regarding digital strategic autonomy in the Netherlands, on the level of central government. This allows for a deeper understanding of the actors involved and the underlying concerns regarding digital strategic autonomy in general.	POL-NAT
Member of the Amsterdam City Council	Elisabeth IJmker is the initiator of a municipal policy proposal in the city of Amsterdam on the digital independence of the city. As such, she can provide further inside in considerations on the municipal level.	POL-MUN
Professor ESG Transformation and Digital Innovation	This interviewee has expertise in sourcing strategies of government organisations, including municipalities. As such, this interviewee can, both from a practical and theoretical perspective provide further insides in sourcing strategies which can contribute to digital strategic autonomy.	SCI
Director Public Affairs of the Dutch Cloud Community	This interviewee represents Dutch cloud providers and offers a perspective form the private sector on digital strategic autonomy. The interviewee is also co-author of a position paper on the topic on behalf of the sector.	COM
Product Owner Cloud Engineering & Enablement Wigo4it	This interviewee is employed at a Shared Service Centre of the four largest municipalities in the Netherlands (G4). As such, the interviewee provides a more technical perspective on digital strategic autonomy. Furthermore, Wigo4it uses services from a US cloud service provider, who promotes Wigo4it as a success case (Microsoft, 2022). Therefore, the interviewee can provide insights into the benefits of using US cloud service providers.	ENG-SSC
Employees at VNG	Multiple employees of the Vereniging van Nederlandse Gemeenten were interviewed to provide insights on the perspective of both VNG as the association of	GOV-VNG-1, GOV-VNG-2, GOV-VNG-3

	municipalities and individual municipalities on digital strategic autonomy.	
Employees at AMS Institute and Amsterdam	A focus group was held with employees at the scientific institute AMS and the city of Amsterdam working on science-based solutions for metropolitan regions like Amsterdam. AMS has developed a beta procurement tool for municipalities to safeguard autonomy (AMS Institute, 2024). As such, the interviewees could further provide a perspective on digital strategic autonomy from a municipal perspective.	GOV-AMS

Appendix B: Informed Consent Form

Here we present the informed consent form, which we developed based on a discussion with the data steward of the TU Delft and was approved by the TU Delft human research ethics committee. All participants agreed to these terms of the research.

B.1 Informed Consent Form

Informed Consent Form voor een interview in het kader van het onderzoek *Digital Strategic Autonomy of Dutch Municipalities*

U werd uitgenodigd om deel te nemen aan een onderzoek genaamd *Digital Strategic Autonomy of Dutch Municipalities*. Dit onderzoek wordt uitgevoerd door Machiel van der Wal van de TU Delft, onder begeleiding van Prof. dr. ir. Nitesh Bharosa.

Het doel van dit onderzoek is het begrip 'Digitale Strategische Autonomie' te conceptualiseren en operationaliseren voor Nederlandse gemeentes om vervolgens een quick-scan te ontwerpen. Het interview zal gebruikt worden voor een masterthesis die wordt gepubliceerd in de TU Delft Repository en een eventuele publicatie in andere vorm. U bent gevraagd om uw kennis en mening te delen over digitale strategische autonomie/digitale soevereiniteit.

U heeft voorafgaand aan het interview toestemming gegeven om deze op te nemen en te transcriberen. Het transcript wordt aan u voorgelegd voor eventuele correcties. Na goedkeuring zal de opname van het interview worden verwijderd. Het transcript wordt niet integraal gepubliceerd. Wel kunnen quotes worden opgenomen in de thesis en zal een codebook worden opgenomen in de bijlage.

Uw functie en organisatie zullen in overleg in geaggregeerde/gepseudonimiseerde vorm worden genoemd in de thesis (bijvoorbeeld: senior beleidsmedewerker bij een middelgrote gemeente), tenzij we iets anders afspreken. De gepseudonimiseerde transcriptie en uw contactgegevens worden ten hoogste 2 jaar bewaard na de publicatie van de thesis.

