Report

Collaborative ecosystem development as an approach to facilitate digital strategic autonomy

Authors
Gijs van Houwelingen PhD
Nick Oostervink PhD

October 2025

TNO 2025 R12054

TNO Vector
Centre for Societal Innovation and Strategy

Contents

Executive Summary

Nation-states are now increasingly recognizing a fundamental challenge: to maintain reasonable control over their critical technology supply chains—including defense, cybersecurity, and semiconductors—they cannot rely solely on industries that include foreign companies or firms with ties to adversarial nations like Russia and China. This shift reflects growing concerns about supply security and the potential risks of technological dependence in an era of heightened international competition. Policymakers worldwide are therefore increasingly prioritizing digital strategic autonomy (the need for both governments and businesses to maintain control over the design, production, supply chains, and use of critical technologies) as a key policy response to current geopolitical tensions.

At the same time, achieving digital strategic autonomy faces significant structural challenges. Much of the required expertise, capacity, and capabilities for ensuring sufficient domestic supply of critical technologies firmly reside within the private sector. However, **domestic suppliers often face a fundamental market problem**: it is often hard to compete with cheaper foreign alternatives, and their domestic markets are frequently too small to achieve the economies of scale needed for viability.

The impetus for this paper stems from recognizing that in many technological domains **governments critically need private sector support to achieve strategic autonomy**. While governments possess policy tools and procurement budgets, they typically lack the technical expertise, innovation capacity, and speed needed to develop cutting-edge technologies in-house. Meanwhile, domestic private companies have the expertise but face high barriers to entry and insufficient market scale. This creates a dependency gap that only active reciprocal collaboration between State(s) and industry can bridge.

To ensure that critical domestic industries can reliably deliver essential digital products and services, governments must move beyond buyer-vendor relationships toward robust public-private partnerships. These partnerships are crucial for guaranteeing security of supply, preventing foreign takeovers, and addressing personnel capacity limitations.

Our core message is: **Governments should take ownership over the initiation and orchestration of flourishing public-private ecosystems that help cultivate the domestic security of supply**. Even though public-private partnership ecosystem orchestration capacity is just one piece of the puzzle needed to achieve strategic digital autonomy, it is a crucial piece. It is this capacity that helps governments move beyond the central tension in striving for digital strategic autonomy when it comes to dealing with industry partners: How to build strong domestic capabilities and maintain control and a sense of "grip" over the supply chain.

In this paper, we propose a strategic framework for collaborative ecosystem orchestration that strengthens strategic digital autonomy while creating sustainable value for all stakeholders in order to support both policy makers and business makers in navigating the complex trade-offs that lead to increasing strategic digital autonomy.

The core takeaways from this paper include:

- **Public-private collaborations are a key tool for achieving strategic digital autonomy**. For many technological domains, governments need to rely on private sector expertise and capabilities to achieve strategic digital autonomy quickly. In such instances, public-private collaboration is key.
- **Invest in co-creation.** Both policymakers and industry leaders must be ready to invest in building collaborative ecosystems through co-creative process such as collaborative business modeling.
- **Aligning public and private interests is crucial.** For the industry to effectively contribute to Nation state's digital autonomy, governments and businesses need to carefully configure and align their (often symbiotic) business models.
- **Collaborative business modeling (CBM) helps building resilient ecosystems**. This iterative process, founded on trust and relational principles like long-term commitment, shared responsibility, and transparency, balances public needs for value chain control and security of supply with the private sector's need for certainty and a clear business case for the involved industry.

1. Introduction: Managing key tensions

In recent times the global pursuit for digital strategic autonomy has emerged as a defining characteristic of national policy agendas. Governments worldwide increasingly recognize that control over digital infrastructures, data governance, and critical technologies is fundamental for economic resilience, political independence, and in general societal trust. From artificial intelligence and cloud computing to semi-conductors and cybersecurity, information technology now underpins national sovereignty. This shift towards enhanced supply chain security and greater overall control is evident in the European Union's pursuit of "*open strategic autonomy*", the United States' initiatives to reshore semiconductor production, and China's continued investment in digital self-reliance. These collective efforts underscore a growing consensus: **digital dependencies can readily evolve into geopolitical vulnerabilities**. And as geopolitical situations develop there can be situations in which nation states can be faced with the consequences of these vulnerabilities (e.g., when Denmark found unexplainable Chinese components in its national supply network[1]). Consequently, states are prioritizing investments in domestic capabilities, establishing regulatory standards, and endeavoring to shape global norms concerning data, algorithms, and digital platforms.

While there are many different definitions of digital strategic autonomy, here we follow Van Veenstra & Stolwijk (2025)'s recent definition:

> "Digital strategic autonomy means having control over the design and use of (business-) critical digital systems, algorithms, and the data that is generated and processed through them." [2]

This definition highlights the fact that digital strategic autonomy is far from a theoretical or abstract concept. Instead, it **directly informs and necessitates concrete actions and strategies by governments**. Control over the design and use of business-critical systems, algorithms and data implies that governments have some say how essential digital infrastructure, software, and hardware are developed, produced, deployed, and operated. This may necessitate policies regarding promotion of, or even mandating, domestic development, setting standards for foreign technologies, or even restricting the use of certain foreign systems if control cannot be assured. Also, an earlier paper from Stolwijk et al. (2022) makes clear that policy makers cannot just focus on software or hardware in isolation, but need to take into account the whole technology stack for any given application landscape (e.g., AI-driven technologies; see also van Veenstra & Stolwijk, 2025).

One reality remains irrefutable: The required infrastructure, innovation, and expertise for constructing and sustaining sovereign digital systems largely reside within the private sector. Commercial entities, including cloud providers, chip manufacturers, cybersecurity firms, and AI developers, are responsible for designing, deploying, and operating the technologies upon which states depend. These companies, in turn, are driven by market dynamics, necessitating profitability, shareholder satisfaction, and competitive-ness within a rapidly evolving global economy. Hence, in many countries and for many technological domains, regulation or diversification of supply will *not* deliver digital strategic autonomy on its own. **Real progress is possible by harnessing the collective capabilities, resources, and incentives of both the public and private sectors**.

