TNO vector

Innovation and earning power in a digital world

Unlocking the socio-economic potential of Digital Trust

TNO Public ⟩ TNO-2026-16225

13 April 2026

Author(s)	Tom Barbereau; Augustinus Mohn
Classification report	TNO Public
Title	TNO Public
Report text	TNO Public
Number of pages	31 (excl. front and back cover)

Name of the programme	KIP'25 Digital Trust
Programme number	060.64082

Contents

Foreword

Digital innovation is reshaping every layer of our society at high speed – from the way we govern and do business to how individuals connect, learn and innovate. Amid this digital acceleration, there is one factor that determines whether progress strengthens – or undermines – our collective future: Digital Trust. Not as an abstract principle, but as a practical foundation for democratic resilience, prosperity, and security.

During the last decade, Digital Trust has moved from a technical concern to a matter of strategic importance. It underpins our ability to safeguard our economy and society in line with our values. It forms the basis of our (digital) transactions – whether between businesses, individuals, or governments. In today's shifting geopolitical landscape, where technological dependencies translate into political and economic vulnerabilities, it also has become a cornerstone of economic resilience and digital sovereignty.

Europe, and the Netherlands in particular, stands at a crossroads. While global powers invest at scale to shape digital ecosystems in their own interests, our strength lies in a different model: one that balances innovation with rights, openness with security, and competitiveness with public value. Digital Trust is not simply a defensive posture; **Digital Trust is our opportunity to lead with a distinctive, values-driven approach to digital innovation, economic growth and prosperity**.

Current efforts to build Digital Trust remain fragmented. Addressing this challenge requires more than isolated policies or technical fixes. It calls for a shared framework that connects technology, economics, governance, and society. The multi-stakeholder perspective of this whitepaper – bringing together government, industry/business, academia/research, and civil society – reflects the reality that trust cannot be imposed; it must be built collaboratively.

This whitepaper – next to offering a conceptual foundation to the problem – provides practical, action-oriented advice. By focusing on innovation, education and governance, it shows how Digital Trust can strengthen strategic autonomy while also driving economic growth and societal wellbeing. In doing so, it positions trust not as a constraint on progress, but as a catalyst for competitiveness.

This work should serve as a reference point for policymakers, researchers, business leaders and citizens alike. Building Digital Trust is not the responsibility of a single sector or institution – it is a collective endeavour that defines our digital future.

Executive summary

Digital Trust is no longer a peripheral issue – it is a strategic imperative for economic resilience and digital sovereignty. As societies and economies undergo rapid digitalisation, trust in digital technologies and their governance determines whether societies can safeguard their economy, protect their interests and values, and maintain strategic autonomy in a digital world.

Current efforts to strengthen Digital Trust are fragmented and lack a structured approach that integrates technological, economic, and socio-ethical dimensions. This gap poses a risk: without robust trust mechanisms and structures, the Netherlands and Europe may compromise their strategic autonomy and values and fail to capture the socio-economic benefits of digital innovation. Global competitors such as the U.S. and China are investing heavily in digital strategies, outpacing Europe in ambition and scale. In this competitive environment, Digital Trust is our unique selling point.

This whitepaper provides a reference framework for Digital Trust and outlines actionable steps to close the identified gap. It introduces a multi-stakeholder model based on the ‘quadruple helix’ that brings together government, industry/business, academia/research, and civil society to build trust collaboratively. Finally, it proposes concrete measures to strengthen Digital Trust through innovation, education, and governance – leveraging Digital Trust as a cornerstone of economic competitiveness, societal welfare, and strategic autonomy.

1 Introduction

1.1 What is Digital Trust and why does it matter?

Trust is a cornerstone of our society and economy. Digital Trust is about trust in digital technologies – their usage and the role they play in our society and economy. It comprises technological aspects (so-called 'trust technologies', which enable trust in the digital space), economic aspects as well as socio-ethical aspects.

As societies and economies become increasingly digitalised, trust in technologies and their governance becomes essential for safeguarding national interests and ensuring resilience against external dependencies. In the digital era, sovereignty and strategic autonomy therefore depend on the ability to establish and maintain Digital Trust as well. Sovereignty implies control over critical digital infrastructures and data, while strategic autonomy ensures that nations can make independent decisions without undue reliance on foreign technologies or frameworks.[1,2] Without a structured approach to Digital Trust – integrating technological, economic, and socio-ethical dimensions – we risk compromising both the socio-economic potential of digital innovation and strategic autonomy.

In a recent survey conducted by ISACA, 77% of respondents reported that Digital Trust "*is crucial to digital transformation*," yet 75% reported that they are "*either unsure or not fully aware of what improving Digital Trust requires in practice*".[3] A 2022 study by international consulting firm McKinsey concluded that "*leaders in Digital Trust are more likely to see revenue and EBIT [earnings before interest and taxes] growth of at least 10% annually*".[4] Likewise, the World Economic Forum sees a "*trillion-dollar opportunity for our global economy*" in building Digital Trust.[5]

Digital Trust at TNO

TNO conducts leading research on all aspects of Digital Trust – technological, societal, and economic. Our interdisciplinary research groups help to:

- Develop and implement **trust-enabling technologies** (incl. digital identities, privacy-enhancing technologies, and cybersecurity technology),
- provide guidance on the **trustworthy usage** and **governance** of digital technologies (incl. artificial intelligence, quantum computing, and identity systems), and
- **support policy- and decision-making** processes that uphold public interests and strengthen the digital transition and transformation of our economy (incl. government- and organisational-level advice, ecosystem building and orchestration).

The digitalisation of our society and economy is generally seen as an accelerator of economic growth.[6,7] Without trust in this digital transition, we risk being unable to leverage its full socio-economic potential. Despite the clear recognition by professionals and businesses alike, efforts to strengthen Digital Trust today are ad-hoc, driven by differing interests, and generally lack a structured approach that brings together the technological, economic and socio-ethical aspects of Digital Trust.

In this whitepaper, we seek to establish a reference frame that brings together the different aspects of Digital Trust and allows for better interactions between different stakeholders and their interests. We identify ways to more effectively and efficiently build Digital Trust, by discussing the roles the different stakeholders need to play to ensure trustworthy digital innovation – and thereby contribute to unlocking the full socio-economic potential of Digital Trust.

1.2 Reading guide to this whitepaper

The whitepaper is structured as follows:

- **Chapter 2** discusses the concept of Digital Trust – from its historical evolution originating in computer security, to the different notions of Digital Trust being in use today. We provide a **Digital Trust reference frame** to conceptualise Digital Trust and enable different stakeholders to create a better understanding of and to have better interactions between their respective areas of work.
- **Chapter 3** unpacks **the socio-economic potential of Digital Trust**. We discuss economic, technological, and socio-ethical aspects. Together with chapter 4, the chapter serves as a basis for defining relevant actions to build Digital Trust (discussed in chapter 5).
- **Chapter 4** considers the various actors and roles they need to play collectively to build Digital Trust and unlock its socio-economic potential. We introduce **a multi-stakeholder model for Digital Trust** – in the form of a quadruple helix – that highlights the different interactions required between the different actors to build Digital Trust effectively.
- **Chapter 5** provides a list of concrete **actions to unlock the socio-economic potential of Digital Trust**, based on the different aspects discussed in chapter 3 (economic, technological, socio-ethical), and involving the different actors and their roles discussed in chapter 4.

2 A reference frame for Digital Trust

2.1 Digital Trust as an evolved concept

Digital Trust is best understood as an evolved concept that builds on earlier questions related to the usage of digital technologies, such as security and privacy (see Figure 2.1).

Digital Trust as an evolved concept

Digital Trust has evolved as a concept in the digital age of society. It builds on and comprises other concepts such as security, privacy, and responsibility – and adds to it additional requirements around the trustworthiness of digital technology in the widest sense.

Figure 2.1: Digital Trust as an evolved concept.