Wij doen ons best om uw antwoorden vertrouwelijk te houden. We minimaliseren de risico's door gebruik te maken van de adequaat beveiligde OneDrive van de TU Delft voor de opslag van alle gegevens. Alleen Machiel van der Wal en Nitesh Bharosa hebben toegang tot deze OneDrive.

Uw deelname aan dit onderzoek is volledig vrijwillig, en u kunt zich elk moment terugtrekken zonder reden op te geven. U bent vrij om vragen niet te beantwoorden.

De contactgegevens van de onderzoekers voor verdere informatie en vragen:
Machiel van der Wal,
Nitesh Bharosa

Appendix C: Interview questions

In this appendix, we present an English translation of the predefined list of interview questions, see also Section 2.4.1. The interviews themselves were conducted in Dutch. This list formed the core of each interview. We added additional questions before each interview, depending on the expertise of the interviewee.

C.1 Interview questions (translated)

Introductory Questions

1. [Question about the profession and background of the interviewee]
2. Have you seen digital autonomy become more important in your work, and if so, how?

Conceptual questions

3. What does the concept of digital strategic autonomy mean to you?
4. How do you see terms such as digital sovereignty, digital strategic autonomy, and open strategic autonomy relating to each other?
5. What do you see as the consequences and risks of these dependencies for the government/municipality?
6. Do you see any examples of dependencies that are already problematic?

Questions on possible Solutions

7. In your opinion, what is the best strategy for municipalities to become more autonomous
8. What actions should municipalities take now?
9. What do you see as the biggest challenges and barriers for governments to become more autonomous?
10. What do municipalities need according to you?
11. How do you view the relationship between municipalities, the VNG and the central government in this regard?

Questions about the self-assessment tool

12. Do you have suggestions for indicators or elements I should include in a self-assessment for the state of digital strategic autonomy in a certain municipal process?

Other Questions

[Here, questions specific to the expertise of the interviewee were added]

Conclusion

13. Is there anything important we haven't discussed yet, but that you think is relevant to this topic?
14. Are there any other respondents you would recommend?

Appendix D: Codes and their groundedness

Here we present the codes that we used during the analysis of the interview transcripts, including the groundedness of each code in Table 9. This number refers to the amount of times a code has been applied. The codes are divided into six groups: definition, drivers for cloud (adoption), indicators (for digital strategic autonomy), obstacles for municipalities (with regards to improving digital strategic autonomy), problem (with regards to a low digital strategic autonomy) and solution (to improve digital strategic autonomy). The code in each row is indicated with a ○ **.** The other columns show the structure of the codes. For example, the code 'Data' is a subcode to Technology, which is part of the Definition category. The groundedness of this code then shows how many times a respondent specifically mentioned digital strategic autonomy being specifically about data. Figure 14 presents a tree with the categories and corresponding codes.