1.1 The tension: Avoiding vendor lock-in while ensuring security of supply and achieving grip

One major key challenge in advancing digital strategic autonomy that we address in this paper lies in actively managing two intertwined risks: **vendor lock-in** (i.e., the unhealthy dependence on a limited number of suppliers for critical technologies), and **lack of security of supply** (i.e., when the continued availability, integrity, and confi-dentiality of essential digital components and capabilities cannot be not assured). These risks are often compounded by the globalization of value chains, making it difficult to guarantee both technological independence and resilience. This complex balancing act highlights the necessity for a new approach that can surface and resolve these trade-offs collaboratively—beyond what government policy alone can achieve.

Traditional procurement strategies are focused on formal transactions: they emphasize supplier diversification as a risk mitigation tool, operating under the assumption that multiple viable alternatives exist within acceptable risk parameters.

1 Unexplained components found in Denmark's energy equipment imports, industry group says | Reuters
2 https://www.tweedekamer.nl/downloads/document?id=2025D17099

However, when strategic digital autonomy is the objective, this conventional wisdom faces critical limitations. For highly specialized or emerging technologies—particularly those involving critical infrastructure, advanced semiconductors, quantum computing, or AI systems—the global supplier base is often concentrated among a small number of predominantly foreign entities. In these contexts, **diversification strategies may inadvertently increase strategic vulnerability rather than reduce it**.[3] While spreading risk across multiple foreign suppliers may help mitigate supply risks, it can simultaneously expand the potential (control) points of failure and even attack in the supply chain, multiply regulatory compliance challenges, and create dependencies on multiple foreign jurisdictions with potentially conflicting geopolitical interests.

Furthermore, the domestic industrial base for such technologies is often characterized by capability gaps that cannot be addressed through traditional market mechanisms alone, requiring coordinated public-private partnerships, strategic investments in R&D infrastructure, and long-term industrial policy commitments that extend beyond conventional procurement timelines.

Hence, **diversification does not inherently confer the degree of strategic influence or oversight that governments require** over business- or even mission-critical processes and technologies required for digital strategic autonomy, especially in highly dynamic technological domains. This is because diversification typically diminishes a supplier's dependence on governmental procurement, thereby rendering them more susceptible to broader market dynamics and ultimately eroding the government's strategic leverage. Indeed, technology suppliers of mission-critical digital infrastructure, hardware, software, or services that receive comparatively limited governmental support may be compelled to seek foreign investment, which subsequently compromises domestic ownership and consequently their utility from a strategic autonomy perspective.

1.2 So how to navigate this tension to achieve digital strategic autonomy?

To achieve digital strategic autonomy, policymakers must navigate a series of complex trade-offs. They must balance the government's imperative to avoid overreliance on a limited number of suppliers (i.e., **vendor lock-in**) with the need to maintain control over crucial industries and ensure sustained governmental support and procurement for domestic suppliers. A solution can be found in new forms of **public-private collaboration** that extend beyond mere procurement and compliance, fostering shared responsibility for the digital future. In this evolving landscape, autonomy is not merely about control; it encompasses cooperation with industry, trust, and the collective ability to shape technology in the public interest.

Our aim in this paper is to equip both government and industry decision-makers with a strategic framework for collaborative ecosystem orchestration that strengthens strategic digital autonomy while creating sustainable value for all stakeholders. Specifically, we seek to demonstrate how coordinated business modeling approaches can transcend traditional transactional relationships to build resilient, innovation-driven ecosystems that serve both commercial viability and strategic national interests.

This paper addresses a critical gap in current policy and business practice: while governments increasingly recognize the limitations of traditional procurement diversification for achieving strategic autonomy, and while industry acknowledges the risks of excessive foreign dependencies, both sectors often lack practical frameworks for effective collaboration.

1.3 Collaborative ecosystem orchestration as a possible solution

Building on TNO's scientifically grounded and validated collaborative business modelling expertise, the collaborative ecosystem approach we describe in the rest of the paper offers significant promise to address the aforementioned dilemma between vendor lock-in versus the need for control and grip. By bringing together diverse stakeholders across the value chain, from both public and private parties, this framework does more than align industry incentives with strategic policy aims: it enables transparent, iterative exploration of value chain design choices, risk mitigation strategies, and mutually beneficial paths to digital strategic autonomy. By interweaving policy goals and business drivers, collaborative business modeling empowers governments and industry alike to navigate the delicate trade-offs inherent to digital strategic autonomy, forging partnerships equipped to secure our digital future.

Put differently: if nation states depend on private parties, and those private parties depend on the public sector for demand and income, we identify a collaborative way forward where both public and private parties receive the certainty they require (i.e. certainty of supply and sufficient revenue, respectively).

3 Farrand, B. (2025). The economy–security nexus: Risk, strategic autonomy and the regulation of the semiconductor supply chain. *European Journal of Risk Regulation*, 16(1), 279-293.

The following chapter analyzes several exemplary cases where public-private partnerships moved beyond transactional interactions to create collaborative ecosystems that delivered both strategic autonomy and commercial value. These cases serve as more than illustrations—they are the empirical foundation from which we derived our collaborative business modeling framework. Our systematic analysis of these successful partnerships identified the key design principles, governance mechanisms, and value-creation models that enable governments and industry to align their interests while maintaining their respective strategic objectives. The patterns and success factors revealed by these cases directly informed the frameworks and tools presented in later sections of this paper.

2. Examples of successful collaborative approaches for strategic digital autonomy

In the journey to identify strategies to cope with these earlier mentioned tensions we identified several existing and developing projects that provide promising exemplary handles to come to new public-private collaborations. Specifically, we identified four cases that highlight why a more collaborative approach to government-industry interactions, in contrast to the traditionally more transactional approach, delivers results that are crucial for digital strategic autonomy.

2.1 Open source as an approach to reduce dependencies on individual(ly owned) standards

Open source software (OSS) has emerged as a pivotal enabler of digital strategic autonomy, offering transparency, adaptability, and a reduction in vendor lock-in. Its collaborative development model not only accelerates innovation but also leverages the collective expertise of a global community to scrutinize and improve code—commonly referred to as the "many eyes" effect. This approach has proven especially valuable for foundational digital infrastructure, including operating systems, development tools, and middleware, where open-source solutions empower organizations and nations to build robust digital capabilities with greater control over underlying technologies.[4] [5] The shared ownership and collective advancement intrinsic to open source make it a compelling component of strategies aimed at fostering digital independence.