Numerous public, private and academic stakeholders conceptualise Digital Trust in different ways – from technological, economic or socio-ethical points of view, and with social, organisational or scientific perspectives. It is no wonder then that Digital Trust is described as complex and multidimensional.[8,9] With this whitepaper, we want to provide clarity in discussing Digital Trust, to enable better interactions between the different stakeholders and thereby contribute to more effective ways of building Digital Trust in order to unlock its socio-economic potential.

Historically, first work on the topic of trust in digital technologies can be traced back to notions of computer security established with the advent of computers and

computing technology in the 1960s. Early on, researchers discussed the subjectivity and normativity of trust, as well as its role within societal systems and government. Later, with the rise of corporate conglomerates and large-scale online platforms, researchers considered to what extent these organisations and other institutions within our society and economy help to create (or dismantle) trust themselves.[9]

With the arrival of the first computer viruses in the late 1980s, trust grew in importance in the wider space of information security and assurance. With the mainstream adoption of digital technologies – notably, through personal computers and the emergence of the internet – cybersecurity grew as a field in the early 2000s. In the 2010s, with the internet and the expanding collection of data by corporations and governments alike, data breaches and scandals lead to an increased focus on notions of privacy. In recent years, with the broad adoption of artificial intelligence, questions around the responsible use of digital technologies have become pertinent.

Digital Trust is the latest phase in this evolution, comprising not only security, privacy, and responsibility, but adding additional requirements around the trustworthiness of digital technology in the widest sense (Figure 2.2).[10] In the subsequent sections, we discuss this notion in more detail.

Figure 2.2: Digital Trust as an evolved concept in the digital transition.

2.2 Trust in digital technology vs. trust enabled by technology

Trust in the digital world is facilitated both by the trustworthy usage of digital technologies and by so-called trust technologies themselves. Trust technologies (or 'trust tech' for short) comprise any digital technologies that help to facilitate trust in the digital space; they provide the technological infrastructure that is required to enable trusted digital interactions. Typical examples in this regard are the verification of digital identities and the secure sharing of sensitive data.

Trust in the usage of digital technologies, on the other hand, is about the usage of technology in a trustworthy way. In this sense, Digital Trust is technology-agnostic; it is not about the technologies that enable trust (the 'trust technologies' mentioned above), but about the trustworthy usage of any digital technology. This form of trust can typically be achieved with the help of governance and transparency measures. The World Economic Forum, for example, released a Digital Trust decision-making framework to support organisational leaders in making decisions about the usage of digital technologies to strengthen Digital Trust.[11] Trust in the usage of digital technologies may also be achieved by proxy: if an entity or organisation that

provides a digital technology or service is trusted, then the users of that technology or service may be more inclined to also trust the technology or service itself.

It is not the aim of this whitepaper to provide yet another definition for Digital Trust. Rather, our aim is to provide analytical clarity by establishing a reference frame that allows to have an informed exchange between different stakeholders working on or having an interest in the topic of Digital Trust. In doing so, we aim to contribute to better interactions between different perspectives – and ultimately contribute to a more effective and efficient way to build Digital Trust.

2.3 TNO's Digital Trust reference frame

Mutual understanding is crucial for knowledge exchange and effectively and efficiently building Digital Trust. As acknowledged by the OECD, "*short-term, isolated, single stakeholder approaches are no longer sufficient to tackle systemic societal challenges*".[12] Digitalisation is one of those challenges, and Digital Trust plays an important role in it, in particular when it comes to the adoption and societal acceptance of new technologies.[13,14] Creating a better understanding between different perspectives on Digital Trust is essential for better collaboration between different stakeholders.

To reduce misunderstandings between different perspectives and enable a pragmatic exchange and more effective interactions between different stakeholders, a common reference frame is required. Such a reference frame should enable different actors working on (or having an interest in) the topic of Digital Trust to better understand what their respective goals and methods are and identify areas of collaboration. To this end, we map commonly associated themes, concepts, stakeholders, and aspects associated with Digital Trust in a matrix (Figure 2.3). We distinguish between three different aspects of Digital Trust (technological, economic, socio-ethical) and intersect them with four different stakeholder groups (government, industry/business, academia/research, civil society).

Within the resulting fields (e.g. researchers working on technological aspects of Digital Trust), we give examples of typical interests and activities in the relevant field (e.g. 'technological research and development of trust technologies'). TNO's research on Digital Trust, for example, mostly falls within the Academica/Research row, covering all aspects (technological, economic and socio-ethical).

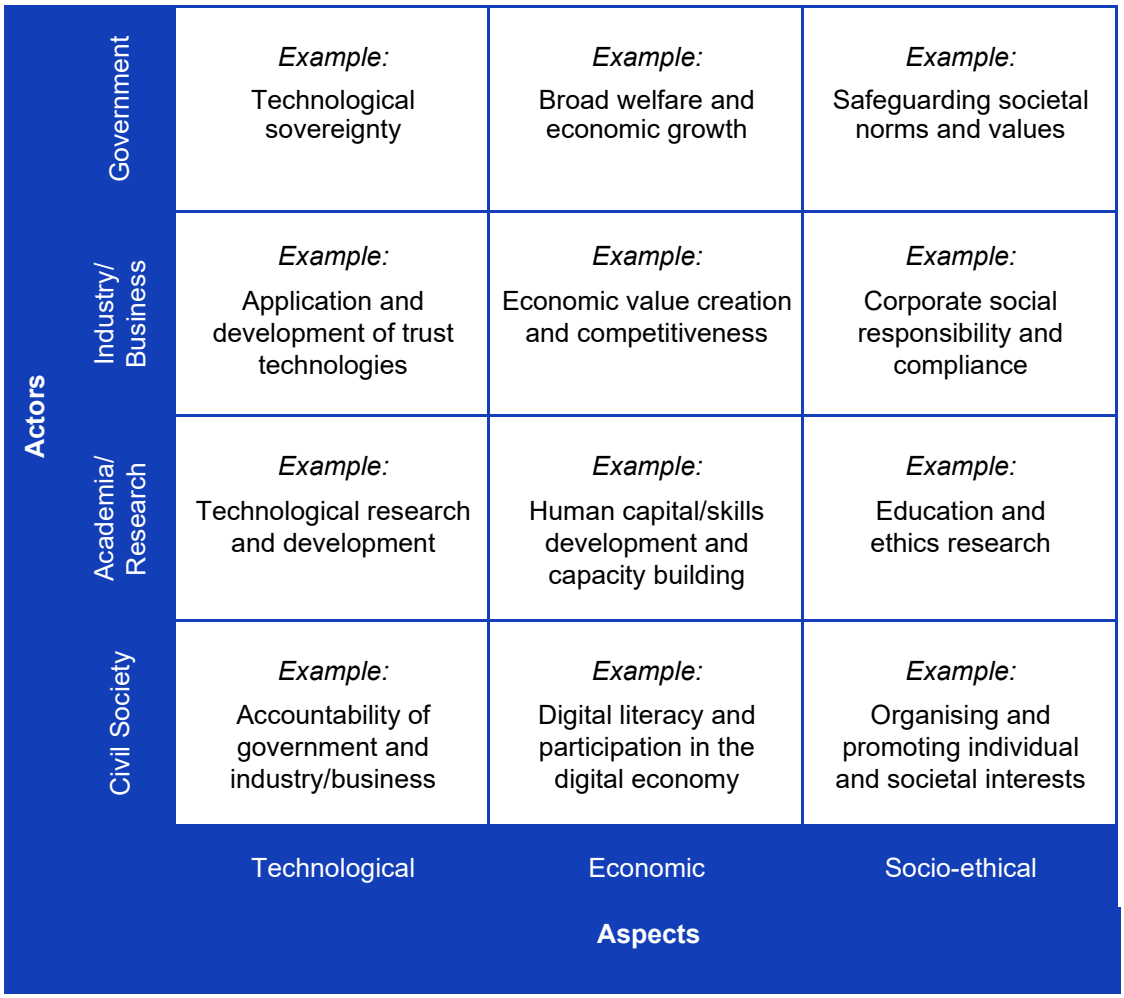


Figure 2.3: TNO's Digital Trust reference frame with examples.