Table 9: Codes and groundedness

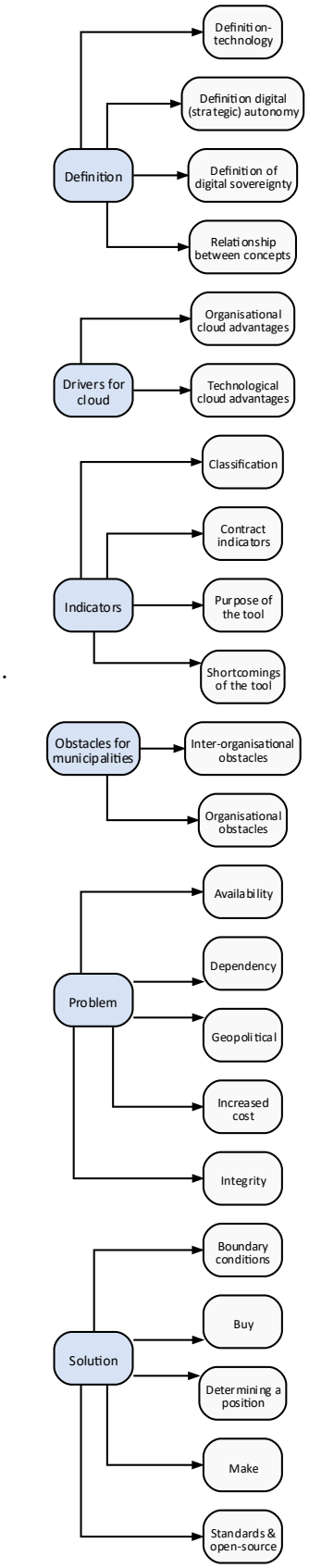
Code			**Grounded**
○ **Definition**			35
Definition	○ Definition - technology		13
Definition	Definition - technology	○ Artificial Intelligence	1
Definition	Definition - technology	○ Critical infrastructure	2
Definition	Definition - technology	○ Data	4
Definition	Definition - technology	○ Identities	1
Definition	Definition - technology	○ Whole stack	5
Definition	○ Definition digital (strategic) autonomy		11
Definition	Definition digital (strategic) autonomy	○ Capabilities	4
Definition	Definition digital (strategic) autonomy	○ Capacities	2
Definition	Definition digital (strategic) autonomy	○ Control	8
Definition	○ Definition of digital sovereignty		6
Definition	Definition of digital sovereignty	○ Binary	1
Definition	Definition of digital sovereignty	○ Connected in international and european contexts	1
Definition	Definition of digital sovereignty	○ Hijacked terminology	2
Definition	Definition of digital sovereignty	○ Previously: GDPR-compliance	1
Definition	Definition of digital sovereignty	○ Who has the last word?	1
Definition	○ Relationship between concepts		6

Definition	Relationship between concepts	○ Connotation with municipal autonomy	1
Definition	Relationship between concepts	○ Interchangeable	2
Definition	Relationship between concepts	○ No consensus on definition	3
○ **Drivers for cloud**			16
Drivers for cloud	○ Organizational cloud advantages		9
Drivers for cloud	Organizational cloud advantages	○ Avoiding responsibility	1
Drivers for cloud	Organizational cloud advantages	○ Business continuity	1
Drivers for cloud	Organizational cloud advantages	○ Cost reduction	4
Drivers for cloud	Organizational cloud advantages	○ CSP Knowledge	1
Drivers for cloud	Organizational cloud advantages	○ Flexibility	1
Drivers for cloud	Organizational cloud advantages	○ Less vendor lock-in compared to own data centres	1
Drivers for cloud	○ Technological cloud advantages		7
Drivers for cloud	Technological cloud advantages	○ Automatic compliance check	2
Drivers for cloud	Technological cloud advantages	○ CSP Data localisation	1
Drivers for cloud	Technological cloud advantages	○ Security advantages	4
○ **Indicators**			10
Indicators	○ Classification		5
Indicators	Classification	○ Critical processes	2
Indicators	Classification	○ Data classification	1
Indicators	Classification	○ Sub-vendors	2
Indicators	○ Contract indicators		2
Indicators	Contract indicators	○ Contracting	1
Indicators	Contract indicators	○ Technical agreements	1
Indicators	○ Purpose of the tool		1
Indicators	Purpose of the tool	○ Indicate why it should be a priority	1
Indicators	○ Shortcomings of the tool		2
Indicators	Shortcomings of the tool	○ Note the level of analysis	2
○ **Obstacles for municipalities**			49
Obstacles for municipalities	○ Interorganizational obstacles		18
Obstacles for municipalities	Interorganizational obstacles	○ Decentralized decision making	8
Obstacles for municipalities	Interorganizational obstacles	○ Dependency municipalities on central government	1