For example, though broader in scope, the EuroStack initiative exemplifies the promise of open-source software for digital strategic autonomy by actively building a European digital stack based on transparency, collaboration, and interoperability. Through its focus on open-source technologies and European-led development, EuroStack seeks to empower organizations and public administrations with greater control over their digital infrastructure, while reducing dependence on external vendors and aligning with European regulatory and ethical standards. By fostering a vibrant ecosystem where public and private sectors can jointly develop, maintain, and audit critical digital solutions, EuroStack demonstrates how open source can serve as a strategic asset for achieving digital independence—while also offering a model for collective action and innovation that safeguards Europe's technological future.[6]

However, while open source delivers significant benefits, it does not inherently guarantee digital strategic autonomy, particularly for technologies critical to national security. The transparency that strengthens security through broad code review also exposes vulnerabilities to all actors—including potential adversaries.[7] [8] In highly sensitive domains such as advanced cybersecurity systems, cryptographic implementations, and secure communication protocols, the imperative for sovereign control over development, deployment, and auditing becomes paramount.[9] [10] Reliance solely on open source can introduce challenges related to maintaining specialized expertise, ensuring rapid response to zero-day vulnerabilities, and managing supply chain risks—especially when key contributors may operate under adversarial jurisdictions.

As a result, a balanced and nuanced approach is essential. For critical security technologies, national or trusted-entity-led development, rigorous oversight, and strict governance are necessary to ensure the "grip" required for true digital strategic autonomy.[11] [12] By carefully selecting where and how to deploy open source, organizations and nations can maximize its advantages while safeguarding the most sensitive aspects of their digital ecosystems.

2.2 European Data Spaces Initiative – Centre of Excellence Data Sharing & Cloud

Another collaborative approach to digital strategic autonomy informs the European digital strategy that includes a focus on Common European Data Spaces. These create a trustworthy and secure framework

4 Lerner, J., & Tirole, J. (2002). "Some Simple Economics of Open Source." Journal of Industrial Economics, 50(2), 197–234.
5 Fitzgerald, B. (2006). "The Transformation of Open Source Software." MIS Quarterly, 30(3), 587–598.
6 Bria, F., Timmers, P., Gernone, F. (2025): EuroStack – A European Alternative for Digital Sovereignty. Bertelsmann Stiftung. Gütersloh, EuroStack – A European Alternative for Digital Sovereignty – Francesca Bria, Bertelsmann Stiftung – EuroStack.
7 Wheeler, D. A. (2015). Why Open Source Software / Free Software (OSS/FS, FLOSS, or FOSS)? Look at the Numbers!
8 Zimmermann, M., Staicu, C. A., Tenny, C., & Pradel, M. (2019). "Small World with High Risks: A Study of Security Threats in the npm Ecosystem." Proceedings of the 28th USENIX Security Symposium.
9 ENISA (European Union Agency for Cybersecurity). (2020). "Open Source Software in the Public Sector."
10 National Institute of Standards and Technology (NIST). (2020). "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." (NIST SP 800-161)
11 European Commission. (2021). "Open Source Software Strategy 2020–2023."
12 Kesan, J. P., & Hayes, C. M. (2009). "Open Source Software and the Intellectual Commons." American University Law Review, 58(5), 1171–1225.

for businesses, public administrations, and individuals to share data while retaining control over their generated data. By establishing interoperable data-sharing environments across strategic sectors like health, energy, and manufacturing, these spaces:

- Pool resources through public-private partnerships
- Standardize governance using EU legal frameworks
- Enable innovation while preventing vendor lock-in

This collaborative structure is intended to form the "core tissue" of Europe's interconnected data economy, directly supporting the Digital Decade Policy Programme's goals.

A notable example of this approach is the Centre of Excellence for Data Sharing and Cloud (CoE-DSC) in the Netherlands. The CoE-DSC acts as a central hub for organizations seeking to overcome data sharing and cloud adoption challenges. It brings together expertise from initiatives such as the Data Sharing Coalition, the Dutch AI Coalition (NL AIC), and the Gaia-X Hub Netherlands, creating a unified platform for knowledge, tools, and best practices. By developing generic building blocks and trust mechanisms, the CoE-DSC supports scalable, secure, and interoperable data spaces—enabling organizations to realize the full value of data sharing while reducing costs and fragmentation.

The CoE-DSC's mission is to unlock the transformative potential of data sharing by supporting organizations across sectors and geographies. Through collaboration with European initiatives such as the Data Spaces Support Centre (DSSC), SIMPL and alignment with EU regulations like the Data Act, the CoE-DSC has the ambition and intention to assure that Dutch and European organizations remain at the forefront of secure, sovereign data sharing. This model not only increases confidence in cross-organizational data sharing but also facilitates international cooperation, helping to accelerate the adoption of data spaces and smart solutions in areas like energy, mobility, and finance.

By combining open standards with robust governance, collaborative business models—exemplified by the CoE-DSC—enable Europe to harness collective innovation while maintaining control over its digital future. This approach is central to the success of Common European Data Spaces, which are designed to underpin Europe's digital economy and strategic autonomy in a globalized digital landscape.

2.3 Platform Nederland Radarland – becoming leading in radartechnology

Nederland Radarland is a public-private partnership established in 2002 by the Dutch Ministry of Defence, Thales Netherlands, TNO, and TU Delft – often called the "*Gouden Driehoek*" or Golden Triangle. Unlike traditional government innovation models reliant on formal tender procedures, Radarland was founded on a committed, multi-decade collaboration, anchored by strategic roadmaps such as the "Radar and Integrated Sensor Suites 2020–2030".[13]

The partnership's strength lies in integrating public and private expertise. The Ministry of Defence sets strategic requirements and provides testing facilities; TU Delft advances foundational research; TNO prototypes the requirements; and Thales Netherlands scales breakthroughs to market application. Joint governance, co-funded research positions, regular secondments, and transparent agreements on intellectual property and risk foster trust and accelerate decision-making.

This ecosystem features multi-stakeholder steering committees and iterative development cycles, reducing lead times, spreading costs, and enabling ongoing knowledge exchange. The result is a robust learning environment supporting continuous innovation. Through these mechanisms, the Netherlands has established itself as a global leader in radar technology, and Radarland sets a template for future strategic industrial policy initiatives.

Radarland demonstrates how collaborative public-private ecosystems align digital strategic autonomy with market-driven innovation. Its governance structures, shared investments, open knowledge sharing, and rotating secondments balance the State's need for sovereign radar capabilities with industry's imperative for competitive product cycles, building deep trust and reducing external dependencies. This approach accelerates innovation and generates sustainable, collective value beyond individual transactions.