The reference frame should allow different stakeholders to better understand from each other in which 'field' they are working on Digital Trust, and place their interests and work into the context of those of others. This, in turn, should enable better interactions and collaboration between the different factions – and thereby enable more effective and efficient ways to build Digital Trust and unlock its full socio-economic potential.

In the preparation of this whitepaper, for example, we used the reference frame to debate and provide clarity on the following questions: What aspects of Digital Trust do we seek to make an impact on (economic, technological, socio-ethical)? Our answer is: mostly economic, somewhat socio-ethical. Who are the actors that should be involved in this and that we want to engage? Our answer: All four stakeholder groups (government, industry/business, academia/research, and civil society). Fundamentally, we seek to integrate the "*knowledge of people and society with technological opportunities*",[15] in order to unlock the socio-economic potential of Digital Trust for society and the economy.

In the next chapter, based on the different aspects identified in the aforementioned reference frame, we unpack the socio-economic potential of Digital Trust.

3 The socio-economic potential of Digital Trust

3.1 Economic aspects

With economic aspects of Digital Trust, we refer to the link between Digital Trust and economic metrics – both at the micro level of individual organisations and at the macro level of the economy in general.

At the micro level, Digital Trust refers to the confidence one has in actors, technologies and processes to establish trusted digital interactions.[a] An example is the implementation of relevant standards (e.g. technical or governance) by a company to create a trusted environment where consumers and users are more confident to engage in. Increasing the confidence in digital interactions, services and products via trusted security measures, for example, is seen to have positive effects on a company's profitability.[17] Research shows that efforts put into increasing Digital Trust yield a clear return on investment: according to international consulting firm McKinsey, for example, leaders in Digital Trust are more likely to see growth of at least 10% annually.[4]

At the macro level, Digital Trust refers to the economic growth stimulated by increased confidence in services and products of the digital economy. Confidence may be increased, for example, by wide-scale adoption of specific standards within an economic sector, by following practices of data minimisation (e.g. implementing relevant governance measures, following principles of privacy-by-design and using privacy-enhancing technologies), or by the use of digital infrastructures (e.g. cloud solutions) situated within a regulated geographic area.[1] Greater Digital Trust – through increased confidence in the provided digital services and products – results in greater quality and quantity of digital interactions. Users tend to distrust the digital services and products offered by 'Big Tech' oligopolies.[18] Conversely, users are more inclined to trust digital interactions that are more secure, private, and offered by more effectively regulated organisations.

[a] Formally, the "*confidence of stakeholders on the competence of actors, technologies, and processes for establishing reliable and secure business networks*" (see [16]).

Trust in institutions, entrepreneurship and growth

Numerous studies have tied economic growth to trust in public institutions. Trust in institutions is a key determinant of entrepreneurial activity and, by extension, the expansion of an economy and the creation of new jobs.[19] More generally, trust in public institutions is a vital determinant of long term economic growth (Figure 3.1).[20] This is due to trust being a predeterminant of the smoothly functioning of business or, in economic terms, trust reduces transactions costs.[a]

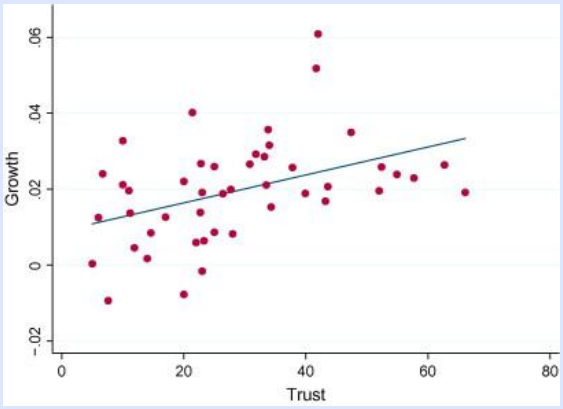


Figure 3.1: Trust and growth, cross-country evidence.[a]

3.2 Technological aspects

Technologies that enable trust in the digital space can be understood as trust mediators.[b] They can strengthen trust in a given (digital) system and between its users.

These technologies, also referred to as 'trust technologies' (or 'trust tech' for short), have received considerable attention in the past decade from researchers and practitioners alike. Work on cryptography and trustworthy computing, for example, has yielded a number of so-called privacy-enhancing technologies (PETs) for trusted analysis (e.g. differential privacy and multi-party computation), applications (e.g. blockchain and verifiable credentials), computation (e.g. federated learning and homomorphic encryption), and accreditation (e.g. zero-knowledge proofs and trusted execution environments). In addition to these PETs, we also include distributed ledger technologies (blockchain) and specific protocols in identity management.

In practice, these technologies are applied for example to data sharing in cancer research,[20] selective disclosure in the art market,[21] secure computation in financial auditing,[22] and consumption data aggregation in the energy domain.[23] When these technologies are put to work in specific contexts and in a targeted manner to enable trust between participants, the economic impacts can be considerable. In particular, in cases where data can leave the boundaries of organisations (or devices) in a trusted way, value can be unlocked.

[b] Formally, we account for the fact that "*interpersonal relations are increasingly being mediated*" by and "*institutions [become] more reliant*" on digital technologies and become mediators of trust in the process (see [19]).

Figure 3.2 shows an overview of common requirements for Digital Trust (privacy, fairness, etc.), trust technologies, their features, possible use cases and how those use cases contribute to different objectives (such as efficiency gains, generation of insights, etc.).

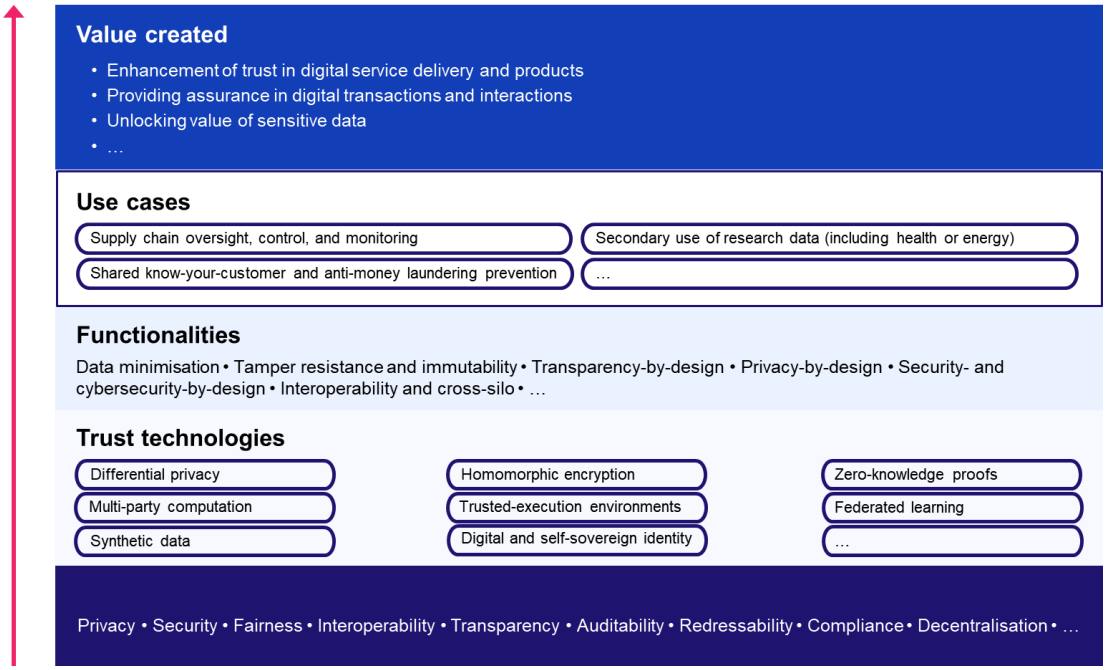


Figure 3.2: Overview of Digital Trust requirements, technologies, features, use cases and objectives.[c]

Note that technological aspects of Digital Trust go beyond the mere technology itself. In competitive markets (such as finance and energy) or sectors dealing with particularly sensitive data (such as healthcare and insurance), for example, technology alone is not enough to foster better collaboration.[24] As trust is increasingly mediated by technology, we also need to consider how these technologies shape the ways individuals and/or organisations trust each other. These questions are fundamentally about the governance of digital technology. Provided past failures, "*technological safeguards must be complemented by adequate internal governance structures and clear external accountability*".[19] This is discussed in the following section.