Obstacles for municipalities	Interorganizational obstacles	○ Difference between gov orgs	1
Obstacles for municipalities	Interorganizational obstacles	○ Difference between municipalities	2
Obstacles for municipalities	Interorganizational obstacles	○ Difference gov org and businesses	1
Obstacles for municipalities	Interorganizational obstacles	○ Framework agreement	1
Obstacles for municipalities	Interorganizational obstacles	○ Mainly SaaS	3
Obstacles for municipalities	Interorganizational obstacles	○ Standards are too soft in practice	1
Obstacles for municipalities	○ Organizational obstacles		31
Obstacles for municipalities	Organizational obstacles	○ Lack of awareness	3
Obstacles for municipalities	Organizational obstacles	○ Lack of capacity	2
Obstacles for municipalities	Organizational obstacles	○ Lack of control	3
Obstacles for municipalities	Organizational obstacles	○ Lack of information	6
Obstacles for municipalities	Organizational obstacles	○ Lack of knowledge	11
Obstacles for municipalities	Organizational obstacles	○ Lack of resources	2
Obstacles for municipalities	Organizational obstacles	○ No gap analysis	2
Obstacles for municipalities	Organizational obstacles	○ Not an end in itself to leave US Cloud	1
Obstacles for municipalities	Organizational obstacles	○ Procurement	3
Obstacles for municipalities	Organizational obstacles	○ Tender written with CSP in mind	1
Obstacles for municipalities	Organizational obstacles	○ Tight labour market	1
Obstacles for municipalities	Organizational obstacles	○ Wet markt en overheid	1
○ **Problem**			31
Problem	○ Availability		7
Problem	○ Dependency		2
Problem	○ Geopolitical		19
Problem	Geopolitical	○ Changing geopolitical situation	7
Problem	Geopolitical	○ Confidentiality	5
Problem	Geopolitical	○ Third country jurisdiction and data location	7

Problem	○ Increased cost		1
Problem	○ Integrity		2
○ **Solution**			32
Solution	○ Boundary conditions		10
Solution	Boundary conditions	○ Encryption	5
Solution	Boundary conditions	○ Exit strategy	4
Solution	Boundary conditions	○ Risk analysis	1
Solution	○ Buy		7
Solution	Buy	○ Enable business case	1
Solution	Buy	○ Government as launching customer	1
Solution	Buy	○ Knowledge sharing	1
Solution	Buy	○ One-stop shop	1
Solution	Buy	○ Public-private partnership	1
Solution	Buy	○ Sourcing life cycle	2
Solution	○ Determining a position		4
Solution	Determining a position	○ One govt approach	2
Solution	Determining a position	○ Taking a stance	2
Solution	○ Make		5
Solution	Make	○ Government cloud service(s)	3
Solution	Make	○ Government provides infra	2
Solution	○ Standards and open-source		6
Solution	Standards and open-source	○ Bijenkorf megascaler	1
Solution	Standards and open-source	○ Commonground hosting	1
Solution	Standards and open-source	○ Open Source	2
Solution	Standards and open-source	○ Standard setting	1
Solution	Standards and open-source	○ VNG Haven	1

Figure 14: Codes tree



Appendix E: Formal Chart

In this appendix we present the formal chart. Enserink et. al (2022) describe a basic procedure for actor analysis which covers six steps, of which we will follow the first three steps. Firstly, we formulate the problem and the associated decision arena. Then, we identify the actors involved. Lastly, we map the formal institutional playing field.

E.1 Problem Formulation and problem owner

Firstly, the problem owner is Dutch municipalities. Presently (summer 2025), the Netherlands has 342 unique different municipalities, varying widely in size and population. However, they have a set of tasks that is essentially similar or the same for all municipalities. Currently, Dutch municipalities are largely dependent on US cloud service providers for the provisioning of cloud services, including the hosting of data and the provisioning of applications (Software as a Service) which enable and shape public service provisioning. This raises concerns about the availability and confidentiality of data and services, and over the protection of public values. The gap between the current and the desired situation is the lack of control over IT providers in general, and specifically regarding US cloud service providers. Municipalities often have limited resources and a lot of (other) tasks, and have a limited size compared to IT-providers.

E.2 Identify actors involved

A brainstorm was held regarding the actors involved in the decision arena that is in scope for this thesis. We used the techniques suggested by the methodology, namely to follow an interest-based approach, an institutional approach and a reputational approach (via the interviews held). For composite actors (such as the United States), we included different units of the actor when they have different objectives and/or responsibilities. The list of actors is presented in Table 10.