2.4 Dutch National Crypto(graphy) Strategy (NCS) – establishing a flourishing Dutch ecosystem

A fairly recent example is that of the Dutch Crypto(graphy) Strategy.[14] Classified information (i.e. state secrets and the like) of the Dutch government needs to be encrypted with specific cryptographic products and services to be able to be communicated (for example specially developed phones for secure conversations). The technologies to make this happen are developed and produced by a small number of highly specialized private organizations. Hence the Dutch

13 Radar and Integrated Sensor Suites 2020–2030 roadmap, Nederland Radarland initiative, Dutch Ministry of Defence, Thales Netherlands, TNO, TU Delft, 2002 onwards. Available at: https://kivi

14 Een nieuw samenwerkingsmodel voor de Nationale Crypto Strategie | Rapport | Rijksoverheid.nl

government depends on these companies to make sure it is able to encrypt and transfer state secrets.[15] Some of the major take aways described below highlight why a collaborative approach is needed in the context of digital strategic autonomy when it comes to encryption-related technologies:

Due to the symbiotic relationship between de State and the private parties, the current situation in this industry (a fairly niche industry) is characterized by a certain level of interdependence. The State needs these companies and the companies need the State as it is one of its largest customers. This long-standing interdependence thereby provides fertile ground for the development of a collaborative ecosystem. By formally recognizing and organizing this relationship into roles such as “strategic partners” and “preferred suppliers,” such an ecosystem can create space for co-creation, shared risks, and collaborative roadmap development. Though other industries may not provide such a specialized market situation, the case highlights the need a collaborative approach to establish an ecosystem that can work for both State and industry.

A key collaborative element in the described ecosystem for the NCS is for example also the recommendation to provide multi-year guarantees around expected projects and product procurement. This may offer private companies the financial and operational certainty required to invest in high-grade facilities and personnel—especially crucial in markets with steep entry barriers. In return, these private companies can be asked to commit to transparency and delivery capacity, forming a reciprocal arrangement aligned with our described collaborative ecosystem focus on sustainable win-win relationships.

From a procurement perspective this project also represents a clear shift away from traditional transactional procurement models towards an ecosystem-based approach in which the government and industry share responsibility for continuity and innovation. Rather than relying on isolated contracts with limited guarantees, the focus has shifted to designing a collaboration model that couples the State’s need for certainty of supply with a more viable business case for industry. This embodies a key principle of our proposed ‘collaborative ecosystems’ thinking to generate mutual value through structured, long-term cooperation rather than transactional exchange.

Finally, the report also advices to jointly develop roadmaps and start up initiatives to shorten lead times through more intensive collaboration. By enabling the State and industry to co-govern strategic (capacity) planning and evaluation processes, a shared direction can be established for innovation and production.

2.5 Collaboration for Strategic Digital Autonomy

The cases outlined above serve as examples to highlight the importance of collaborative (ecosystems) thinking to establish robust and flourishing ecosystems. Especially when it comes to industries that are crucial to the security and/or economy of nation states. The table below highlights the most important commonalities (or success-factors) of the cases described and thereby provides an initial idea of where State-actors should focus their attention on when trying to assure digital strategic autonomy in cases where they are dependent on private parties.

15 Informatie- en communicatietechnologie (ICT) | Tweede Kamer der Staten-Generaal

Success Factor	Description
1. Awareness of the need for shifting from transactional (procurement) to a flourishing ecosystem with mutual shared goal	A shared feeling that both public and private parties are not able to achieve the goals in isolation. Hence a shared feeling that "we need each other", both public and private parties across digital value chains; leveraging complementary capabilities to strengthen strategic autonomy.
2. Broad institutional mandate	Support on a high level from both public and private parties is crucial for real impact. Political emergency and readiness from both political leaders, top civil servants and CxO's to engage in constructive discussions is needed to make things happen, keep each other committed, and coordinate collaboratively.
3. Pro-active Orchestration	The realization from both public and private parties that *"this problem"* won't solve itself through market dynamics. It needs active orchestration to make sure digital strategic autonomy is achieved because we need to navigate along novel procurement procedures and mindsets. Hence point 1 and 2 are supported by active orchestration.
4. Ambitious innovation roadmap	To actually achieve successful orchestration and hence the goals that need to be achieved it is crucial that the parties involved develop certain (ambitious) roadmaps. Not just plans for a few years ahead but for the years to come. This helps to assure that both public and private parties have the same view of what needs to be achieved. Hence there is also the need for private parties to become involved as (proactive) innovation actors for R&D activities.
5. Long-Term Relations	In line with point 4: to achieve such ambitious roadmaps it is needed that the parties involved do so with a long-term commitment. Achieving complex digital strategic autonomy cannot be achieved through short term, procurement driven processes but requires long term commitment.

Table 1. Key succes factors for collaborative approaches to strategic digital autonomy

Summarized, the success factors distilled from the cases described above illustrate that for long term digital strategic autonomy, both public and private parties need to have a shared feeling that "we're in this together", and need to engage in constructive discussions to make things work. If states are dependent on specific industry players, and those industry players are (at least to some extent) dependent on those Nation States, regular market dynamics are not sufficient. What is needed is an active orchestration process to bring together the different wants, needs, and requirements. One way of achieving this through a process of Collaborative Ecosystem Development[16], as outlined in the following section.

16 We describe our method as 'collaborative ecosystem development' to distinguish it from collaborative business modeling, upon which it is modelled. While both approaches are co-creative and take multiple value perspectives, collaborative business modeling traditionally focuses on how parties collaborate to deliver specific services or service portfolios. Our method, by contrast, focuses on building and orchestrating entire public-private ecosystems—creating networks of relationships, establishing governance frameworks, and coordinating long-term strategic initiatives that transcend individual service delivery.

3. A collaborative ecosystem approach to achieve balance

The example cases highlighted in Chapter 2 illustrate that digital strategic autonomy is not achieved by focusing on a single technology or vendor, but by ensuring control, autonomy, and resilience across every layer of the digital technology stack. On each level, policy makers need to strike a balance in the delicate trade-off between mitigating the risk of vendor lock-in while simultaneously preventing the loss of domestic suppliers who are vital for long-term security and innovation and building grip and control over the supply chains of mission-critical technologies. Collaborative principles are therefore essential at every level of the stack, enabling the informed choices and shared strategies needed to balance these competing priorities and build a truly sovereign digital future.