[c] Adapted from Prof. Nigel Smart (KU Leuven).

Fostering trust for health data sharing

In the HERACLES project, 13 public and private parties are jointly conducting research into two types of cancer. The challenge is to enable analysis across different organisations and sources without putting privacy-sensitive data at risk. Data spaces and privacy-enhancing technologies (PETs) help make this possible.

TNO plays a key role in the project as it facilitates the secure development of the data space with the help of PETs. In doing so, trust is established in sharing highly sensitive data in a manner that is compliant.

► Read more about HERACLES.

3.3 Socio-ethical aspects

Socio-ethical aspects of Digital Trust consider shared sociological or cultural dimensions related to trust.[25] Examples include shared norms and rules that feature in (trustworthy) interactions. Regulatory frameworks and governance must evolve to keep pace with technological advancement, providing clear guidelines and accountability mechanisms to prevent misuse and safeguard public interest.[26]

Aligning technology with our values and norms requires a multidimensional approach that integrates normative frameworks, participatory design practices, and regulatory oversight. First, embedding normative frameworks — which include principles such as fairness, transparency, and inclusivity —into the design and deployment of technology ensures that innovations respect human dignity and social priorities.[27,28] This requires involving diverse stakeholders in decision-making processes to surface overlooked perspectives and ensure technologies address genuine societal needs. Indeed, fostering a culture of participatory design bridges the gap between technical creators and end-users, enabling iterative feedback that aligns outcomes with societal expectations.

A practical example in today's world is sovereignty, which has become a pillar of European policy-making. Sovereignty, when viewed through a socio-ethical lens, extends beyond economic independence (refer to 3.1.), encompassing a community's ability to make decisions that reflect its own norms and values.[29] This autonomy is essential in fostering responsible innovation and development, where technological advancements align with ethical considerations, cultural contexts and normative practices. By respecting societal sovereignty, innovation becomes a collaborative effort that empowers communities rather than imposing external agendas – those that ever so often threaten democratic institutions.[30] This approach not only ensures inclusivity and accountability but also lays the foundation for Digital Trust. When individuals and communities see their sovereignty upheld in digital spaces, confidence in technologies and their governance strengthens, enabling a more equitable and secure digital future.

Digital Trust and sovereignty

Monopolists like Amazon, Microsoft and Google dominate value chains from datasets and research to production and applications. Our reliance on these multinational corporations, and their extended monopolisation of the digital realm, threatens our societal sovereignty and strategic autonomy to its core.[34] The need for trust frameworks in digital infrastructures is pivotal to respond to this high concentration of power and dependence. At TNO, we have discussed this matter extensively in our report entitled *Towards a sovereign digital future* (2024).[1]

► Dive into the report here.

4 A multi-stakeholder model to build Digital Trust

Innovation and entrepreneurship are the catalysts that drive competitiveness and economic growth. Features of these catalysts include the sustained cooperation between government, academia/research, industry/business, and civil society. [31] Within innovation sciences, the helix perspective captures these cooperation networks. It allows to rethink socio-economic development, with a focus on knowledge instead of resources.[32] In the Netherlands, the helix model materialised in the form of innovation ecosystems and, by inclusion of the aforementioned stakeholders, has proven particularly successful to promote regional competitiveness. Noteworthy outputs from the innovation system are Quantum Delta NL and the Netherlands AI Coalition. TNO plays an active role in both of these ecosystems.

For the case of Digital Trust, the helix perspective provides value to formulate a vision for an innovation system. Instead of featuring the three common stakeholder groups alone (comprising government, academia/research, industry/business – the so-called 'triple helix'), we include civil society within the innovation system as a fourth essential stakeholder group to unlock the potential of Digital Trust. As such, we adopt the helix perspective to map four actors to three impact areas – effectively creating a *quadruple helix*[33,34] – in order to identify cooperation networks and targets for action centred around regional development and competitiveness. In the following sections, we discuss each elements of the framework.

4.1 Government

Government, or rather, public institutions more generally, play specific roles within the helix. For Digital Trust, we define three roles to be assumed by key and supportive stakeholders within government.

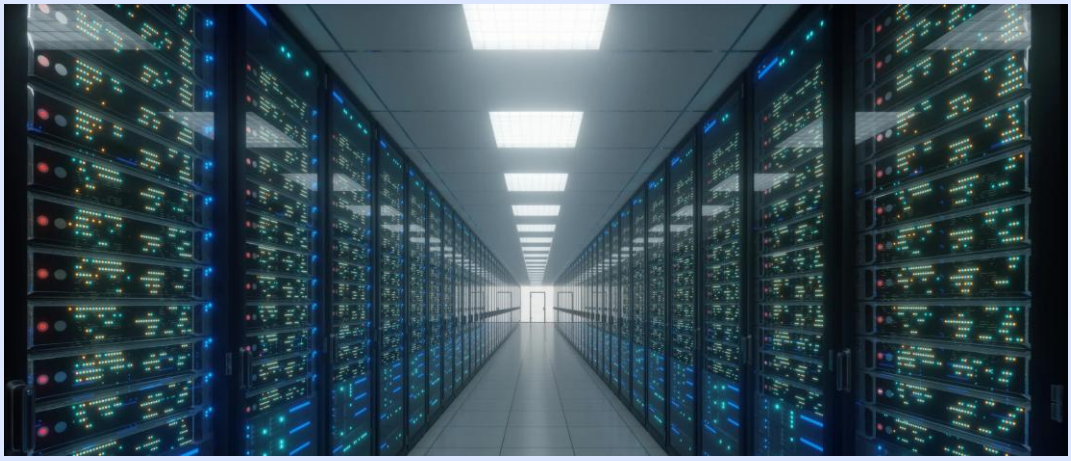
Government as visionary

The central government, led by specific ministries and agencies, can largely drive the ambitions around Digital Trust by developing thought leadership, coordinating ecosystems, and providing financing. With the aim of increasing (regional) competitiveness, this requires political capital.[31] One example of the government acting as visionary within the helix is that of Singapore. There, the government has largely facilitated the establishment of the Digital Trust Center – a research and innovation centric body that pushed the implementation and adoption of trust technologies.

Government as enabler

The government can act as enabler for the Digital Trust sector of the economy by provision of tailored resources. One example of the government acting as enabler is the Swiss Digital Initiative and the user-centric approach taken to its Digital Trust Label. The label suits organisations deploying digital services (where sensitive data is shared and/or an automated decision is made) and acts as signalling tool that increases confidence towards users. Additionally, initiatives like Germany's Federal Agency for Disruptive Innovation (SPRIN-D) or the Dutch Nationaal Agentschap voor Disruptieve Innovatie (NADI) can provide the necessary capital to promising technologies – which typically get stuck in an intermediate phase, where risks are too great for the market and existing public instruments are insufficiently geared towards speed, focus, and uncertainty.