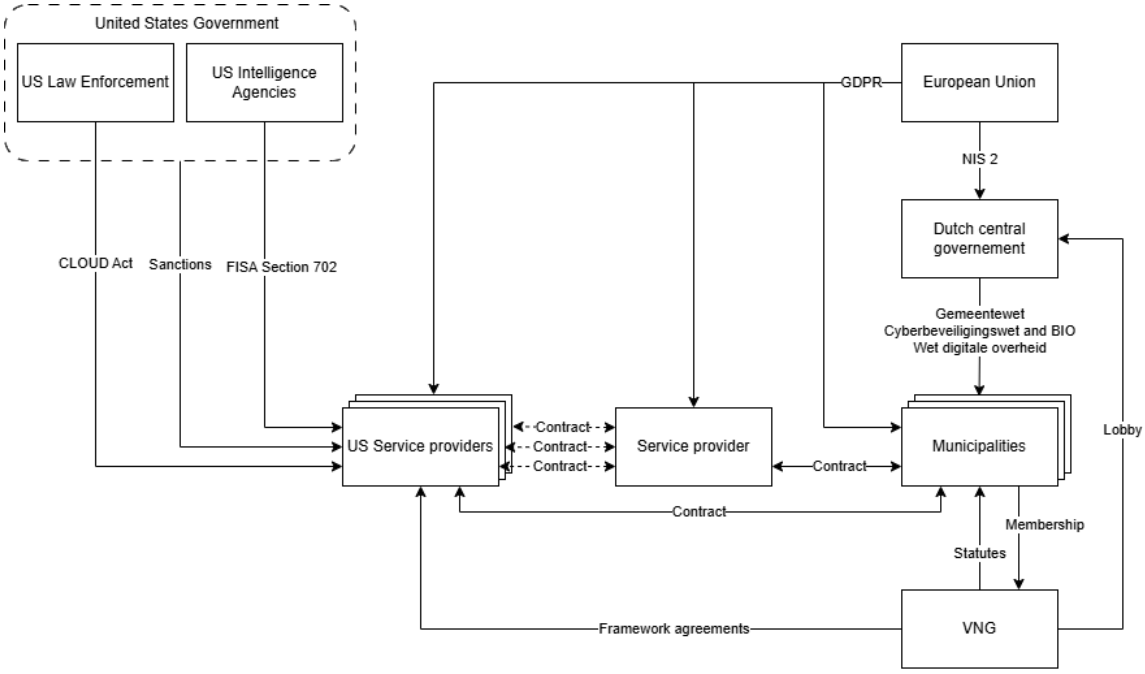
Table 10: List of actors

Actor
European Union
US Government
US Intelligence Agencies
US Law Enforcement
Dutch central government
342 Dutch municipalities
Vereniging van Nederlandse Gemeenten
US service providers
Service providers

E.3 Formal chart

Because formal institution influence the (possible) interactions between actors, a formal chart is drawn. Actors are placed on the chart roughly according to their formal hierarchy. The labels on the arrows indicate the formal relationship between the corresponding actors. The formal chart is presented in Figure 12.

Figure 15: Formal chart



As can be seen from the formal chart, municipalities rely on service providers based on contracts. Some service providers, however, fall under foreign jurisdiction of the US, with different types of legislation applying. This is not the case for other service providers, but these other service providers themselves can depend on these US service providers.

The VNG is an association of public law bodies, and not a government organization. As such, it is placed below the municipalities. The municipalities, as members, have influence over the actions and goals of the VNG. Because municipalities are members, the VNG can by its statutes influence the actions of municipalities, limited by the internal association structure (sanctions by the VNG only apply internally).

The formal chart is further explained throughout the thesis. Dotted arrows refer to *possible* formal relationships - as a service provider often depends on many sub-providers. The CLOUD Act, US Sanctions and FISA Section 702 are explained in Section 5.5. 'US Service providers' refer to service providers over which the US claims jurisdiction, see the same section. The position of the VNG vis-à-vis municipalities is explained in Section 6.1.1. Attention to the GDPR, to NIS 2 and the BIO and to the Wet digitale overheid is given in Sections 7.3-7.5 respectively. Framework agreements are discussed in Section 7.2.4.