The process of Collaborative Ecosystem Orchestration enables stakeholders to navigate these choices in a structured and strategic way. Based on our analysis of the examples of successful public-private collaborations discussed in Chapter 2, we we outline a six-step operational framework to guide policymakers and industry leaders through this process. Our approach follows the following six-phases as outlined below:

1. Ecosystem Analysis and Stakeholder Engagement
2. Co-Creation of Shared Objectives
3. Collaborative Business Model Design
4. Implementation & Ecosystem Building
5. Monitoring & Feedback
6. Iteration

It is important to note that this approach, and specifically the six phases described, are not meant as a magic bullet and are not set in stone. Our approach allows for customisation in each phase. Tailoring each phase reduces “single-point” dependencies. Through this iterative orchestration, organizations can secure long-term digital sovereignty while driving impactful, cross-sector collaboration.

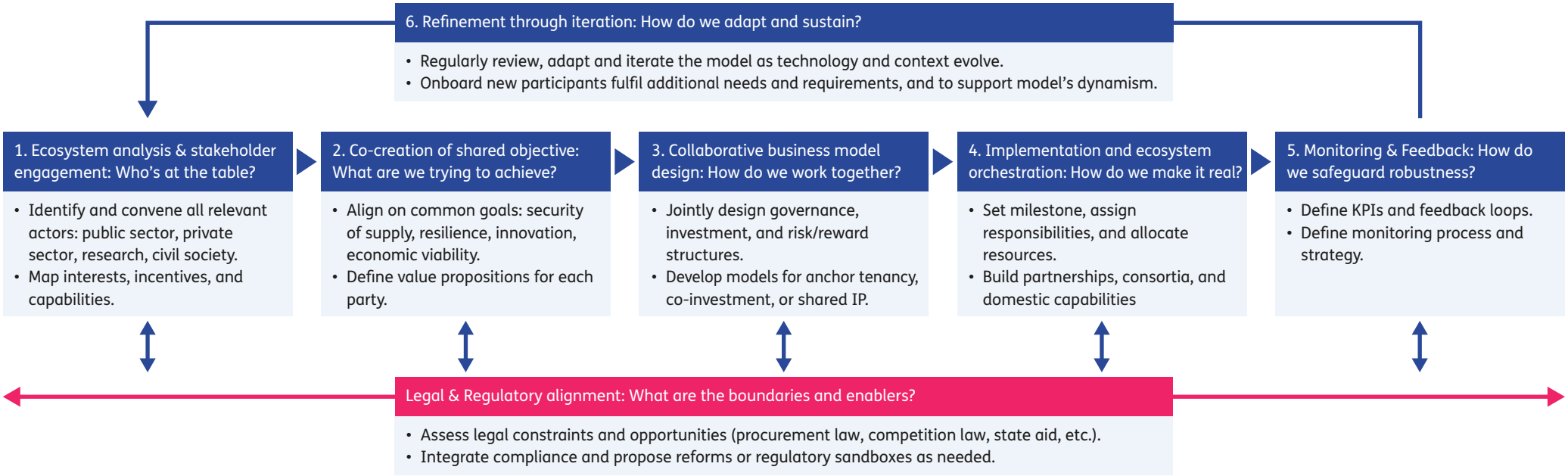

Figure 1. A graphical depiction of the six-phase process

3.1 Design principles of our collaborative ecosystem orchestration approach

The success factors for collaborative approaches to strategic autonomy listed above give rise to several interconnected principles designed to foster robust public-private ecosystems. When applied to the pursuit of digital sovereignty, these principles help mitigate key risks such as vendor lock-in, lack of security of supply, and the challenge of balancing diversification with domestic industrial support.[17]

Design principles	1. Relational, Trust-Based Engagement	2. Shared Responsibilities and Long-term Strategic Alignment	3. Co-Creation of Shared Objectives and Value	4. Integrated Ecosystem Design with Joint Governance	5. Continuous Monitoring, Feedback, and Iteration	6. Proactive Legal and Regulatory Alignment
Description	Collaborative ecosystem orchestration fundamentally shifts the public-private relationship from transactional to relational.	Partners share fundamental responsibility for the common good that the ecosystem generates or supports (i.e. strategic digital autonomy).	Public values (e.g., national security, data governance) and private incentives (e.g., profitability, innovation) are explicitly acknowledged and integrated.	Joint governance structures help establish comprehensive ecosystems that define roles, responsibilities, risk-sharing, investment strategies and intellectual property arrangements.	Systematic monitoring, feedback loops, and iterative refinement of the ecosystem allows for adaptation to evolving technological, market, and geopolitical contexts.	Proactive assessment and alignment with legal and regulatory frameworks throughout the entire process.
How it helps to safeguard strategic digital autonomy	Enables secure reliable, long-term access to critical technologies and expertise from trusted partners. Mitigating the risk of sudden supply disruptions or unaligned vendor interests. Trust-based engagements also facilitate sharing of sensitive information necessary for co-developing secure solutions and addressing vulnerabilities proactively.	This shared responsibility isn't merely theoretical; it's reflected in the enduring relationships between partners, each contributing based on their specific roles within the model. This strategic alignment ensures that all participants are invested in the long-term health and autonomy of the digital landscape, moving beyond transactional exchanges to build a resilient and self-reliant future.	The solutions developed are inherently aligned with national interests, preventing situations where commercial drivers might inadvertently compromise strategic autonomy or lead to reliance on untrusted foreign entities. It also helps in defining a "sufficient business case" for domestic industries to invest in critical capabilities.	Joint governance ensures ongoing oversight and influence over the development, deployment, and operation of sensitive technologies, directly addressing concerns about control over the technology stack. By structuring shared investments and IP, it can prevent domestic suppliers from becoming overly reliant on foreign capital, thus safeguarding national ownership and strategic relevance.	The rapidly changing nature of digital threats and technologies means that static approaches quickly become obsolete. This iterative principle ensures that the collaborative models remain relevant and effective in securing strategic digital autonomy.	By actively interpreting and, where necessary, shaping legal frameworks, collaboration enables the creation of partnerships that are both compliant and effective in achieving national security objectives. It provides the legal certainty needed for long-term investments in domestic capabilities.