Developing a trustworthy, sovereign large-language model



With financing by the Ministry of Economic Affairs and Climate Policy, TNO joined forces with the cooperative association of Dutch educational and research institutions (SURF) and the Netherlands Forensic Institute (NFI) to develop a large-language model – GPT-NL – that is aligned with public interests. The initiative is an important step towards transparent, fair and trustworthy use of artificial intelligence, with respect for Dutch and European values and guidelines, and with an eye for data ownership.

To uphold trust, as was described in a recent paper,[39] several measures were taken. The model's development is firmly rooted in fundamental rights and aligns with the EU's Guidelines for Trustworthy Artificial Intelligence. GPT-NL has a public (not-for-profit oriented) justification, serves equality, features a co-design process, follows key technical standards, and is open for validation.

► Read more about trust and our development efforts for GPT-NL.

4.2 Industry/business

Businesses and private organisations (incl. SMEs) have specific roles within the helix. In the context of Digital Trust, we define the following roles for this group.

Industry/business as innovation launchpad

In the Netherlands, industry has traditionally served as a critical launchpad for innovation by identifying and scaling technologies developed in academic and research settings. Companies – such as Philips, ASML, etc. – act as a bridge between theoretical knowledge and market application, investing in R&D to commercialise academia/research-derived innovations in areas like high-tech systems, life sciences, and sustainable energy, effectively acting as a launchpad for innovation backed by capital.

Public-private partnerships are central to enabling businesses to fulfil their role as launchpads. Through collaborative initiatives such as Brainport Eindhoven, the Dutch AI Coalition and the Topsector programmes, companies, universities, and government entities jointly pool resources and expertise to accelerate innovation. These partnerships de-risk investment for private companies while ensuring that academic research is aligned with industry and societal needs.

Industry/business as knowledge integrator

Beyond launching innovations, Dutch industry/business excels at integrating knowledge from diverse sources to develop holistic solutions, with Digital Trust emerging as a unifying priority. Businesses act as hubs where insights from academia/research, market trends, and government policy converge, fostering multidisciplinary innovation. In sectors like financial technology and agri-food, companies synthesise academic research on ethics, customer insights, and regulatory frameworks to build secure, trustworthy systems. This integrative role positions industry/business as not just a driver of innovation but also a steward of trust in a rapidly digitising world, aligning technological advancements with societal and ethical expectations.

For the Netherlands, TNO plays a critical role in supporting industry/business as a knowledge integrator. Acting as a bridge between fundamental research and practical application, TNO collaborates closely with businesses to develop and implement cutting-edge solutions in areas from cybersecurity and responsible development to quantum computing and collaborative business modelling. In the domain of Digital Trust, we provide cutting edge research and set agenda on the matter via Dutch and European programmes. By partnering with TNO, organisations gain access to applied research and expertise that strengthens their ability to integrate diverse knowledge streams into impactful, market-ready innovations.

Orchestrating a Dutch ecosystem around quantum

TNO started getting involved with the development of quantum technologies in 2014, and began to forge partnerships and expanding our knowledge and experience in this domain. Over the years, TNO has built expertise in quantum technologies by blending our own targeted research and development with significant strategic partnerships.

This eventually led to the National Agenda on Quantum Technology, which resulted in the establishment of Quantum Delta NL (QDNL) as the overarching Dutch quantum ecosystem organisation. TNO is one of the founding partners of QDNL and is one of the key players within the ecosystem. From computing and communication to sensor development, we work within QDNL to drive Dutch innovation and ensure the trustworthy integration of these technologies by alignment to societal values and needs.

► Learn more about Quantum Delta NL.

4.3 Academia/research

Research and development primarily emerges and occurs within the academic/ research space. By its very nature, the unique feature of research and knowledge institutions, is the "*availability of significant free time, space and facilities to initiate new activities*" and, therefore, it "*plays a key role in creating growth as well as intellectual advance*".[35] From our perspective, in the context of Digital Trust, we view two central roles for academia/research.

Academia/research as knowledge creators

In knowledge driven, globalised economies, innovations are a means to ensure a competitive advantage and foster regional development – necessary ingredients for economic growth. At the heart of this status quo are universities and research

organisations. Fundamentally they are institutions characterised by rather unusual organisational features (if compared to other knowledge institutions such as schools, libraries, or think tanks). These exhibited features are unique in the sense that the "*distributed, self-organising mode of knowledge production [in academia/research] maintains a diversity of approaches, topics and solutions needed in frontier research, which involves generating relevant knowledge under uncertainty*".[36] In short: universities and research organisations operate at an uncertain frontier of knowledge, attempting to push the boundaries of our actual knowledge. Knowledge and innovation, in turn, are critical to economic prosperity.

There are a number of channels through which universities and research organisations may affect growth, not least by provision of a greater supply of human capital (in the case of universities) and churning out innovation. Research found robust evidence that an increase of the presence of universities within a region is positively associated with faster subsequent economic growth.[37]

Academia/research as entrepreneurial laboratory

Universities and research organisations can be proactive and increase the process of technology transfer from academia/research to practice. This model has proven to be beneficial for regional development and economic growth.[38] The laboratories offered for ambitious entrepreneurs by research organisations such as TNO, for example, allow to form organisations – most knowingly, spin-offs – and bring (digital) technologies to practice.

Universities equally have "*the capacity to transfer technology and organise firms, taking some of the role of industry*".[39] Key to developing this capacity at university-level is to invest in human capital and empower students. Delft University of Technology, and its incubator YES!Delft for example, provide an environment where students can grow promising ideas into successful companies. As to the strategic orientation, to for example Digital Trust, both government and industry/business can influence the direction of entrepreneurship through seed funding and tailored research grants. The Technical University of Munich, and its UnternehmerTUM for example, have such orientated funds and grants made available by public and private parties for select topics – such as sustainability and mobility.

4.4 Civil society

Civil society plays a unique role within the helix: it is the foundation for collaboration between academia/research, industry/business, and government. It provides "*the launch pad for take-off*" for their interactions.[40] Leydesdorff adds that these sectors grow out of civil society itself.[34] While the importance of civil society in driving innovation and public involvement is clear, in the subsequent paragraphs we emphasise their pivotal role in the context of Digital Trust.

Civil society as a trust advocate

Civil society organisations act as watchdogs and advocates for transparency, accountability, and ethical practices in the digital domain. They ensure that technological innovation does not compromise fundamental rights such as privacy, security, and fairness. By engaging in policy debates, monitoring compliance, and raising awareness, such organisations are needed to help build public confidence in

digital ecosystems. Their involvement is critical to embedding societal norms and values into Digital Trust frameworks, making trust not just a technical feature but a social contract.

Civil society as an enabler of participation and literacy

Beyond advocacy, civil society fosters digital literacy and inclusion. Through education campaigns, community programmes, and partnerships with schools and local governments, societal organisation play a key role to empower citizens to understand and navigate digital technologies safely. This role is essential for reducing the digital divide and ensuring that trust principles are understood and embraced by all segments of society. In doing so, civil society strengthens the social fabric that underpins digital transformation, ensuring that innovation benefits everyone rather than a select few.

5 Actions to unlock the socio-economic potential of Digital Trust

5.1 Defining the action lines

In the Draghi report, the European Union and its Members were urged to integrate "*far more coordinated industrial policy, more rapid decisions and massive investment if it wants to keep pace economically with rivals*".[41] These points were iterated for the Netherlands in particular with the Wennink report.[42] In consideration of this call, the actions to unlock the potential of Digital Trust are formulated under the umbrella of three lines – integrate, innovate, and ideate & educate (Figure 5.1). Each is aligned with the competitiveness compass put forward by the European Commission,[43] and directed at the collective of Digital Trust stakeholders. Essentially, the action lines and underlying actions form the basis for a collective Digital Trust programme.