Appendix F: Existing assessment tools

In this appendix, we describe two existing tools for assessing the digital strategic autonomy of a government organisation. We describe the context and purpose of each tool and discuss the relevance for the self-assessment tool which is developed in Chapter 6 of this thesis.

F.1 'MOT-certification for digital autonomy in the smart city'

The scientific branch of the Dutch social liberal party D66 has developed a 'MOT-certification for digital autonomy in the smart city' (De Vries, 2022). The tool, which is presented in Table 11 and draws inspiration from Groeneveld and Timmersmans (2021), formulates thirteen yes/no statements which can be used to test the 'democratic grip' of the municipal administration, which is seen as the municipal executive (College van B&W) and the municipal council (gemeenteraad).

Table 11: MOT-certification for digital autonomy by De Vries (2022, p. 26-27)

#	Statement
1	The municipal council has a Digital Affairs committee.
2	The municipal executive has an alderman responsible for the Digital Affairs portfolio.
3	The municipal executive has a public overview of all smart city applications, including explanations of which data is collected by which parties, and for what purpose.
4	The municipal executive has conducted a Data Protection Impact Assessment for each of these applications, and shared it with the municipal council.
5	The municipal executive has a public sensor register.
6	The municipal executive has a public algorithm register.
7	The municipal executive commissions an annual audit by an independent organization of the software and digital infrastructure that are part of smart city applications.
8	The municipal executive has an overview of contracts concluded in the context of smart city projects and with which companies, and has shared this with the municipal council.
9	The municipal executive has an overview of contracts with companies for smart city applications that are on a subscription basis, and has shared this with the municipal council.
10	The municipal executive has stipulated in contracts with companies for smart city applications that it has access to all collected data.
11	The municipal executive has made clear agreements about what companies may and may not do with the collected data in the context of smart city applications.
12	The municipal executive has established the exit strategy when procuring smart city applications, and has shared this with the municipal council.
13	The municipal executive has included requirements for technical and procedural transparency and explainability in contracts with software suppliers.

As the purpose of the tool is to test the democratic grip, many of the statements concern the transparency and accountability of the municipality itself. For example, the establishment of a public sensor register (statement 5) and a public algorithm register (statement 6) serve transparency. They

increase the visibility of which sensors and algorithms are deployed in the municipality. This supports public scrutiny and democratic oversight. However, transparency does not necessarily enhance digital strategic autonomy. The existence of such registers does not, by itself, increase the municipality's capabilities (knowledge, skills, tools), capacity (resources), or control (influence over decisions and actions) regarding these digital systems. A municipality may be fully transparent about its use of externally managed, proprietary algorithms or sensors, but if it lacks the expertise, resources, or contractual leverage to influence their design, operation, or data flows, its digital strategic autonomy remains limited.

Statement 1 and 2, on a Digital Affairs committee and an alderman with this portfolio can say something about the capabilities and capacities of a municipality, depending on i.a. the expertise, mandate and budget for these actors. Statement 7 on auditing, statement 10 on contractual agreements on data access, statement 11 on contractual agreements on data use, statement 12 on an exit strategy and statement 13 on technical and procedural transparency and explainability from suppliers all concern the control of a municipality.

Overall, the scope of the tool is 'high-over', not with relation to a specific process or on specific stack layers, nor is a distinction made between capabilities, capacities and control. This does, however, improve the usability of the tool, because less specialized knowledge is needed by a municipal employee. The yes/no questions further improve usability by a general audience.