Table 2. Design principles for the collaborative ecosystem orchestration approach

17 International Data Spaces Association (2023) "New Business Models for Data Spaces Grounded in Data Sovereignty"

3.2 New roles for market and state

Collaborative ecosystem development to support digital strategic autonomy requires a shift in mindset regarding how governments and industries collaborate with one another. Both government and industrial actors must evolve their roles to meet the demands of a more volatile, strategically charged geopolitical landscape. In this section we highlight the main shifts in interaction and collaboration that need to happen for collaborative business models to support the goal of digital sovereignty.

- **From transactions to strategic collaboration:** Public-private interactions were hitherto most often grounded in formal, competitive tenders designed to promote efficiency, transparency, and cost-effectiveness. Such models mostly lack the mechanisms to support long-term alignment, innovation, and/or strategic national interests. Especially for innovative and mission-critical technologies, the need for certainty of supply, technological sovereignty, and trusted partnerships may outweigh the value of efficiency and transparency. Put simply: autonomy is has a price. For critical technologies, sustained collaboration, mutual commitment, and a shared responsibility, hallmarks of a more strategic, relational mode of engagement, should be preferred.
- **Governments: From passive buyer to active orchestrator:** When moving to collaborative models to shape interactions with market parties, governments must adopt a more assertive role—what is increasingly referred to as "*industrial policy*".[18] Rather than simply procuring solutions, states are called to shape markets, support domestic capacity, and safeguard technological sovereignty. This means:
  - Direct intervention in critical areas to secure domestic production capabilities.
  - Strategic orchestration of industry ecosystems to ensure resilience and readiness.
  - Targeted measures that go beyond general subsidies to guarantee mission-critical capabilities (be a "launching customer").

  Yet this shift must be a controlled shift. Governments must avoid heavy-handed interventions that distort markets or breed inefficiencies. Instead, the emphasis is on intelligent orchestration—aligning incentives, setting strategic direction, and enabling trusted actors to co-develop essential capabilities.
- **Industry: From supplier to strategic partner:** This transition also demands a transformation on the part of industry. It is no longer sufficient to passively respond to tenders. Companies must position themselves as proactive contributors to national resilience and digital sovereignty. This entails:
  - Investing in domestic capabilities aligned with public priorities.
  - Engaging in continuous dialogue with public actors—not only to respond to needs, but to anticipate them.
  - Demonstrating reliability, strategic alignment, and a willingness to co-invest in shared national objectives.

  Those industrial actors who step into this role become more than vendors; they become co-creators of public value and stewards of long-term national capability.

This triple shift—from transactional procurement to strategic partnership, from passive buyer to orchestrator, and from supplier to co-creator—lays the foundation **for resilient digital ecosystems**. In such ecosystems:

- Governments maintain oversight and ensure public value is embedded throughout.
- Industry partners bring innovation, agility, and execution power.
- Both parties co-design models that balance short-term efficiency with long-term sovereignty.

This new balance of roles is not about discarding competition or abandoning market principles. It is about creating the institutional arrangements and collaborative capacity to meet a new strategic imperative—where digital sovereignty is no longer just a policy goal but a shared operational responsibility.

18 Industrial policy | OECD

4. Applying the collaborative ecosystem development approach in practice

In this chapter we describe how the collaborative ecosystem approach can be put to practice. We start by elaborating the fundamentals to be able to start with this approach and consequently outline the different steps and the roles & responsibilities associated with those steps for the different actors within the collaborative ecosystem.

4.1 What needs to be in place to make a collaborative ecosystem approach work?

- A "**coalition of the willing**": a group of stakeholders from both the private and public sector with "skin in the game", that is, with an active interest in the improving the robustness of the ecosystem. In addition, depending upon the technical context, research institution, civil society organizations etc can be invited to become part of the coalition.
  - Among the **public sector stakeholders** there should be the actors who are budgetholders for the technology in question, who have sufficient procurement capacity and expertise and / or own relevant the technology roadmap(s) to be able to support the domestic industry that is needed.
  - Among the **private sector stakeholders** there should be actors who have significant domestic innovation, development and production capacities. It is possible, and likely even desirable, to onboard stakeholders with additional and complementary non-domestic capacities. However, it should be kept in mind that the goal of a building a robust ecosystem for digital strategic autonomy is unlikely to be achieved when the starting coalition exclusively consists of international, non-domestic, suppliers.
  - **Other stakeholders** (research institutions, civil society organizations) need to be invited only in as far as they can add value and robustness to the ecosystem that is to be build. It is advisable to start small (for instance only with public and private sector stakeholders) in order to keep the complexity of the process under control.
- An **orchestrator** who guides and coordinates this process from beginning to end and is willing to take ownership over the process. Preferably that is a third party which helps and guides the stakeholders through the process. It is easier for a third party to be independent.

4.2 Applying the steps in practice

Step 1

Ecosystem analysis & Stakeholder Engagement: Effective collaboration begins with a comprehensive understanding of the ecosystem.

This phase lays the groundwork for collaboration by systematically identifying all relevant stakeholders and understanding their interests, influence, and potential contributions. It involves mapping the ecosystem, building initial relationships, and establishing channels for open communication and trust-building among diverse actors.

Why it is needed: Effective stakeholder engagement is essential for ensuring that all critical perspectives are included from the outset. By mapping and connecting the right partners, this phase helps prevent blind spots, minimizes resistance, and creates a foundation of trust and mutual understanding necessary for successful long-term collaboration

Step 2

Co-Creation of Shared Objectives: Building strategic digital autonomy requires a shared vision.

In this phase, stakeholders come together to develop a unified vision and align on common goals. Through collaborative workshops and structured dialogue, participants articulate the value proposition, clarify expectations, and reach consensus on what the initiative aims to achieve.

Why it is needed: Co-creating shared objectives ensures that all parties are working toward the same outcomes and understand the collective value of the collaboration. This alignment is crucial for building commitment, reducing misunderstandings, and setting the stage for effective joint action in subsequent phases.

Step 3

Collaborative Business Model Design: Move beyond transactional relationships to genuine partnership.

This phase is about translating the shared vision and objectives into a concrete, actionable business model. Stakeholders work together to design the value proposition, define clear roles and responsibilities, establish governance mechanisms, and develop shared responsibility frameworks for managing ecosystem-wide risks. This collaborative approach to risk—spanning financial, technical, compliance, and national security concerns—ensures that all parties actively participate in joint mitigation strategies rather than simply transferring risk between stakeholders.