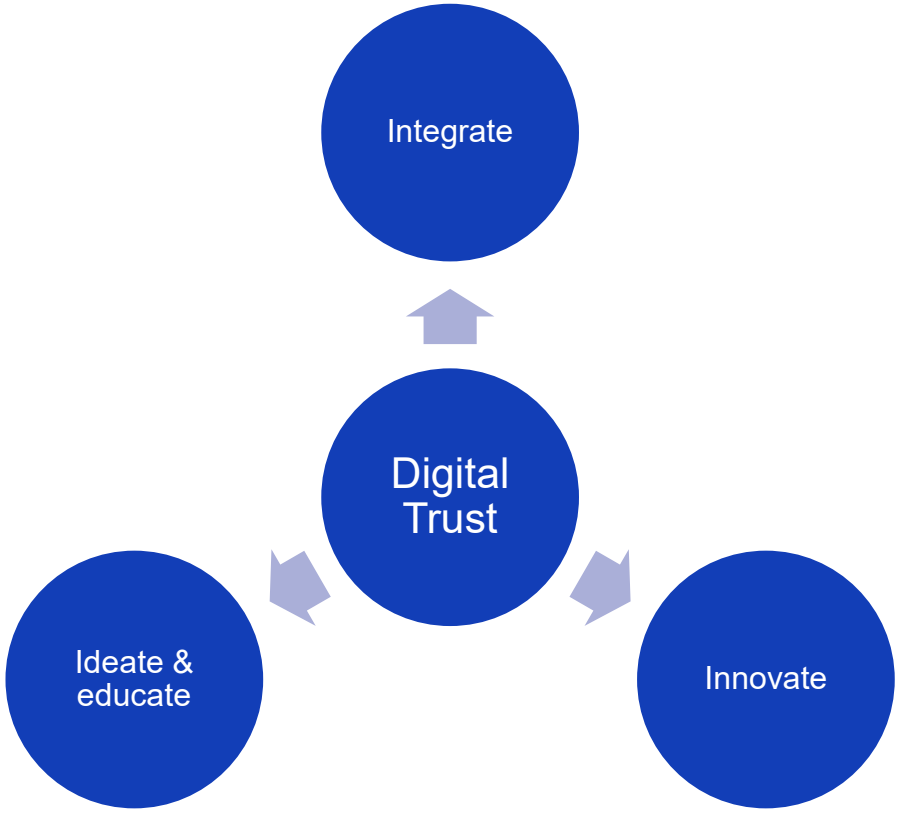


Figure 5.1: Three actions lines to unlock the potential of Digital Trust.

5.2 Integrate

A robust digitalisation can stimulate economic growth by creating a competitive digital economy. This involves not only regulating the digital market, for example, to ensure fair competition, but also by investing in digital skills, infrastructure, and integrative capacities.[44] By doing so, regions can become breeding grounds for entrepreneurship, attracting investments and talent – ultimately, nurturing competitiveness and contributing to growth.

5.2.1 Embedding trust technologies

Motivation

To drive the practical application of emerging technologies and bridge the gap between innovation and real-world impact, building robust use cases is essential, bringing together technology, its users, and researchers. A key component of this process is integrating trust technologies, which safeguard sensitive data while enabling secure collaboration and analytics. Additionally, efforts that aim to establish shared ethical and procedural frameworks, ensuring that technology adoption aligns with societal values and regulatory standards, should be supported as well. Together, these efforts create a foundation for deploying technology responsibly and effectively in diverse domains.

How

- *Collaborative ecosystem development*: Foster partnerships among technologists, researchers, and end-users to co-create use cases that address real-world challenges, ensuring practical relevance and usability. This requires, for example, the establishment of collaborative business models.
- *Implement and scale technologies*: Integrate trust technologies to enable data security and trust in technology applications. Technologies mature best when integrated within real-world applications. They are necessary to bring technologies towards a higher technology readiness level (TRL).
- *Establish and codify norms*: Develop and standardise ethical, legal, and procedural norms through interdisciplinary collaboration to guide responsible technology deployment and implementation and ensure alignment with societal values.

5.2.2 Creating a Digital Trust label

Motivation

A Digital Trust label or certification serves as a vital indicator of an organisation’s or technology’s Digital Trust maturity, akin to how food labels provide transparency and build consumer confidence. By offering a standardised and easily recognisable assurance of trustworthiness, it empowers users to make informed decisions about the technologies they adopt, fostering greater confidence in digital ecosystems. For organisations, such certifications can differentiate their products in a competitive market, demonstrating accountability and compliance with best practices or regulatory standards. Additionally, a trust label can drive widespread adoption of secure and trust-enabling technologies, ultimately building a culture of transparency and reliability across industries.

How

- *Define standardised criteria and governance*: Establish a clear framework of trust principles covering Digital Trust requirements such as security, privacy, ethical use, etc., and compliance with relevant regulations. This should be developed collaboratively with industry/business, academia/research, policymakers and civil society to ensure credibility and broad acceptance.
- *Develop certification and audit mechanisms*: Create a transparent process for organisations and technologies to obtain the label, including independent audits, periodic reviews, and mechanisms for revocation in case of non-compliance. This ensures the label remains a trusted and dynamic indicator of Digital Trust.

5.2.3 Translation of concepts to practice

Motivation

The number of interventions and frameworks made available to ensure responsible innovation has grown significantly. However, most of these lack applicability.[45] Organisations are pragmatic and are in dire need for more practical tools.[45] When it comes to research, Digital Trust is often reduced to specific technologies, without developing a robust methodology that systematically addresses Digital Trust.

How

- *Field labs and task forces*: These vehicles can support the integration of practices around Digital Trust towards organisations. Within these, support in the practical development of use cases with a scientific perspective and responsible approach to innovation is a productive approach.[46]

5.2.4 Policy toolkit

Motivation

A policy toolkit for Digital Trust provides governments and regulators with practical instruments to embed trust principles into national and regional strategies. Similar to the World Economic Forum's frameworks for organisational decision-makers,[5] this toolkit should operate at the macro level, enabling policymakers to address systemic challenges such as sovereignty, cybersecurity, and privacy protection. By offering structured guidelines, actionable templates, and decision-support tools, the toolkit can empower governments to design coherent policies that foster secure and transparent digital ecosystems. Monitoring and benchmarking mechanisms ensure accountability and allow to measure progress against international standards, strengthening sovereignty and competitiveness in the global digital economy.

How

- *Develop a structured policy framework*: Create comprehensive guidelines for integrating Digital Trust principles into national strategies, covering relevant requirements such as security, privacy, ethical AI, and compliance.
- *Provide actionable templates and decision-support tools*: Offer ready-to-use policy templates, checklists, and risk models for consistent implementation.
- *Establish monitoring and benchmarking mechanisms*: Implement KPIs and comparative benchmarks to track progress and ensure continuous improvement.

5.3 Innovate

Digital technologies involve multiple elements – data centres and graphic cards, networks and connectivity, data, and applications, and much more.[1] Digital Trust is a factor in each of those layers. While national and European strategies to increase digital innovation more broadly show momentum, the scale in both ambition and financial terms is far below that of Chinese and American strategies. To take action, a strategy to pursue is to make strategic investements control points.[47] This allows to balance national interests, economic earning power and, in connection to Digital Trust particularly, bring additional aspects of broad welfare.

The Netherlands, as one of the most innovative countries in Europe (according to the European Innovation Scoreboard), is well positiend to do so. In response to these developments, we propose two research programmes designed to drive innovation.

5.3.1 Whitespot analysis

Motivation

A whitespot analysis identifies gaps and untapped opportunities in the current Digital Trust landscape, serving as a foundation for targeted innovation. While Europe and the Netherlands have made progress in areas such as digital resilience and data protection, significant gaps remain in integrated trust frameworks, cross-sector collaboration, and scalable solutions for emerging technologies. These whitespots often occur at the intersection of technology layers - such as between infrastructure and application security - or in domains where trust concerns are rapidly evolving, like AI, quantum-safe cryptography, and privacy-enhancing technologies.[48]

By mapping these gaps against global benchmarks and industry/business needs, the Netherlands (and Europe) can prioritise research and development efforts where strategic impact is highest. This includes, for example, identifying control points that influence sovereignty and competitiveness, such as secure cloud infrastructure, trusted identity systems, and interoperable standards. Addressing these whitespots will strengthen Digital Trust and thereby create economic opportunities and reinforce economic and societal resilience in the face of an accelerating digitalisation.