F.2 Netherlands Court of Audit

The Netherlands Court of Audit (2025) has recently published a report on the cloud use by the Dutch central government and its cloud policy. Out of the 1588 cloud services that were in scope, 44% were public cloud services, 30% were private cloud services (e.g. in a government data centre) and 26% of the services was (notably) unknown. Furthermore, for 67% of the public cloud services that are vital to an organisation's primary task, not one risk assessment was conducted. With reference to the definition of digital strategic autonomy as followed in this thesis, the authors define this as *"the ability to take autonomous decisions and actions on essential digital aspects of the economy, society and democracy"* (Netherlands Court of Audit, 2025, para. 3.4).[93] The Court of Audit (2025, pp. 5–6) concludes that the Dutch central government has limited inside into is cloud use, does not make appropriate strategic risk assessment and that the audited contracts do not adequately safeguard digital strategic autonomy.

The Court of Audit established an audit framework to answer the question to which extend three selected public cloud contracts of central government organisations safeguard digital strategic autonomy (and business continuity and data protection). The part of the audit framework focussing on digital strategic autonomy is presented in Table 12.

Table 12: Audit framework to assess the digital strategic autonomy of public cloud contracts (Netherlands Court of Audit, 2025, pp. 65–67)

#	Control domain	Criteria
1	Contract closure	Conclusion of the contract was preceded by a risk assessment. The contract states who is responsible at the

[93] The Netherlands Court of Audit refers to this as 'digital sovereignty' or 'sovereignty' in the context of their report.

		CSC [Cloud Service Customer] and the CSP [Cloud Service Provider] for contract management.
2	Interoperability and portability	Interoperability and portability are included in the cloud service agreement, with agreements established for: a. roles and responsibilities of the CSP and the CSC on interoperability and portability; b. interoperability of data exchange and processing; c. portability of cloud systems.
3	Interoperability and portability	CSCs' access to data upon contract termination are included in the cloud service agreement and include: a. data format in accordance with Open Standards; b. time period during which data will be stored; c. scope of data stored and made available to CSCs; d. data deletion policy; e. encryption of the export file.
4	Interoperability and portability	The CSP must ensure and demonstrate that the CSC's data from its systems and each subprocessing system is transferable to other CSPs within the time and format agreed upon in the cloud service agreement, at the CSC's option.
5	Disclosure Notification	The procedure for managing and responding to requests for disclosure of personal data by law enforcement authorities in accordance with applicable laws and regulations has been established by the CSP and communicated to the CSC. In doing so, the CSP highlights the notification procedure to interested CSCs unless otherwise prohibited, such as a prohibition under criminal law to maintain the confidentiality of a law enforcement investigation
6	Data Location and Data Flow	- The CSC identifies geographic areas of regulatory risk, such as embargoed countries. - The CSP has defined procedures and measures to specify and document the physical locations of data, including locations where data is processed or backed up. - The CSP transfers data from the CSC to a country outside the European Economic Area only if agreed as part of the Cloud Service Agreement. - Documentation on data flows are in place to determine what data are processed, stored or transmitted where.
7	Right to audit	Procedures related to audits requested by the CSC are defined, documented and transparently communicated to the CSC and, if applicable, the mandated auditor.

The audit framework is quite specific and designed to be applied by specialists, i.e. professional auditors. The different element can however serve as inspiration for the self-assessment framework in this thesis. The scope of the framework is a specific contract. As such, the indicators focus on the control a government organisation has over de cloud service provider and its processing, and not so much on the capabilities (knowledge, skills, tools) and capacity (resources) of the organisation itself.

Criterium 1 is a notable exception, and focusses on conducting a risk assessment before a contract is concluded. The ability to perform such an assessment will depend on capabilities and capacities. This conclusion is also supported by a similar report from the Central Government Audit Service (2025): *"In all cases studied, the picture is that the process of risk assessment places a heavy burden on available knowledge and capacity. The question here is to what extent implementation of risk assessment will be sufficiently scalable in the future as more IT services are moved to the public cloud"* (p. 12). Furthermore, similar assessments could lead to different outcomes because of a different risk appetite. Lastly, the Audit Service suspects that government organisations are duplicating work in this way. We can assume that the same conclusions can be drawn for municipalities. As such, this serves as a driver for pooling capacities and capabilities and serves as an argument for the strategic partnership approach as compared to a risk management approach, see Section 3.3.2.