Why it is needed: A thoughtfully designed business model ensures that all actors understand their contributions and benefits, reduces ambiguity, and creates a robust foundation for implementation. It also helps anticipate challenges and align incentives, making the collaboration more resilient and scalable.

Step 4

Implementation & Ecosystem Building: Translate shared models into action and build domestic capabilities.

In this phase, the collaborative business model moves from concept to reality. Stakeholders operationalize their agreements, integrate new processes, and build the necessary infrastructure to support the ecosystem. This is where partnerships are activated, resources are allocated, and the collaborative model begins to deliver value in practice.

Why it is needed: Implementation is critical for transforming strategic intent into tangible outcomes. Building the ecosystem ensures that the collaboration is not just theoretical but delivers real-world results, with mechanisms in place for coordination, support, and adaptation as the initiative grow.

Step 5

Monitoring & Feedback: Operationalizing collaborative models is an ongoing process.

This phase focuses on systematically tracking progress, collecting data, and gathering feedback from all participants. Performance against objectives is assessed, and any emerging issues or opportunities are identified. Regular reviews and transparent communication help maintain alignment and trust among stakeholders.

Why it is needed: Continuous monitoring and feedback are essential for ensuring that the collaborative business model remains effective and relevant. This phase enables early detection of problems, supports evidence-based decision-making, and builds a culture of accountability and shared learning.

Step 6

Continuous refinement through iteration: adapt the model in response to technological, market, or geopolitical changes. This ensures the partnership remains relevant, effective, and aligned with evolving strategic needs.

The final phase is about refining and improving the collaborative model based on insights from monitoring and feedback. Stakeholders adapt strategies, processes, and structures to respond to changing conditions, new opportunities, or lessons learned. Iteration may also involve scaling successful elements or pivoting aspects of the model as needed.

Why it is needed: No ecosystem is perfect from the outset. Iteration ensures that the collaboration remains dynamic, resilient, and capable of delivering sustained value over time. It embeds a culture of continuous improvement, allowing the ecosystem to evolve with its environment and stakeholder needs. In addition, it ensures the ecosystem stays dynamic and relevant by opening up pathways for new entrants.

4.3 Different roles and responsibilities for different actors in an ecosystem

The table below describes the different roles and responsibilities of the different actors that are relevant within a collaborative ecosystem for digital strategic autonomy.

Roles & activities per phase	(1) Ecosystem analysis and stakeholder engagement	(2) Co-creation of shared objectives	(3) Collaborative business model design	(4) Implementation & ecosystem building	(5) Monitoring & feedback	(6) Refinement through iteration
Orchestrator(s)	Conduct ecosystem and stakeholder analyses and establish a platform for engagement.	Facilitate collaboration to synthesize diverse perspectives into shared objectives, establish ground rules for engagement.	Coordinate business model design, value blueprint mapping, broker partnerships, and define collaborative governance mechanisms.	Oversee implementation rollout, manage ecosystem development, coordinate integration activities, establish performance monitoring systems.	Implement feedback collection systems, monitor key performance indicators, facilitate regular review sessions, manage stakeholder communication.	Lead iterative improvement cycles, facilitate adaptation workshops, coordinate model refinements, manage change processes.
Public sector	Provide access to relevant regulatory bodies and data.	Clarify public policy objectives, provide societal needs perspective, ensure regulatory alignment.	Provide regulatory guidance, offer public sector integration opportunities, support policy innovation.	Facilitate regulatory compliance, provide infrastructure support, align public programs with ecosystem goals.	Monitor policy impact, track regulatory compliance, assess public value creation, provide oversight.	Adjust policies based on outcomes, refine regulatory approaches, update public programs, support scaling initiatives.
Private sector	Map competitors and provide (individual) openness about strategic priorities.	Articulate business goals, define value creation targets, commit to shared success metrics.	Co-design value streams, define resource commitments, establish operational interfaces and synergies.	Execute operational integration, adapt business processes, invest in ecosystem capabilities, train teams.	Report on business outcomes, share performance data, participate in evaluation processes, identify operational issues.	Implement operational improvements, scale successful practices, adjust business strategies, expand partnerships.
Other stakeholders	Map and connect to relevant knowledge networks to facilitate exchanging experiences.	Validate proposed objectives against academic literature and empirical evidence. Design research questions that support the collaborative model's development.	Provide case study analysis and comparative research. Offer modeling and simulation capabilities to test business model assumptions. Establish research data sharing agreements and protocols.	Provide technical expertise & advisory. Conduct PoC-research. Offer training and capacity-building programs. Establish living labs and research testbeds for collaborative innovation.	Conduct independent impact assessments. Provide data analysis and research interpretation.	Provide evidence-based recommendations for improvement. Research emerging trends and technologies. Support knowledge transfer and scaling initiatives through research dissemination.
Case example	**Eurostack:** success depends on engaging a wide range of stakeholders. Orchestrators assure representation from both large and small parties.	**NCS:** public & private collaboration to co-create a national vision for cryptographic autonomy. E.g. aligning on strategic goals and committing to a shared value proposition.	**NCS:** Companies and governmental participated in co-creation workshops, helping to set design criteria for the collaborative business model of the ecosystem	**CoE DSC** brings together data sharing initiatives, service providers and policy makers in order to collectively orchestrate scaling of federated data sharing technology through proof-of-concepts, living labs, and use case development.	**NL Radarland:** Continuous monitoring through regular stakeholder reviews and independent assessments. Feedback loops for early identification of security risks and operational bottlenecks.	**NL Radarland** stayed aligned with European digital sovereignty goals by regularly updating its business model and architecture in response to regulatory changes and user needs, enabling scalable growth.

Table 3. Roles and responsibilities of stakeholders in the collaborative ecosystem orchestration process

4.4 Legal & Regulatory Alignment

Legal and regulatory alignment is foundational to successful collaborative ecosystem orchestration, as partners from different sectors must navigate complex laws affecting data sharing, intellectual property, market access, competition, and consumer protection. Without proactive alignment, initiatives face regulatory uncertainty, operational delays, and potential disputes, while proper alignment creates a level playing field that fosters trust, reduces risk, and provides the legal certainty needed for innovation and investment. This alignment transforms ambitious collaborative ideas into sustainable, scalable, and compliant business ecosystems by establishing clear rules that enable partners to confidently innovate while maintaining transparency and accountability as regulations evolve.