How

- *Benchmark against global leaders*: Conduct comparative analysis of Dutch and European capabilities versus U.S. and Chinese strategies to identify areas of underinvestment and strategic vulnerability.
- *Engage stakeholders for gap validation*: Organise workshops with industry/business, academia/research, and policymakers to validate whitespots and prioritise those with the highest socio-economic impact.
- *Dynamic whitespot map*: Develop a living document or dashboard that visualises gaps across technology layers and sectors, updated regularly to reflect emerging trends and risks.
- *Link whitespots to innovation programmes*: Use the analysis to inform technology-agnostic and technology-specific research agendas, ensuring resources are allocated to areas with the greatest strategic leverage.

5.3.2 Technology-agnostic measures

Motivation

A technology-agnostic research and innovation programme for Digital Trust should focus on developing foundational principles, frameworks, and methodologies that can be applied across diverse technologies and industries. Such a programme should explore universal concepts like transparency, accountability, ethics, and privacy while identifying trust metrics that remain relevant regardless of the underlying technology.

Research needs to emphasise understanding user expectations, shifts in societal norms, and regulatory requirements to design systems that prioritise trust “by design”. Collaboration with policymakers, businesses, and civil society ensures that the findings are broadly applicable and foster an adaptable, technology-neutral approach to building trust in digital ecosystems.

How

- *Interdisciplinary research*: Establish interdisciplinary research teams to develop universal trust frameworks and metrics, focusing on collaboration with policymakers, civil society, and industry/business to ensure broad applicability.
- *R&D funding*: Provide funding and resources for long-term studies and pilot projects that explore cross-industry/business trust mechanisms and their societal impact.

5.3.3 Technology- and/or industry-specific measures

Motivation

In contrast to the technology-agnostic measures, a technology-specific research programme for Digital Trust should dive into applied research for particular domains where the topic of trust is seen most critically. Tentatively, we observe a need in e-Government, healthcare, and the financial sector amongst others.

This programme should address real-world challenges in these industries by designing, prototyping, and testing solutions tailored to specific technologies. Interdisciplinary researchers should work closely with developers, regulators, and end-users to create deployable tools and refine their implementation, bridging the gap between innovation and practical application while directly addressing domain-specific risks and opportunities. Underlying this research is the assumption that technology alone often does not suffice in addressing questions of Digital Trust.[19]

How

- *Research partnerships*: Partner with startups and industry/business leaders to accelerate the development and deployment of these solutions, ensuring they address real-world challenges and scale effectively.
- *Develop field labs and innovation programmes*: Create dedicated labs or testbeds to design and test technologies.

5.4 Ideate & educate

Digital trust is not just a technical concept; it is a societal and economic imperative that requires active ideation and education. While initiatives to strengthen sovereignty and strategic autonomy in Europe are gaining traction, the ambition and scale remain modest compared to global competitors. To close this gap, fostering a culture of innovation and knowledge exchange is essential. A physical location can serve as a control point - bringing together technologists, policymakers, and industry/business leaders to align efforts and accelerate regional competitiveness. By embedding trust principles into education and research, and by creating collaborative platforms for startups and academia/research, we can ensure that Digital Trust becomes a driver of economic growth, societal resilience, and broad welfare.

5.4.1 Toward a centre for Digital Trust

Motivation

It is advisable to establish a physical (or at least hybrid), centralised platform to foster collaboration, innovation, and the exchange of knowledge among technologists, researchers, policymakers, and industry/business stakeholders, with a strong focus on driving regional competitiveness. By positioning the centre as a leader in Digital Trust and related topics such as digital resilience, sovereignty and autonomy, the Netherlands can attract startups and emerging talent, creating an ecosystem where innovation thrives and economic growth is accelerated – all while respectful of norms and values.

Match-making events, hackathons, and academic conferences should serve as key opportunities to bring together diverse actors. This dynamic centre should empower startups to play a pivotal role in shaping the future of secure and ethical digital ecosystems while advancing the region’s leadership in this critical domain.

How

- *Build collaborative infrastructure*: Establish a physical and virtual hub equipped with state-of-the-art facilities for research, co-creation, and testing. This includes secure labs, shared workspaces, and digital platforms to enable continuous collaboration among startups, academia/research, and industry/business.
- *Stimulate innovation through engagement programmes and funding*: Organise matchmaking events, hackathons, and academic-industry conferences to foster partnerships and accelerate the development of trust-enabling technologies. These programmes should be designed to attract talent, encourage knowledge exchange, and create pathways for commercialisation of research outcomes.

5.4.2 Teaching and training

Motivation

Education plays a pivotal role in both research programmes elaborated on before by equipping individuals with the knowledge and skills to drive innovation and apply trust-enabling principles effectively. In the context of a technology-agnostic programme, teaching and training should focus on foundational topics like ethical

frameworks, trust metrics, data governance, and interdisciplinary approaches to trust, ensuring a broad understanding that can adapt to diverse technological landscapes.

For the technology-specific programme, education should emphasise hands-on, applied learning, such as the integration PETs into systems, developing secure protocols, or implementing cybersecurity measures for specific industries. By creating tailored curricula, workshops, and professional development opportunities, these programmes can cultivate a skilled workforce that bridges theoretical insights with practical expertise, ensuring that Digital Trust principles are embedded into both research and real-world applications.

How

- *Develop tailored curricula*: In conjunction with leading research institutions and universities of applied sciences, achieving the above should entail the creation of educational programmes. These programmes ought to be interdisciplinary by nature and integrate the latest academic knowledge as well as to consider real-life uses cases and geopolitical developments.
- *Foster academic-industry partnerships*: Establish collaboration and knowledge transfer programmes with universities, research institutions, and industry/business leaders to co-design research and entrepreneurial opportunities that provide students and professionals with real-world experience and access to cutting-edge technologies. This model is well-established with the case of Stanford and MIT, amongst others.