Legal and regulatory alignment requires coordinated effort across all ecosystem partners. The orchestrator leads by facilitating risk assessments, integrating compliance into project planning, and developing governance structures that reflect regulatory obligations while maintaining ongoing dialogue between legal, risk, and business teams. It is again a collaborative approach where the different public and private stakeholders need to conduct their own assessment. This collaborative approach transforms complex regulatory landscapes into clear pathways for sustainable innovation.

It is important to note that with the recent geopolitical developments governments should be aware that procurement rules offer more flexibility than commonly believed, especially for national security needs.[19] [20] Countries can use innovative procurement methods, security exemptions, and broad definitions of "unreliable suppliers" to support domestic partnerships and protect strategic interests. However, **overly strict interpretations of these rules often block collaborative approaches**.[21] The solution is adopting a more flexible, goal-oriented approach to existing rules rather than treating them as rigid requirements. Laws already provide the necessary tools—the challenge is using them effectively to balance competition with national security needs.[22]

19 Sundstrand, A. (2023). Article 346, EU Defence Procurement and the European Court of Justice. The Procurement Journal, 2, 15 – 27.
20 European Defence Agency, Guide on Security of Supply in the context of Directive 2009/81/EC on the award of contracts in the fields of defence and security (n.d.), https://eda.europa.eu/docs/documents/guide-sos_en.pdf.
21 Senden, L. (2004). Soft Law in European Community Law. Hart Publishing.
22 Meershoek, J. (2023). Defence Procurement in the Netherlands: Balancing Security and Competition.

5. Recommendations and key takeaways

In conclusion. strategic digital autonomy is, and will remain for the foreseeable future, a Gordian knot for governments. Strategic digital autonomy presents governments with seemingly contradictory objectives: reducing vendor lock-in while supporting domestic suppliers and securing mission-critical supply chains while maintaining competitiveness. The central message of this paper can be put simply: Collaborative ecosystem development, in which policy makers take ownership over the orchestration of robust public-private ecosystems with support and engagement of industry, represents a “sword of Alexander” that helps policy makers cut through the knot we sketched. Our claim is emphatically *not* that collaborative ecosystem orchestration alone will help governments achieve strategic digital autonomy across different sectors or technologies. Rather, we have argued that collaborative ecosystem orchestration is a much needed additional tool in the policy maker’s toolbox next to more traditional regulatory approaches.

Collaborative ecosystem development requires moving beyond transactional relationships toward trust-based collaboration that prioritizes shared objectives, long-term value creation, and ecosystem resilience. Success demands recognizing that digital sovereignty, innovation, and sustainable growth are best achieved through ongoing partnership, mutual investment, sharing responsibilities over risks mitigation and adaptive governance. The recommendations that follow below provide actionable guidance grounded in practical experience, showing how both policymakers and industry leaders can leverage their unique capabilities to drive successful collaborative ecosystem orchestration.

Key take-aways		
	For policy makers	**For industry leaders**
1	**Use the policy levers and tools at your disposal:** Policymakers can enable collaborative public-private ecosystems through six key tools: strategic procurement and long-term partnerships to stimulate domestic innovation; direct investment and targeted funding for R&D and infrastructure; regulatory sandboxes for safe experimentation with new business models; active ecosystem orchestration and platform building; capacity building through skills development and knowledge sharing; and ongoing monitoring with iterative policy adjustments to maintain alignment with strategic goals.	**Align your value proposition with public sector strategic goals.** Governments are prioritizing security of supply, resilience, and control over critical technologies. Clearly articulate and continuously adapt your value proposition to support digital sovereignty objectives—such as transparency, supply chain security, and compliance with local standards. Demonstrate alignment with public values and be prepared to adjust as policy goals and regulatory requirements evolve.
2	**Embrace co-creation: From transactions to trust.** Actively initiate and sustain ecosystem orchestration processes. Bring government, industry, and research partners together at every stage—from initial ideation to ongoing evolution—to co-design solutions, establish robust governance structures, and define shared objectives for critical digital systems and infrastructure. This approach ensures collective ownership and fosters the long-term commitment essential for national and European digital resilience.	**Engage Early and Proactively in Co-creative processes.** The era of passive response to government tenders is over; strategic autonomy requires genuine co-creation. Actively participate in all phases of collaborative ecosystem orchestration —from initial ecosystem analysis and co-creation of objectives to implementation, monitoring, and iteration. Bring your technology, market, and innovation insights to every stage to help shape robust, sustainable business models.
3	**Align public and private incentives for sustainable ecosystem growth.** Use collaborative ecosystem orchestration to explicitly negotiate and formalize risk-sharing, investment, and reward structures that are attractive to both public and private actors. Leverage public funding, procurement, and regulatory incentives to ensure private sector engagement is both economically sustainable and strategically aligned, with periodic review to maintain alignment as conditions evolve.	**Invest in ecosystem partnerships and domestic capabilities.** Overreliance on foreign markets or fragmented approaches can erode your strategic relevance and long-term viability. Build or join consortia, joint ventures, and alliances that strengthen domestic technology ecosystems, including partnerships with research institutions and knowledge partners. Invest in local talent, R&D, and infrastructure to position your company as a trusted, innovative partner for mission-critical projects.
4	**Balance supply diversification with strategic domestic support.** Ensure that policy interventions consider the full digital value chain (hardware, software, data, services) and foster collaboration between relevant actors at each layer. Design interventions and regulatory frameworks that address dependencies and risks throughout the stack, and revisit these regularly as part of the monitoring and iteration phases.	**Embrace Adaptability and Continuous Dialogue.** Policy, technology, and geopolitical contexts are evolving rapidly. Establish structured mechanisms for ongoing feedback, monitoring, and adaptation in your public sector collaborations. Regularly review and iterate on business models, governance, and technology strategies to remain responsive to shifting needs, risks, and opportunities.

Table 4. Key takeaways

To conclude, the core message of our paper is that the journey toward strategic digital autonomy requires a fundamental mindset shift—from purely transactional approaches to collaborative, ecosystem-driven models that create win-win outcomes for all participants.

If you would like more information on this research, or are interested in exploring how the results obtained through this research can be used in practice, feel free to contact the following TNO researchers.

Gijs van Houwelingen PhD
gijs.vanhouwelingen@tno.nl

Nick Oostervink PhD
nick.oostervink@tno.nl

TNO Vector
Centre for Societal Innovation and Strategy

tnovector.nl