References

1. Stolwijk, C. *et al. Towards a Sovereign Digital Future – the Netherlands in Europe*. https://vector.tno.nl/en/articles/digital-transformation-europe/ (2024).
2. van Houwelingen, G. & Oostervink, N. *Collaborative Ecosystem Development as an Approach to Facilitate Digital Strategic Autonomy*. https://publications.tno.nl/publication/34645136/yIctWPUY/TNO-2025-R12054.pdf (2025).
3. ISACA. *State of Digital Trust 2024*. https://www.isaca.org/resources/reports/state-of-digital-trust-2024 (2024).
4. Boehm, J., Grennan, L., Singla, A. & Smaje, K. *Digital Trust: Why It Matters for Businesses*. https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters#/ (2022).
5. Hayat, Z. Digital trust: How to unleash the trillion-dollar opportunity for our global economy. *World Economic Forum* (2022).
6. Dedola, L. *et al.* Digitalisation and the Economy. *European Central Bank Working Paper Series* https://doi.org/10.2139/ssrn.4429773 (2023) doi:10.2139/ssrn.4429773.
7. World Bank. *Digital Progress and Trends Report 2023*. https://www.worldbank.org/en/publication/digital-progress-and-trends-report (2024).
8. Kelton, K., Fleischmann, K. R. & Wallace, W. A. Trust in digital information. *Journal of the American Society for Information Science and Technology* **59**, 363–374 (2008).
9. Paliszkiewicz, J., Cusumano, J. L. G. & Gołuchowski, J. *Trust, Digital Business and Technology: Issues and Challenges*. (Routledge, New York, 2022).
10. BSI. *Evolution of Digital Trust*. https://www.bsigroup.com/siteassets/pdf/en/insights-and-media/insights/white-papers/bsi-eodt-whitepaper.pdf (2024).
11. Dobrygowski, D., Ben-Atar, A., Mohn, A. & Stanhaus, A. *Earning Digital Trust: Decision-Making for Trustworthy Technologies*. https://www.weforum.org/publications/earning-digital-trust-decision-making-for-trustworthy-technologies/ (2022).
12. OECD. *Mission-Oriented Innovation*. https://oecd-opsi.org/work-areas/mission-oriented-innovation/, https://oecd-opsi.org/work-areas/mission-oriented-innovation/ (2022).
13. Rijswijk, K., de Vries, J. R., Klerkx, L. & Turner, J. A. The enabling and constraining connections between trust and digitalisation in incumbent value chains. *Technological Forecasting and Social Change* **186**, 122175 (2023).
14. Duenas-Cid, D. & Calzati, S. Dis/Trust and data-driven technologies. *Internet Policy Review* **12**, (2023).
15. Arnoldus, M., Braams, R., Dorst, K., Hekkert, P. & Veenstra, A.-F. *Agenda: Key Enabling Methodologies, 2024-2027*. (CLICKNL, 2024).
16. Mubarak, M. F. & Petraite, M. Industry 4.0 technologies, digital trust and technological orientation: What matters in open innovation? *Technological Forecasting and Social Change* **161**, 120332 (2020).
17. Podrecca, M., Culot, G., Nassimbeni, G. & Sartor, M. Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry* **142**, 103744 (2022).
18. Ibrahim, H., Debicki, M., Rahwan, T. & Zaki, Y. Big Tech Dominance Despite Global Mistrust. *IEEE Transactions on Computational Social Systems* **11**, 3741–3752 (2024).
19. Bodó, B. Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society* **23**, 2668–2690 (2021).
20. Pati, S. *et al.* Federated learning enables big data for rare cancer boundary detection. *Nat Commun* **13**, 7346 (2022).
21. Barbereau, T., Sedlmeir, J., Smethurst, R., Fridgen, G. & Rieger, A. Tokenization and Regulatory Compliance for Art and Collectibles Markets: From Regulators' Demands for

Transparency to Investors' Demands for Privacy. in *Blockchains and the Token Economy* (eds. Lacity, M. C. & Treiblmaier, H.) 213–236 (2022). doi:10.1007/978-3-030-95108-5_8.
22. Cao, S. S., Cong, L. W. & Yang, B. Distributed Ledgers and Secure Multiparty Computation for Financial Reporting and Auditing. *Management Science* https://doi.org/10.1287/mnsc.2023.02577 (2024) doi:10.1287/mnsc.2023.02577.
23. Fernández, J. D., Menci, S. P., Lee, C. M., Rieger, A. & Fridgen, G. Privacy-preserving federated learning for residential short-term load forecasting. *Applied Energy* **326**, 119915 (2022).
24. Barbereau, T., Fernandez Delgado, J. & Potenciano Menci, S. The governance of federated learning: a decision framework for organisational archetypes. *Data & Policy* **7**, (2025).
25. Bodó, B. & Janssen, H. Maintaining trust in a technologized public sector. *Policy and Society* **41**, 414–429 (2022).
26. Eke, D. & Stahl, B. Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies. *Digital Society* **3**, 11 (2024).
27. Steen, M., Timan, T. & van de Poel, I. Responsible innovation, anticipation and responsiveness: case studies of algorithms in decision support in justice and security, and an exploration of potential, unintended, undesirable, higher-order effects. *AI Ethics* **1**, 501–515 (2021).
28. Veenstra, A.-F., van Zoonen, L. & Helberger, N. *ELSA Labs for Human-Centric Innovation in Artifical Intelligence*. https://nlaic.com/wp-content/uploads/2022/02/ELSA-Labs-for-Human-Centric-Innovation-in-AI.pdf (2021).
29. Fratini, S., Hine, E., Novelli, C., Roberts, H. & Floridi, L. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Digital Society* **3**, 59 (2024).
30. Floridi, L. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philos. Technol.* **33**, 369–378 (2020).
31. Farinha, L., Ferreira, J. & Gouveia, B. Networks of Innovation and Competitiveness: A Triple Helix Case Study. *Journal of the Knowledge Economy* **7**, 259–275 (2016).
32. Leydesdorff, L. The knowledge-based economy and the triple helix model. *Annual Review of Information Science and Technology* **44**, 365–417 (2010).
33. Carayannis, E. G. & Campbell, D. F. J. 'Mode 3' and 'Quadruple Helix': toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management* **46**, 201–234 (2009).
34. Leydesdorff, L. The Triple Helix, Quadruple Helix, …, and an N-Tuple of Helices: Explanatory Models for Analyzing the Knowledge-Based Economy? *Journal of the Knowledge Economy* **3**, 25–35 (2012).
35. Viale, R. & Etzkowitz, H. Third academic revolution: polyvalent knowledge; the"DNA" of the triple helix. in *Fifth Triple Helix Conference* (2005).
36. Hormio, S. & Reijula, S. Universities as Anarchic Knowledge Institutions. *Social Epistemology* **38**, 119–134 (2024).
37. Valero, A. & Van Reenen, J. The economic impact of universities: Evidence from across the globe. *Economics of Education Review* **68**, 53–67 (2019).
38. Jones-Evans, D. & Klofsten, M. Role of the university in the technology transfer process: a European view. *Science and Public Policy* **25**, 373–380 (1998).
39. Etzkowitz, H., de Mello, J. M. C. & Almeida, M. Towards "meta-innovation" in Brazil: The evolution of the incubator and the emergence of a triple helix. *Research Policy* **34**, 411–424 (2005).
40. Etzkowitz, H. Making a humanities town: knowledge-infused clusters, civic entrepreneurship and civil society in local innovation systems. *Triple Helix* **2**, 1 (2014).
41. Draghi, M. *The Future of European Competitiveness: A Competitiveness Strategy for Europe*. https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en (2024).

42. Wennink, P. *De Route Naar Toekomstige Welvaart*. https://www.rapportwennink.nl/downloads/rapport_wennink_12december2025.pdf (2025).
43. European Commission. *A Competitiveness Compass for the European Union*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_339 (2025).
44. Edler, J., Blind, K., Kroll, H. & Schubert, T. Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy* **52**, 104765 (2023).
45. D9+. *Declaration of the D9+ Ministerial Meeting in Copenhagen, 27th of September 2024* -. https://cepa.org/article/the-danish-d9-answer-to-europes-digital-challenges-more-denmark/ (2024).
46. Cools, H., Helberger, N. & de Vreese, C. Co-creating research at The AI, media, and democracy lab: Reflections on the role of academia in collaborations with media partners. *Journalism* 14648849251318622 (2025) doi:10.1177/14648849251318622.
47. Pisa, D., Vierhout, J., Geurts, A. & van Bree, T. *Grip Op Control Points*. https://vector.tno.nl/artikelen/grip-control-points-gerichter-innoveren/ (2024).
48. Barbereau, T., Weigl, L. & van Veenstra, A. F. Untangling the Digital Governance Landscape of the European Union: A Framework and Application to Digital Technologies. in *Electronic Participation* (eds. Hofmann, S. et al.) 159–175 (Springer Nature Switzerland, Cham, 2026). doi:10.1007/978-3-032-02515-9_10.

Acknowledgements

This report was undertaken as part of the Knowledge Investment Project on Digital Trust (2025-2026) as part of the impulse financing Transitions & Transformations.

The authors thank Anne Fleur van Veenstra, Alexander van den Wall Bake, Sarah van Drumpt, Miriam Veronesi, Thijmen van Gend, and Iris Leussink for their contributions and valuable feedback to this whitepaper.

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
tno.vector.nl

TNO Vector